

[+] (IN)SECURE Magazine

07 | 2021

ISSUE 69

Cyber skills

**Why threat hunting is obsolete
without context**

**Review: Group-IB Threat Hunting
Framework**

**Navigating the waters of maritime
cybersecurity**



CIS Controls

Version 8

Simplified & prioritized
cyber defense guidance

Download CIS Controls v8

<https://www.cisecurity.org/controls/v8/>



CIS Controls
Version 8

v8

Table of contents

PAGE 04	Why threat hunting is obsolete without context	PAGE 49	INDUSTRY NEWS
PAGE 07	Review: Group-IB Threat Hunting Framework	PAGE 55	Reformulating the cyber skills shortage
PAGE 25	Navigating the waters of maritime cybersecurity	PAGE 59	Cybersecurity industry analysis: Another recurring vulnerability we must correct
PAGE 30	Defending against Windows RDP attacks	PAGE 62	For CISOs and artificial intelligence to evolve, trust is a must
PAGE 32	SECURITY WORLD	PAGE 64	Quantum computing is imminent, and enterprises need crypto agility now
PAGE 38	The evolution of the modern CISO	PAGE 67	When the adversarial view of the attack surface is missing, digital transformation becomes riskier
PAGE 41	Understanding the cloud shared responsibility model		
PAGE 44	Why is patch management so difficult to master?		
PAGE 47	Preventing security issues from destroying the promise of IoT		

Featured experts

BOBBY CHRISTIAN, COO, Deepwatch

PIETER DANHIEUX, Chairman/CEO, Secure Code Warrior

AMEESH DIVATIA, CEO, Baffle

HEATHER GANTT-EVANS, CISO, SailPoint

TONI GRZINIC, Security Researcher

ANNE HARDY, CISO, Talend

MIKE HEREDIA, VP EMEA & APAC, XM Cyber

MIKE JUMPER, CEO, Glyptodon

PATRICK MELAMPY, Juniper Fellow, Juniper Networks

TODD MOORE, VP of Encryption Solutions, Thales

JUAN PABLO PEREZ-ETCHEGOYEN, CTO, Onapsis

AARE REINTAM, CTO, CybExer Technologies

BRIAN SATIRA, Chief Hacking Officer, Redoubt Research

Visit the magazine website and subscribe at www.insecuremag.com

Mirko Zorz

Editor in Chief

press@helpnetsecurity.com

Zeljka Zorz

Managing Editor

press@helpnetsecurity.com

Berislav Kucan

Director of Marketing

bkucan@helpnetsecurity.com

Why threat hunting is obsolete without context

Bobby Christian

COO, Deepwatch

Cybersecurity is an undisputed concern within any industry – but how are organizations and businesses using the security data and information they collect to best ensure their businesses are protected from cyber threats?

According to PwC, 71% of U.S. CEOs said they are “extremely concerned” about cyber threats – ahead of pandemics and other health crises. Threat hunting is one of the more recent methodologies implemented by IT professionals to find dormant or active threats on their network to better understand and harness network visibility and threat actor entry points. Yet this capability can only be effectively leveraged when practiced in a broader security context.

There exists a need for a slyer intelligence-gathering strategy than what is currently deployed across most organizations, with a focus on not only speed, but accuracy in evaluating incoming threats. Understanding a network environment by maintaining full data visibility, leveraging multiple platforms via a capable, relational MSSP, and consistently monitoring the flow of information and overall network habits are all inextricably tied to effective threat hunting. Without such informational context and external partners, threats could easily be missed and go unaddressed, giving hackers the enough time to wreak havoc.

Investment in threat hunting is on the rise, however reaping the benefits of such an



investment may take a while longer. Although threat hunting's proactive appeal has made it an increasingly popular practice to secure networks, its success is only as valuable as the contextual information gathered within the network the threat was found in, which inherently requires a more sophisticated, comprehensive approach to threat detection and identification.

Understanding a network environment by maintaining full data visibility, leveraging multiple platforms via a capable, relational MSSP, and consistently monitoring the flow of information and overall network habits are all inextricably tied to effective threat hunting.

With companies eager to invest in threat hunting training for their respective security teams, implementing a clear deployment and upkeep strategy for such a deliberate security effort should be a top priority. Automation, responsiveness, data analysis and threat management are four key capabilities of a larger, modernized SOC that aims to effectively add threat hunting to its arsenal of tools:

Automation – The ability to contextualize the exponential amounts of data being produced within a single SOC environment, in addition to responding to what the data indicates, cannot feasibly be carried out by human talent alone. Standing as a customizable tool that lessens the load in a myriad of ways, automation addresses both simple tasks as well as more sophisticated multi-step analysis needs. Intelligent automation can supplement threat hunting efforts managed by personnel, adding an additional layer of security analysis that could easily be overlooked otherwise.

Endpoint Detection and Response (EDR) – Analyzing potential breaches in real-time during both working and non-working hours is non-

negotiable. Attackers aren't always a reflection of their targets – they can originate from other countries, time zones, cultures, or exhibit differing personal habits. By equipping both threat hunters and other trained security analysts with cyber threat intelligence and detection capabilities that identify such activity around-the-clock, security teams can quickly nab an unwelcome visitor. The result is an informed prediction rather than a shot in the dark.

Data analysis – The SOC security perimeter is ever expanding, as evidenced by the dramatic and likely permanent increase in remote work and the pre-existing push to migrate to the cloud. Security events originating from multiple logging areas cannot serve any real contextual purpose if not correlated and cross-examined with each other. Full network visibility is crucial to a comprehensive, educated threat hunting strategy. SaaS, remote devices, and other pieces of the security environment are all potential weak points waiting to be breached. Identifying residual activity across these logging areas requires not only well-trained personnel, but effective software management across disparate platforms.

Full network visibility is crucial to a comprehensive, educated threat hunting strategy.

Threat management – Combining both data analysis and automation tools with a tiered SOC allows for the necessary separation between monitoring, managing, and advising a response to potential threats while maintaining needed communication between each tier in order to execute dedicated tasks adequately. Because of the complexity of a modern SOC, countless security events across scores of platforms can occur within the same security environment, requiring a delegation of responsibilities across a

network to avoid confusion and congestion. Separating monitoring, management, and advising into three tiers eases the workload on a likely overburdened IT department, making room for threat hunting-specific training in addition to existing tasks related to SOC management.

Tracking potential vulnerabilities within IT infrastructure is clearly a necessity. However, its effectiveness is measured by whether these threats can be fully evaluated with tools on-hand.

A powerful combination of security automation with threat detection and response, in conjunction with a relationship focused MSSP, can make threat hunting far more useful than relying on one-off predictions devoid of context.

A powerful combination of security automation with threat detection and response, in conjunction with a relationship focused MSSP, can make threat hunting far more useful than relying on one-off predictions devoid of context.

A robust security posture requires a multi-pronged, layered approach that can be achieved with good partnerships that manage threats effectively without overburdening IT personnel. Threat hunting, although not an antidote on its own, can significantly close the gap by effectively training already experienced IT professionals to not only look for odd behavior within a network, but to harness existing tools at their disposal in a more efficient, proactive, and comprehensive manner. An approach that fosters timeliness, data correlation, automation, and tiered threat management will enable better threat detection and overall risk reduction.

+ **HELPNETSECURITY**



Help Net Security report: XDR

Coming in September 2021.

For promotional
opportunities contact
xdr@helpnetsecurity.com



Review: Group-IB Threat Hunting Framework

Toni Grzinic

Security Researcher

The IT infrastructure of larger organizations is very heterogeneous. They have endpoints, servers and mobile devices running various operating systems and accessing internal systems. On those systems, there is a great number of disparate tools – from open-source databases and web servers to commercial tools used by the organization's financial department. Furthermore, these applications can now also be deployed on different clouds to achieve further resilience, adding even more complexity to an already intricate infrastructure.

Managing IT infrastructure poses a hard problem, especially in these pandemic times where the workforce tends to work remotely. Building an additional layer of security over this infrastructure is a complicated undertaking and the success of

this project will depend on the availability of security personnel and of security monitoring, detection and response tools that can reduce their burden. Unfortunately, due to the complexity of securing infrastructure and the enormous volume of attack vectors, the maturity of organizations' security monitoring can fall behind.

One of the solutions to this problem is to use technologies that can provide visibility in the organization's infrastructure, while simultaneously collecting and detecting anomalous events as well as responding to them.

A few years ago, security expert Anton Chuvakin suggested the concept of EDR (endpoint detection and response) in the form of a lightweight endpoint agent that fills the gap between detection and response capabilities available at that time.

EDR has progressed to the concept of XDR – extended detection and response – which represents a merger of defense and response capabilities between various infrastructure layers (network traffic, email, endpoints, cloud instances, shared storage, etc.).

To be successful, XDR should inspect different layers, record and store events, and – based on its advanced analytics features – correlate events over layers to detect those that should be inspected by higher-tier analysts. The goal is a faster detection and response cycle to reduce the time attackers can lurk in your infrastructure, but also to reduce SOC analysts' alert fatigue and prevent burnout.

We have tested Group-IB's Threat Hunting Framework (THF), which tells the full story of an incident and its mastermind and can correlate events and alerts between different infrastructure layers, before escalating incidents that need additional attention from analysts. Its purpose is to do passive security monitoring, but also to uncover

attacks and reduce the time attackers spend on your systems. It relies on global threat intelligence capabilities by Group-IB that can give analysts additional context regarding security alerts and incidents.

Methodology

For this review, we used a cloud sensor and a Huntbox (management system) instance. We installed Huntpoint, a separate lightweight endpoint agent, on virtualized (KVM) endpoints. The endpoints' operating system was Windows 10 with the latest patches, on which we manually installed Huntpoint. For some use cases we disabled Windows Defender (Microsoft's antivirus solution) so that we can test Huntpoint detection and blocking capabilities in the wild.

On the endpoints, we performed simple test actions to see if these events are later available in THF. We:

- Accessed and downloaded malicious files
- Used Windows Script Host with a VBS script
- Used PowerShell to obfuscate command execution
- Made Wmic process calls
- Dumped NTLM hashes with Mimikatz
- Opened a bind shell with Netcat

We also performed a full infection with the Ryuk ransomware and tried to isolate the host.

To test email detection capabilities, we used various malicious documents (MS Word files, PDFs) and archives that were additionally nested or were password protected. We sent these malicious documents as email attachments from a ProtonMail account, to avoid emails getting blocked from being delivered to the monitored mailbox.

We tested THF Polygon, the malware detonation platform, with the same set of files. We manually tested Ryuk and Sigma ransomware by uploading them to Polygon. Other malicious files from the test dataset were sent automatically from Huntpoint. The collected indicators were used for testing Group-IB Threat Intelligence & Attribution system.

During the test we kept an eye on these success factors that helped us form a final opinion of the product:

- Detection capabilities (endpoint events, files and email)
- Ease of use and integration capabilities
- Threat Intelligence data quality while providing context for existing events
- Resource consumption (CPU/RAM for EDR, etc.)

Threat Hunting Framework

Group-IB's Threat Hunting Framework (THF) is a solution that helps organizations identify their security blind spots and gives a holistic layer of protection to their most critical services both in IT and OT environments.

The framework's objective is to uncover unknown threats and adversaries by detecting anomalous activities and events and correlating them with Group-IB's Threat Intelligence & Attribution system, which is capable of attributing cybersecurity incidents to specific adversaries. In other words, when you spot a suspicious domain/IP form in your network traffic, with a few clicks you can pivot and uncover what is behind this infrastructure, view historical evidence of previous malicious activities and available attribution information to help you broaden or quickly close your investigation. THF closely follows the incident response process by having a dedicated component for every step.

There are two flavors of THF: the enterprise version, which is tailored for most business organizations that use a standard technology stack (email server, Windows domain, Windows/macOS endpoints, proxy server, etc.), and the industrial version, which is able to analyze industrial-grade protocols and protect industrial control system (ICS) devices and supervisory control and data acquisition (SCADA) systems.

Threat Hunting Framework is able to:

- Analyze network traffic and detect suspicious activities (covert channels, tunnels, remote control, C&C beaconing) by using the Sensor module
- Terminate encrypted connections at Layer 2 and Layer 3
- Integrate with on-premises and cloud email systems
- Provide visibility into endpoints and manage incidents on them using the EDR component/system called THF Huntpoint. THF Huntpoint can detect popular privilege escalation attacks and lateral movement techniques (pass-the-hash/ticket, Mimikatz, NTLM bruteforce, use of living-of-the-land binaries and similar tools)
- Analyze files by using the malware detonation platform THF Polygon
- Perform advanced threat hunting using logs from THF Huntpoint, email channel, traffic and behavior markers of each analyzed file from any source
- Detect anomalies and unknown threats by correlating all available data between various THF modules
- Enriching events with data/information from Group-IB's Threat Intelligence & Attribution cloud database

All the data is enriched and available from a central dashboard and management system called THF Huntbox. THF Huntbox enables incident management, correlation of events and collaboration between analysts during threat

hunting and IR activities. All network traffic anomalies, email alerts, Huntpoint detections, and files detonated within Polygon are available and the user can correlate the event data (IoCs) with the Threat Intelligence & Attribution database by using graph analysis and other techniques.

THF can also be paired with CERT-GIB (Group-IB's Computer Emergency Response Team) by sending telemetry data or IoCs for further investigation by experts, which can bring a higher level of expertise to complex incidents and increase the maturity level of your SOC.

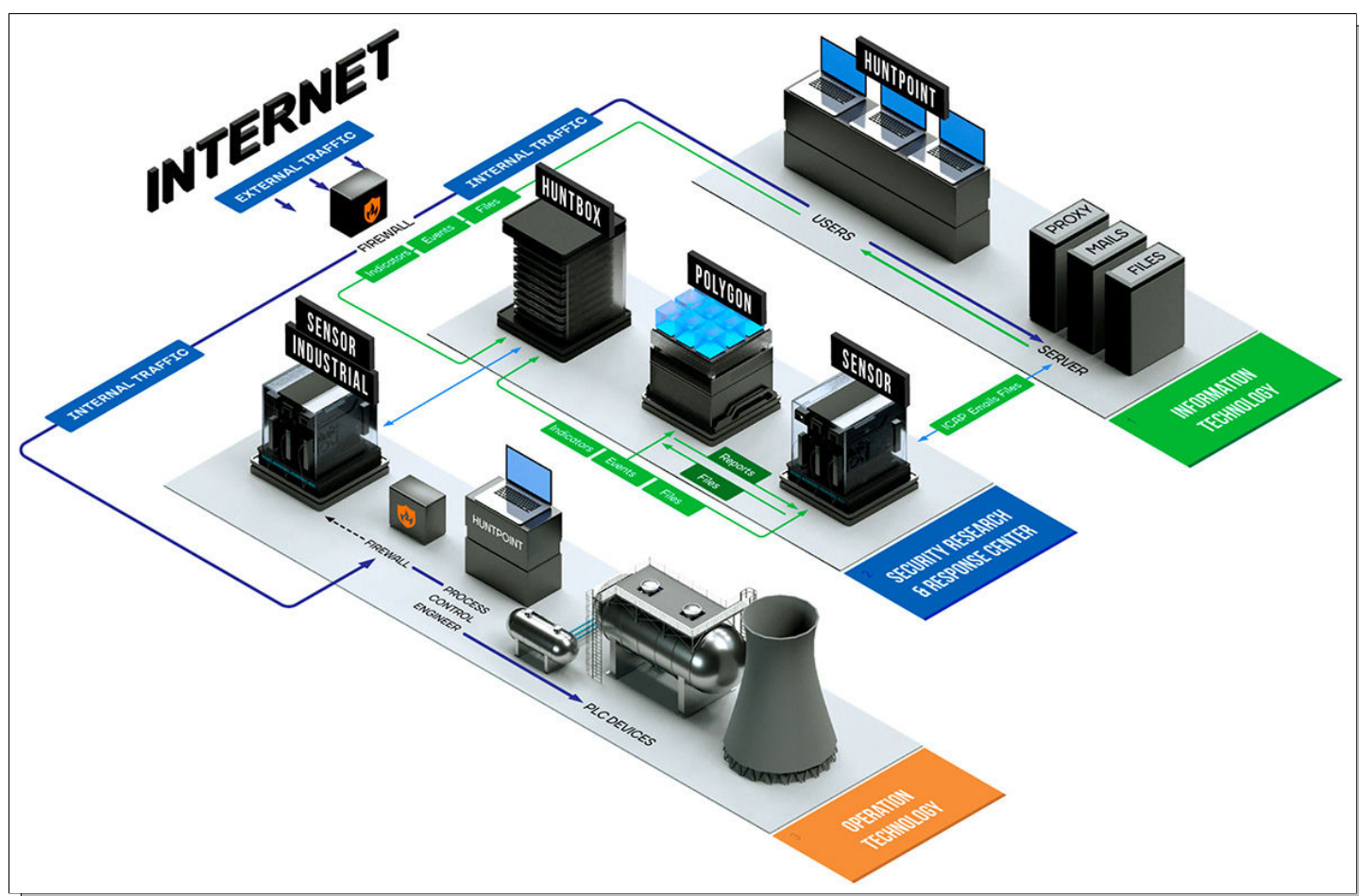


FIGURE 1 – THREAT HUNTING FRAMEWORK'S ARCHITECTURE WITH ALL AVAILABLE COMPONENTS

THF components

THF Sensor and THF Decryptor

THF Sensor is a system used to analyze incoming and outgoing network traffic in real-time, extract files from it, using ML-based intelligence traffic analysis approaches (to detect lateral movement, DGA activity and covert tunnels) and signatures,

block suspicious files (with the proxy, ICAP integration). All files that are collected from the network traffic can be sent to THF Polygon, a file detonation system that is used for behavioral analysis.

Sensor comes as a 1U physical appliance or can be deployed as a Virtual Machine depending on your use case and requirements. For analyzing

250Mbps over a SPAN port, you will need at minimum 32Gb RAM and 12 vCPUs. Sensor can analyze mirrored traffic from the SPAN/RSPAN port, TAP devices or traffic from RSPAN sent over GRE tunnels, meaning that, when deployed, it has no effect on the enterprise network throughput. Sensor supports a wide range of bandwidth configurations, the standard versions support 250, 1000 and 5000 Mbps, but Sensor can support high throughput architectures up to 10 Gbps. Client is able to use more than one Sensor and basically cover any bandwidth, even at the ISP level.

During analysis, THF Sensor can detect network anomalies such as covert channels, tunnels, remote control, and various techniques of lateral movement. It can also extract email content from mail traffic and analyze it – this capability is pretty interesting because it allows it to spot passwords for archive files sent in emails (and avoid brute-forcing them).

There is a special THF Sensor version tailored for industrial systems – THF Sensor Industrial – which is able to dissect ICS protocols. Sensor Industrial supports a variety of ICS protocols (Modbus, S7comm, S7comm+, UMAS, OPCUA, OPCDA, IEC104, DNP3, DeltaAV, CIP, MQTT and other), and can detect topology changes and control integrity of software and firmware used on PLCs. It is also possible to set up detection rules

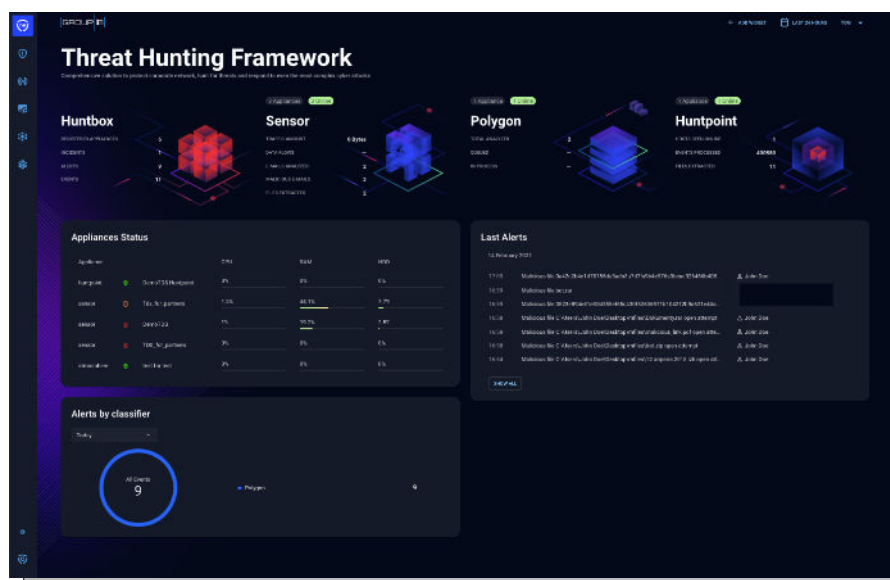
based on policies that are available through the configuration options.

THF Sensor can analyze encrypted sessions by using the THF Decryptor component, which detects TLS/SSL-protected sessions, performs a certificate replacement and can route the proxied traffic. THF Decryptor supports all popular TLS versions (1.1 – 1.3) and cipher suites. It can be deployed and works in various modes: transparent (bridge) mode that works on OSI Layer 2 where it is invisible to the user network, or gateway (router) mode, where it acts as a gateway for the user networks.

THF Huntbox

THF Huntbox is a central management dashboard and reporting point of Group-IB Threat Hunting Framework. It is accessible as a web application and contains management capabilities for THF components (THF Sensor, THF Polygon, and THF Huntpoint) and acts as a correlation engine for managing events, alerts and incidents as well as scalable storage for all collected raw logs and other data. Through the THF Huntbox interface, users can see event details, create reports and escalate incidents, as well as produce reports and do threat hunting in the local and global context. THF Huntbox acts as a front-end for THF Polygon's dynamic analysis reports.

FIGURE 2 – THE THF HUNTBOX WELCOME SCREEN IS A DASHBOARD CONTAINING THE APPLIANCE STATUS, STATISTICS AND LATEST ALERTS



THF Huntbox has the following sections:

- **Incidents** – Critical tickets that need analysts' immediate attention and resolution. It is possible to collaborate and comment on the progress with other analysts within your organization. We collaborated with CERT-GIB, their support is a high value service that can augment users' detection and response ability

- **Alerts** – Potentially malicious events escalated by various THF components (e.g., THF Polygon, THF Huntpoint), containing correlated events and detection information

- **Graph** – Group-IB's tool for network analysis running on Group-IB Threat Intelligence & Attribution database that contains threat data and historical information of all network nodes (including Whois history, SSLs, DNS records, etc.) intelligence, but also unstructured data collected from various underground communication channels, forums and social networks

- **Investigation** – All available events are located here. This section is divided into:

- **Emails** – Containing all analyzed emails

and detections of potentially harmful content

- **Files** – Containing all the files extracted from network traffic, proxy-server, endpoints, emails, file shares. Files also could be uploaded for dynamic analysis manually or automatically with API. For every file there is an available Polygon report that provides a verdict on whether the file is malicious or benign

- **Computers** – Containing details on and available actions (e.g., isolation from network) for all endpoints registered to the THF instance

- **Huntpoint events** – Containing all events collected from Huntpoint clients

- **Network connections** – Containing extracted network connections from the sensors.

- **Reports** – Containing summary reports of all activity in a given date range and reports related to specific incidents, alerts or events.

FIGURE 3 – CORRELATION IN ACTION: MULTIPLE MALICIOUS EMAILS SENT FROM THE SAME ADDRESS RESULTED IN AN ESCALATION OF AN INCIDENT

The screenshot shows the THF Huntbox interface with a dark theme. At the top, there's a header bar with a search icon, a timestamp '14.02.2021 16:59:54', a notification '6 min ago', and a title '(1-24Z) Malicious email from @protonmail.com'. Below the header, there's a section for 'Malicious email from @protonmail.com' with a 'SpyEye +1' badge. To the right, there are statistics: 'Users: 1', 'Computers: 0', 'Files: 2', 'Hosts: 0', and a 'MARK AS' dropdown. The main content area is divided into two panels. The left panel has a 'Attributes TI' section with 'Malware' (2) and 'Threat Actor' tabs, showing 'SpyEye' and 'Zeus' badges. Below it is an 'Alerts' section with a search bar and a 'GO TO ALL' button. The right panel has a 'Timeline' section with 'Comments' (0) and 'All events' (1) tabs, a 'Your Comment' input field, and a 'SEND COMMENT' button. At the bottom, there's a table of alerts with columns: Created, Status, Reason, Target, and Appliance. The table lists two detected malicious files from the same email address.

Created	Status	Reason	Target	Appliance
14.02.2021 16:59:48 10 min ago	Detected	Malicious file Malicious file bot.rar SpyEye Zeus	@mailcheck.group-1	Tds_for_partners
14.02.2021 16:59:12 12 min ago	Detected	Malicious file Malicious file 0523e894e81e00d355ef65c430f52636971b104212b9a621e44aa003816a3be4	@mailcheck.group-1	Tds_for_partners

Found: 2

We spent most of the time in the Investigation section, searching for raw events and combing the files and emails reports. Events and their metadata can be integrated with SIEMs with syslog and with other monitoring systems. THF correlates and aggregates events across all of its modules (e.g., email from THF Sensor and a THF Polygon analysis of malicious attachment) and can block them automatically or manually, based on your configuration, rules and policies (see Figure 3 for email). THF Huntbox workflows are easy to get used to, help reduce analysts' cognitive load and allow them to focus on actionable alerts. All triaging features are present in a central place and searching for additional context is available under the Graph view.

THF Huntbox can also replace a classical ticketing

system for tracking incidents and alerts. The Alerts and Incident sections are helpful for incident response workflows, lots of events can be automatically correlated and analysts can link alerts to incidents, manually correlate events and comment on the timeline.

Alerts are usually triggered by specific indicators of compromise (domains, IPs, files, emails, Huntpoint events) found during threat hunting activities. Incidents contain one or multiple alerts and other relevant events that give more context.

The collaboration option removes the need for having another system for this specific purpose. Analysts can comment and attach files (although a wider view would be helpful for lengthy comments).

Alert Info

Events

Date	Time	Event	Indicators
14.02.2021	16:38	Malicious file 8d54dbe841c95ba67549e8e28a4fbddbf87032e8736f01ec5a4563d3f7e6bfe1	Filename: 8d54dbe841c95ba67549e8e28a4fbddbf87032e8736f01ec5...

Source Details

Hostname:	DESKTOP-9E21DTA
Integration:	Huntpoint
Time Received:	14.02.2021 16:38
Path:	C:\Users\John Doe\Desktop\8d54dbe841c95ba67549e8e28a4fbddbf87032e8736f01ec5a4563d3f7e6bfe1

Threat Details

Filename:	8d54dbe841c95ba67549e8e28a4fbddbf87032e8736f01ec5a4563d3f7e6bfe1 (3207.9 kB)
MD5 / SHA1 / SHA256	674936a2beb25def88db410f3d1b68de
Verdict:	Malicious, 98%
Reports:	7b4d1828d5d006eb2df1c9a4cc3ee7a69519edd0

Timeline

Comments 1 All events 1

Your Comment

15.02.2021

16:15

Comment

Hallo!
We have detected a malicious file on a host.

Danger degree: Malware
Functional: CryptoLocker

Description:
CryptoLocker - as the name implies, when it hits the victim's machine, it starts the

FIGURE 4 – ALERT CONTAINS A TIMELINE WHERE IT IS POSSIBLE TO COLLABORATE AND COMMENT ON NEW FINDINGS



THF Huntpoint

THF Huntpoint is a lightweight agent installed on endpoints that collects and analyzes all system changes and user's behaviour (80+ events types, including created processes, inter-process communications, registry changes, file system changes, network connections, etc.), and extracts files from the endpoints and forwards them to THF Polygon for additional analysis. It is used to achieve full visibility of an organization's endpoints

and provides a complete timeline of events that happened on it.

THF Huntpoint detects anomalies and blocks malicious files and can be used to remotely collect forensic data needed for triage or to isolate the infected machine during incident response. The events can be searched with a query language that is similar to other SIEM query languages, like Splunk and Elasticsearch. An example of event details can be seen in Figure 5.

The screenshot displays the THF Huntpoint interface. At the top, the breadcrumb navigation shows 'Investigation / Huntpoint Events / 02E90FC5'. A search bar contains the query 'Header.EventId: "93FF65A8-533C-7D9F-B043-025002E90FC5"'. Below the search bar, a status bar indicates '54 · No error'. A 'START - END' button is on the left, and a 'Sort by' dropdown is set to 'TIMESTAMP'. The main table lists event details with columns: Time, Domain Name, Host Name, User, Event Type, and Details. The selected event is a 'File creation' event on 'DESKTOP-9E21DTA' by 'John Doe' at '14.02.2021 14:08:12'. Below the table, the 'Event Data' section provides a detailed view of the event's metadata, including timestamps, event ID, host name, machine ID, session ID, login ID, user name, domain name, SID, process unique ID, and thread unique ID.

Time	Domain Name	Host Name	User	Event Type	Details
14.02.2021 14:08:12	DESKTOP-9E21DTA	DESKTOP-9E21DTA	John Doe	File creation	C:\Windows\System32\GroupIB-THF-test.txt

Field	Value
Header.Timestamp	2021-02-14T14:08:12.8671008Z
Header.type_description	File creation
@timestamp	2021-02-14T15:18:47.16908858Z
Delay	4234301
Search_id	eclipse_events_tnz8680y2xp1vzch-000066_-93FF65A8-533C-7D9F-B043-025002E90FC5
Header.EventId	93FF65A8-533C-7D9F-B043-025002E90FC5
Header.HostName	DESKTOP-9E21DTA
Header.MachineId	24EBE0EC-D7B3-9028-6035-E8124F68C3ED
Header.Type	9
Header.SessionId	1
Header.LoginId	0x0-0x4c51e
Header.UserName	John Doe
Header.DomainName	DESKTOP-9E21DTA
Header.Sid	S-1-5-21-3267428317-3493302573-3492962365-1001
Header.ProcessUniqueId	F529B882-FE2F-C5DC-6073-BAE3F5B6C018
Header.ThreadUniqueId	5F4CB1CF-31CC-D432-D56A-9D5A681D57C7

FIGURE 5 – HUNTPOINT EVENT DETAILS



Installing THF Huntpoint is a simple process. We installed it manually, but it can be installed with Group Policy or via a specialized THF Huntpoint Installer that is integrated with Active Directory.

We tested our endpoints with malicious files in various formats (documents, executables, archives

like ZIP, RAR, ISO). Our tests were performed with Windows Defender turned off to not interfere with THF Huntpoint's detection capabilities. Huntpoint detected all malicious files on the first try, files were quarantined and triggered alerts visible in THF Huntbox, as shown in Figure 6.


















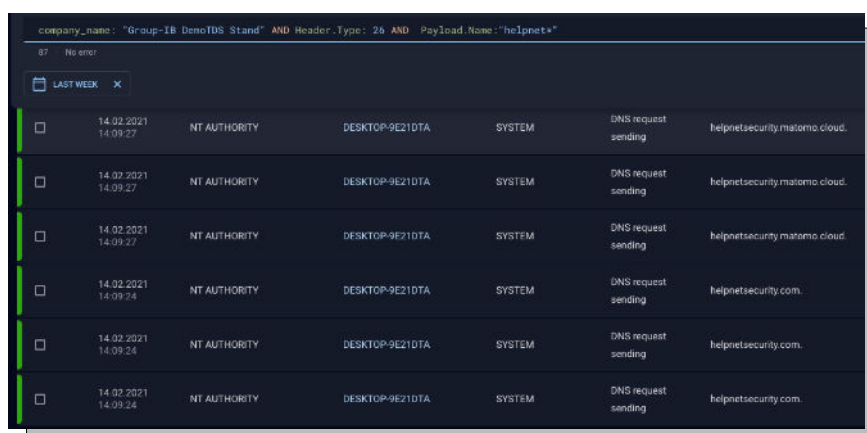
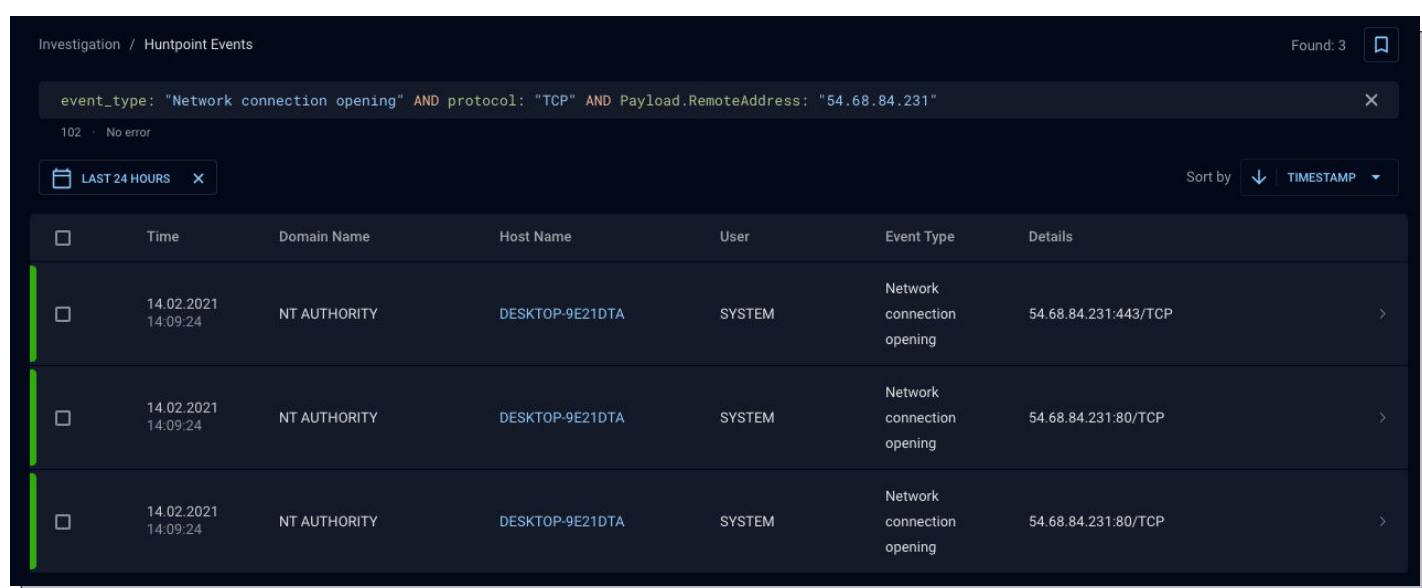
<input type="checkbox"/>	14.02.2021 16:54:59 🕒 2 hours ago	 Blocked	Huntpoint activity Malicious file C:\Users\John Doe\Desktop\vmfiles\12_anpna 2018.lzh open attempt	 John Doe  DESKTOP-9E21DTA	DemoTDS Huntpoint	 2	
<input type="checkbox"/>	14.02.2021 16:41:53 🕒 1 hour ago	 Detected	Huntpoint activity Malicious file bot.exe	 John Doe  DESKTOP-9E21DTA	DemoTDS Huntpoint	 1  2	
<input type="checkbox"/>	14.02.2021 15:58:22 🕒 2 hours ago	 Blocked	Huntpoint activity Malicious file C:\Users\John Doe\Desktop\94823.doc open attempt	 John Doe  DESKTOP-9E21DTA	DemoTDS Huntpoint	 5  2	

FIGURE 6 – MALICIOUS FILES DETECTED WITH HUNTPPOINT

THF Huntpoint gives a lot of insight into what is happening on the endpoint. All user activity – creating or opening of files/processes/ threads/registry keys, network traffic and more – is visible under the Huntpoint Events section in Huntbox.



Time	Domain Name	Host Name	User	Event Type	Details
14.02.2021 14:09:27	NT AUTHORITY	DESKTOP-9E21DTA	SYSTEM	DNS request sending	helpnetsecurity.matomo.cloud.
14.02.2021 14:09:27	NT AUTHORITY	DESKTOP-9E21DTA	SYSTEM	DNS request sending	helpnetsecurity.matomo.cloud.
14.02.2021 14:09:27	NT AUTHORITY	DESKTOP-9E21DTA	SYSTEM	DNS request sending	helpnetsecurity.matomo.cloud.
14.02.2021 14:09:24	NT AUTHORITY	DESKTOP-9E21DTA	SYSTEM	DNS request sending	helpnetsecurity.com.
14.02.2021 14:09:24	NT AUTHORITY	DESKTOP-9E21DTA	SYSTEM	DNS request sending	helpnetsecurity.com.
14.02.2021 14:09:24	NT AUTHORITY	DESKTOP-9E21DTA	SYSTEM	DNS request sending	helpnetsecurity.com.



Time	Domain Name	Host Name	User	Event Type	Details
14.02.2021 14:09:24	NT AUTHORITY	DESKTOP-9E21DTA	SYSTEM	Network connection opening	54.68.84.231:443/TCP
14.02.2021 14:09:24	NT AUTHORITY	DESKTOP-9E21DTA	SYSTEM	Network connection opening	54.68.84.231:80/TCP
14.02.2021 14:09:24	NT AUTHORITY	DESKTOP-9E21DTA	SYSTEM	Network connection opening	54.68.84.231:80/TCP

FIGURE 7 AND 8 – HUNTPPOINT EVENTS SEARCH BY DOMAIN NAME AND IP ADDRESS

To perform a simple test, we created a text file (action visible in THF Huntbox in Figure 5) and we visited helpnetsecurity.com (action visible in THF Huntbox in Figure 7). Without digging deeply in the documentation, we successfully found the needed fields for querying events. Although, time and patience are needed to get used to field names and become nimble with Huntpoint events querying for more complex queries.

In THF Huntbox, you can save searches for future investigations and even share these searches with

your colleagues. This comes in handy when you want to have a “cookbook” of basic queries to detect some popular misuse cases (e.g., suspicious PowerShell downloads).

The other THF Huntpoint tests that we performed were related to malware infections. We infected our endpoint with ransomware, and the executable files have been sent to THF Polygon for detonation and a final verdict. The infections were successfully detected (Figure 9) and were visible in THF Huntbox under Alerts.

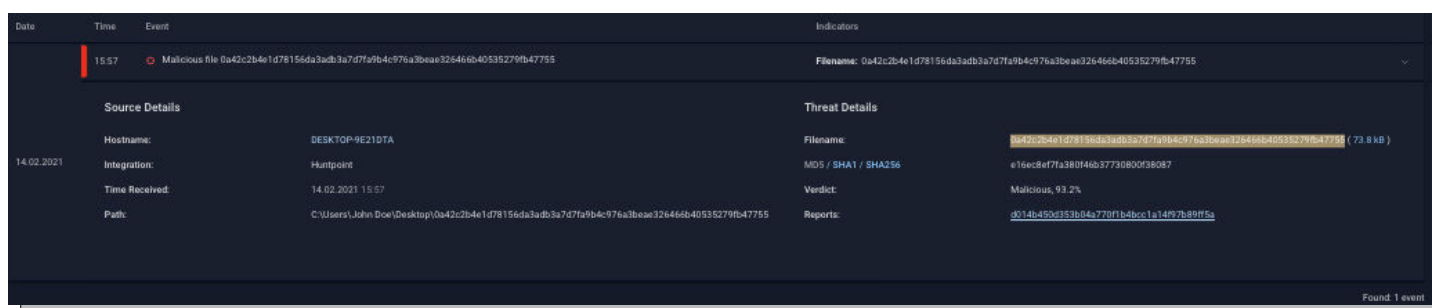
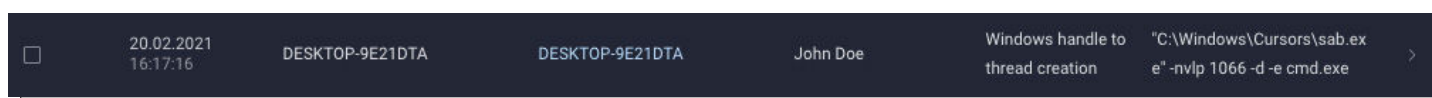


FIGURE 9 – DETECTION OF RANSOMWARE THAT HAS BEEN SENT TO POLYGON

During this last test, the THF Huntpoint client on the endpoint consumed only 20-40 Mb of RAM, with an unnoticeable pressure on CPU usage. From a performance standpoint, you get full visibility with minimum impact on resources. Due to a big number of events during the ransomware infection, we noticed that there was a short delay before some events became available in Huntbox,

but after some time, all events were available for querying.

We performed simple tests to see if all scenarios that can be performed by an attacker are recorded in THF Huntpoint and available in THF Huntbox. E.g., in Figures 10 and 11 you can see the detection of Netcat use and of a simple encoded PowerShell execution of a command.



<input type="checkbox"/>	20.02.2021 16:25:21	DESKTOP-9E21DTA	DESKTOP-9E21DTA	John Doe	Windows handle on the process creation	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Enc cABpAG4AZwAuAGUAeABIA CAAZwBvAG8AZwBsAGUAL gBjAG8AbQA=
--------------------------	------------------------	-----------------	-----------------	----------	--	---

FIGURE 10 AND 11 – EVENTS CONTAINING NETCAT AND POWERSHELL MISUSE

We also tried using Mimikatz to dump NTLM hashes present on endpoints, and this event was also successfully detected and escalated to an incident (Figure 12).

The screenshot displays the THF Huntpoint interface. At the top, a table lists events with columns: Created, Status, Reason, Target, Appliance, and Activity. An event is highlighted with a red bar, showing it was created on 19.02.2021 at 15:35:50, detected 5 days ago, and classified as an incident. Below this, the 'Alert Info' section shows the event details. The event is titled 'Malicious file pap.exe' and is classified as 'Incident'. The event details include a search bar, a classifier dropdown, and a severity dropdown. The event details table shows the date, time, event, and indicators. The event occurred on 14.02.2021 at 20:15. The source details include Hostname: DESKTOP-9E21DTA, Integration: Huntpoint, Time Received: 14.02.2021 20:15, and Path: C:\Windows\Branding\pap.exe. The threat details include Filename: pap.exe (1309.5 kb), MD5 / SHA1 / SHA256: a3cb3b02a6832757e0a0f8a9a5c9e07, Verdict: Malicious, 100%, and Reports: d241df7b9d2ec0b8194751cd5ce153e27c040f4. A 'SEND COMMENT' button is visible on the right side of the interface.

FIGURE 12 – USE OF MIMIKATZ DETECTED ON HUNTPOINT ENDPOINT, VISIBLE AS AN ALERT

THF Huntpoint is available only for Microsoft Windows for now, but in the near future should also be available for other platforms like macOS and Linux.

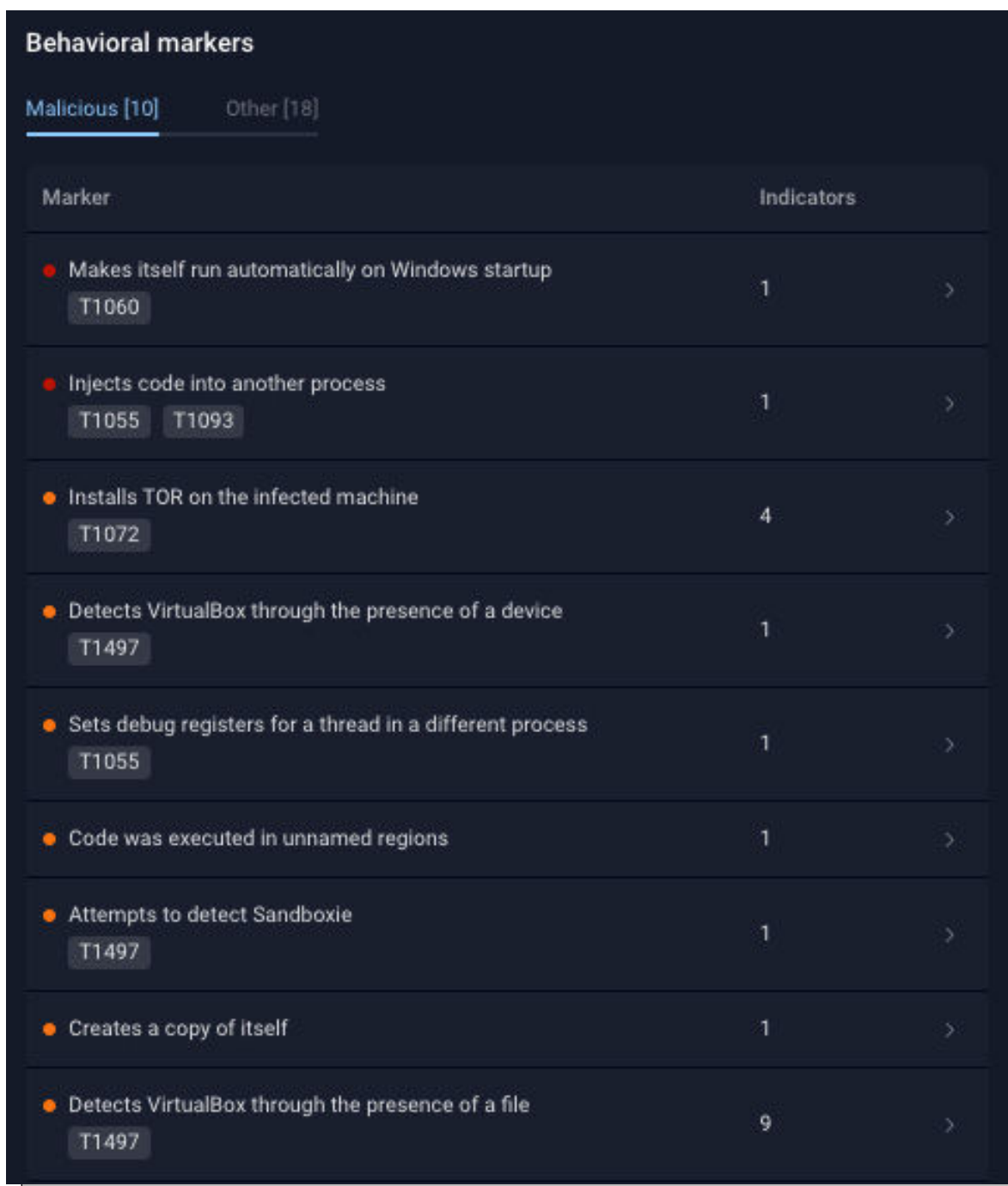
THF Polygon

THF Polygon is a file detonation platform. It is integrated in THF with the purpose to analyze unknown files and emails in an isolated environment. The source of files can be network traffic from THF Sensor, ICAP integration for web-traffic analysis, local/public file storage, the THF Huntpoint client or API integrations.

Group-IB has developed and maintains an open source library to simplify integration with THF Polygon API so it could be employed in any existing application or a workflow that deals with untrusted sources of URLs of files (ticket systems, support chats, etc). The library is available on GitHub and it's really easy to start using it.

Another integration capability we liked is the existing integration with Palo Alto XSOAR solution: this allows to embed THF Polygon to existing security workflows that run on XSOAR platform.





Behavioral markers	
Malicious [10]	Other [18]
Marker	Indicators
<ul style="list-style-type: none">● Makes itself run automatically on Windows startup <div>T1060</div>	1 >
<ul style="list-style-type: none">● Injects code into another process <div>T1055 T1093</div>	1 >
<ul style="list-style-type: none">● Installs TOR on the infected machine <div>T1072</div>	4 >
<ul style="list-style-type: none">● Detects VirtualBox through the presence of a device <div>T1497</div>	1 >
<ul style="list-style-type: none">● Sets debug registers for a thread in a different process <div>T1055</div>	1 >
<ul style="list-style-type: none">● Code was executed in unnamed regions	1 >
<ul style="list-style-type: none">● Attempts to detect Sandboxie <div>T1497</div>	1 >
<ul style="list-style-type: none">● Creates a copy of itself	1 >
<ul style="list-style-type: none">● Detects VirtualBox through the presence of a file <div>T1497</div>	9 >

FIGURE 13 – MALICIOUS BEHAVIOR MARKERS OF THE ANALYZED FILE

The analyzed file is executed in an isolated environment, and after a few (2-5) minutes you get the full behavior analysis report regarding the file, network, registry, process events that were recorded (Figure 13). You can preview the execution changes through a video that shows how the analyzed artifact behaves.

Behavior markers are available as a list or as a populated MITRE ATT&CK matrix (Figure 14). You can also view the file composition and the process tree (Figure 15), which can be useful in detecting techniques that involve process changes (e.g., process injection or process hollowing).

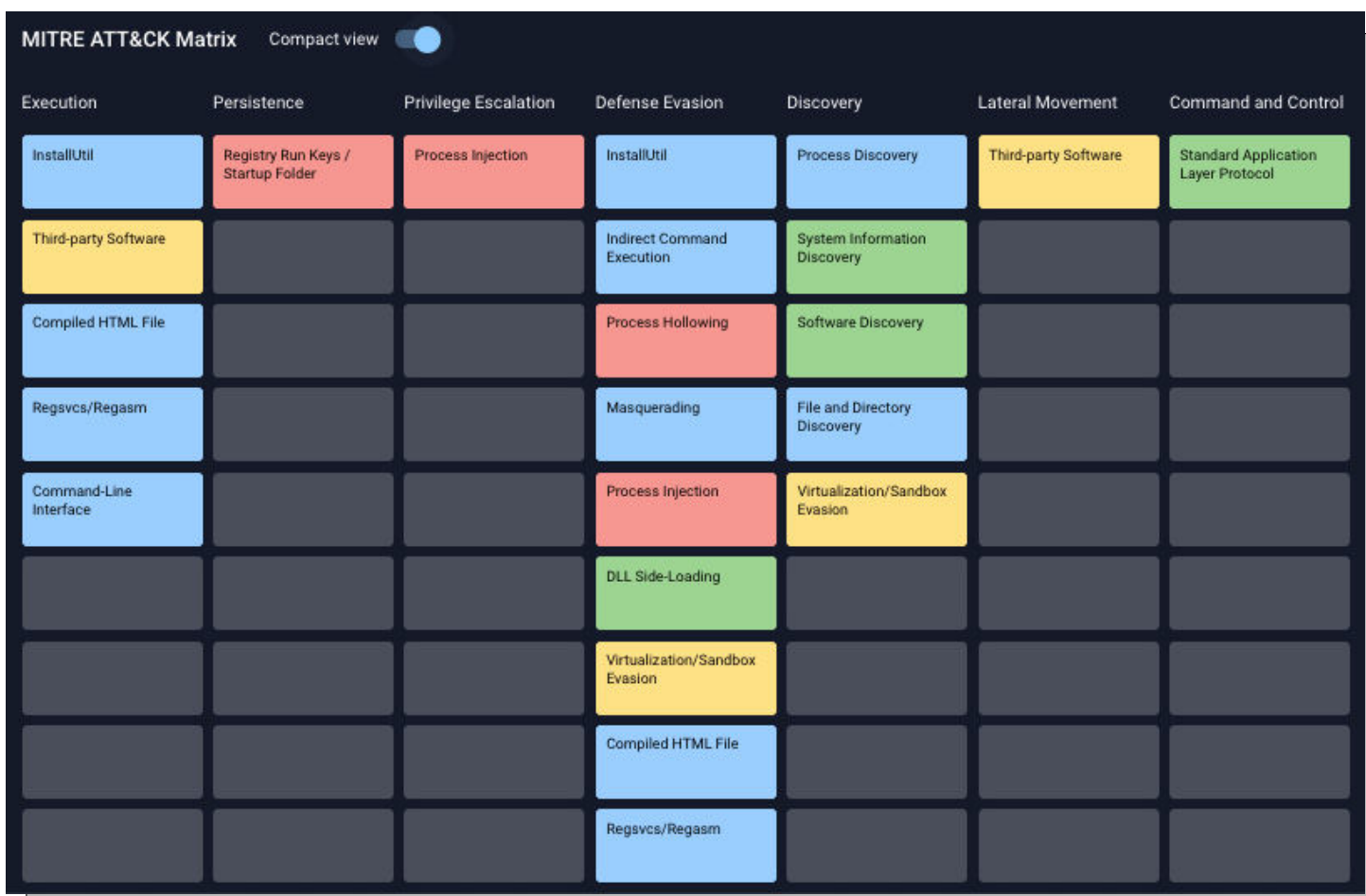


FIGURE 14 – MALICIOUS MARKERS IN A MITRE ATT&CK MATRIX

All IoCs that are collected with THF Polygon can be enriched using Graph Network Analysis to get a global context. THF Polygon can also be used via an API that can trigger analysis and fetch results when it's finished.

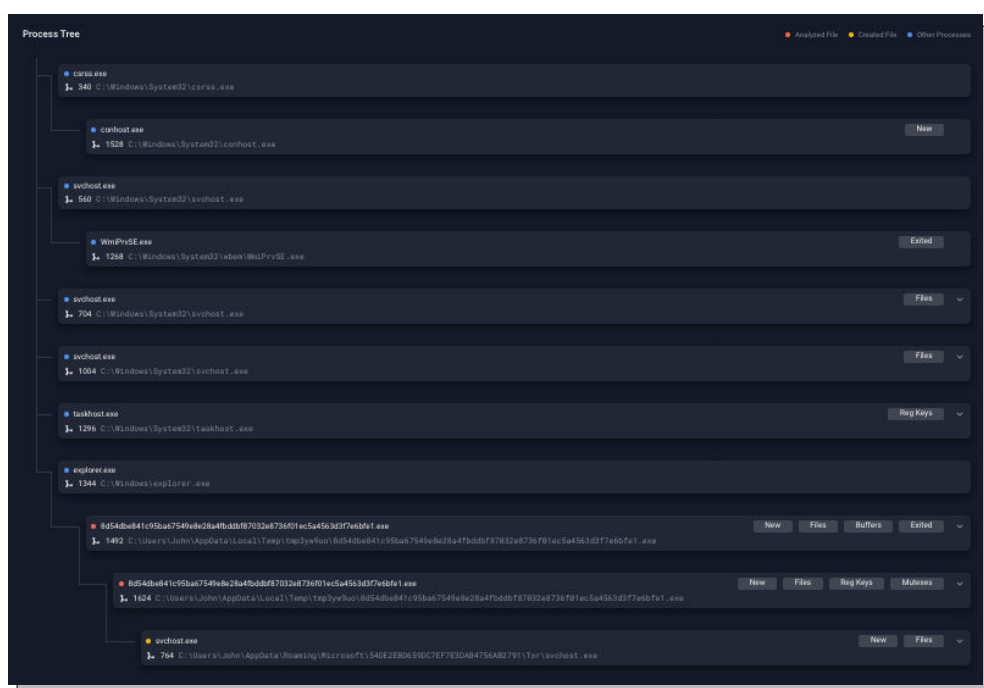


FIGURE 15 – PROCESS TREE IN THE THF POLYGON REPORT

As we described in the Methodology section of this review, we tried sending malicious attachments to the monitored mailbox. In Figures 16-18, you can see that the files that contained a malicious document and the same archived document were successfully detected after scanning the files with THF Polygon. The mail integration is available for internal mail servers but there is also a new

component (Atmosphere) that can scan and detect attacks for mailboxes that are cloud-based (e.g., Office 365 or Google for Business). The mail integration performs attachment and link analysis, but can also detect BEC and spear phishing (i.e., emails that often don't contain attachments or links).

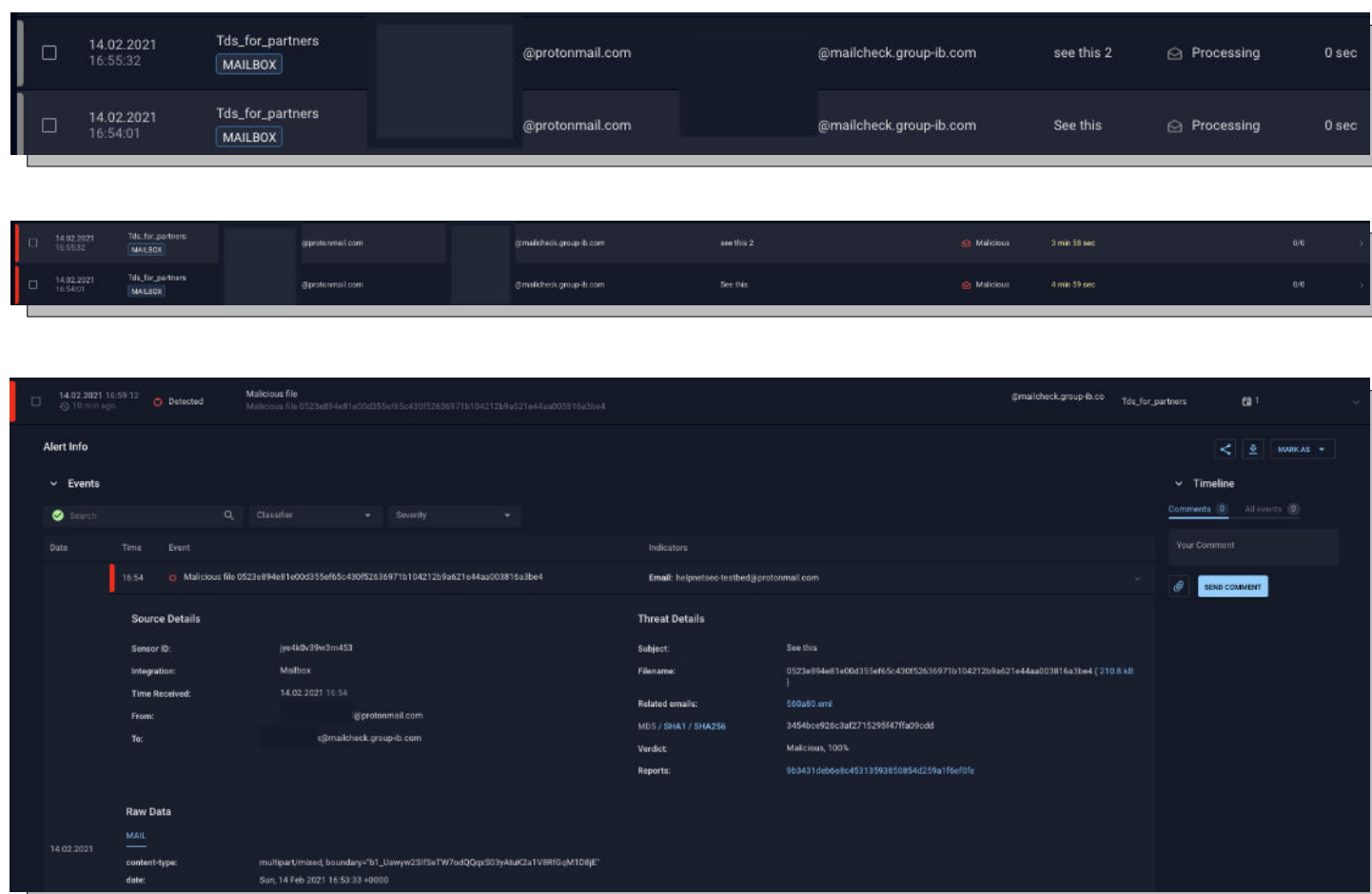


FIGURE 16, 17, 18 – EMAIL PROCESSING AND DETECTION IN ACTION

Graph view (Group-IB Threat Intelligence & Attribution)

Global Threat Intelligence & Attribution is a threat intelligence database and analytical tool that is the result of Group-IB's efforts aimed at meticulously collecting and scanning the internet for more than a decade. The database contains:

- The whole available IPv4 and IPv6 spaces (scanned daily)
- 211 million SSH fingerprints
- 650 million domains with historical data going back for more than 16 years (including DNS registration changes, WHOIS records)

- 1.6 billion certificates
- Hashes of malicious files
- Data collected from forums and social networks
- The interface is simple and similar to that of another Group-IB product – the Fraud Hunting Platform.

This THF component is invaluable, because sometimes you can spot a weird domain or hash while investigating some events and you need

more context around it. You copy the indicator in the Graph view and in seconds you have a whole connected graph that helps you to level up your investigation capabilities.

For example, we used a malicious domain that was part of Emotet campaigns, the result is visible in Figure 19. You can refine your search results by shrinking the timeline under the actual graph. Or you can control the depth of the graph by defining the number of steps that refines the number of indicators you can see from the main one – this is helpful with indicators that have a lot of interconnections.

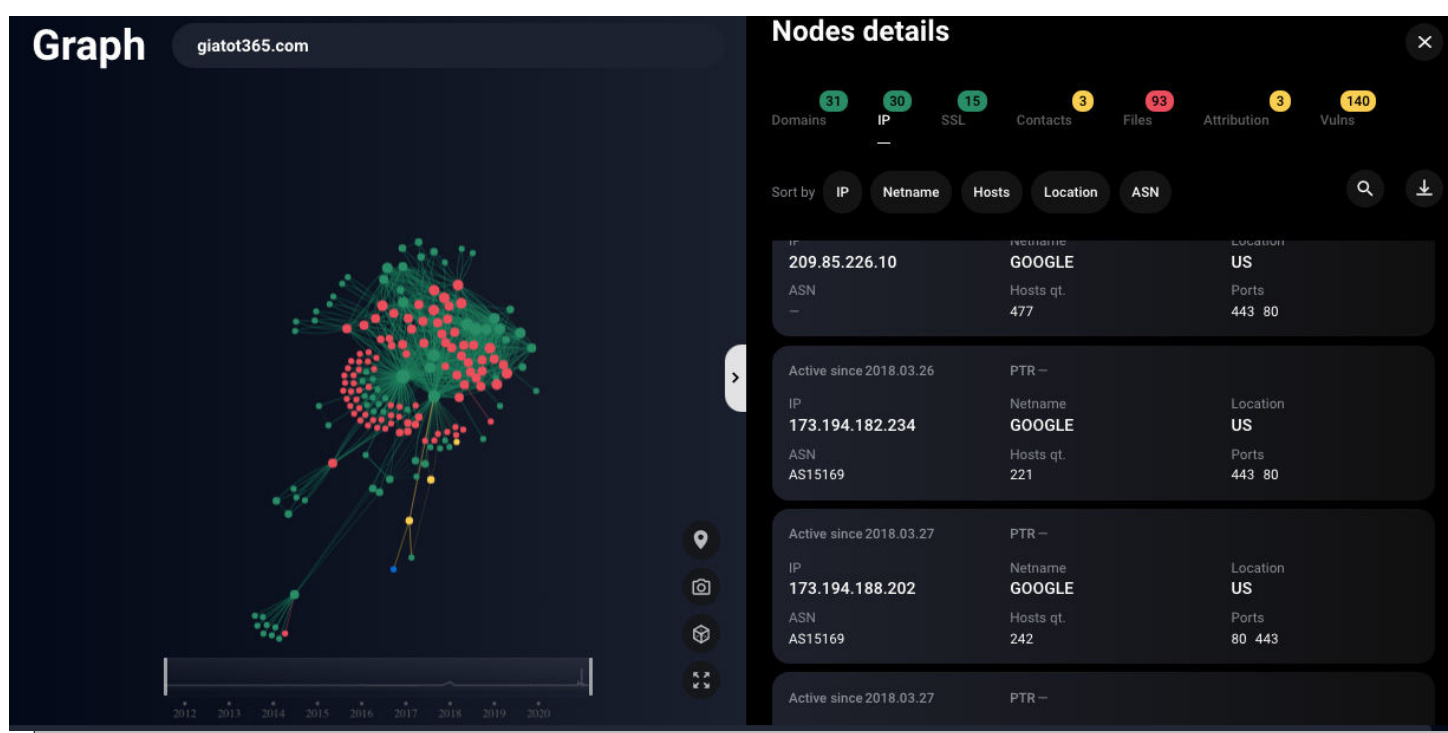


FIGURE 19 – GRAPH SHOWING DATA ABOUT AN EMOTET-LINKED DOMAIN

THF takes care of private data and it is compliant with various data security and privacy legislation, so it uses masks to hide private information (e.g., telephone numbers available from social networks). Graph is certainly helpful to analysts but also to law enforcement, because it can be

used to build a complete image of a malware campaign's back-end infrastructure. It is not uncommon for organizations like national CERTs, INTERPOL and Europol to collaborate and partner with Group-IB in takedowns of malware infrastructure and operations.

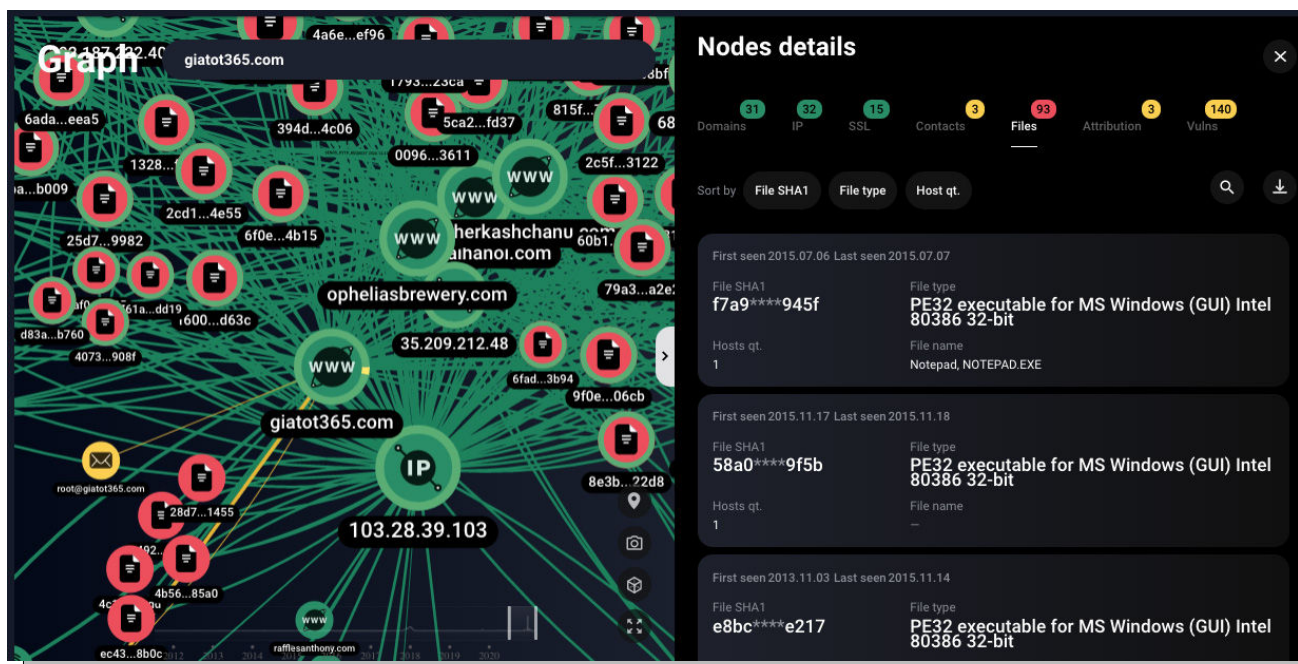


FIGURE 20 – FILES RELATED TO A DOMAIN

Graph Network Analysis enables the attribution of specific indicators to a specific threat, and also to correlate events that at first look unrelated. In Figure 21 you can see that our domain search resulted in the attribution to the Emotet campaign.

Compared to manual analysis, which can be a rabbit hole with single indicators spawning additional ones that also have to be analyzed, graph analysis saves your time when you find a suspicious domain in your logs.

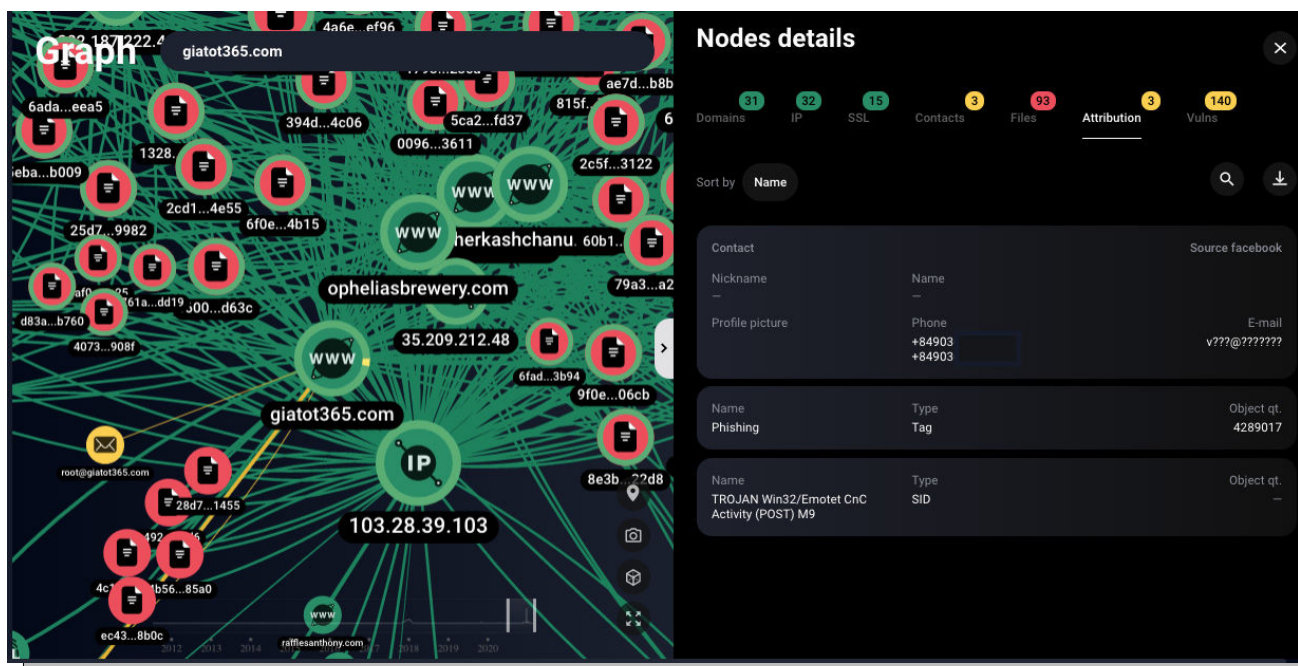


FIGURE 21 – THE DOMAIN GIATOT365.COM IS ATTRIBUTED TO EMOTET, AND UNCOVERS PERSONS RELATED TO IT

Conclusion and verdict

Threat Hunting Framework is a rock-solid product rooted in Group-IB's abundant expertise. It is built around the classical incident handling workflow common in Community Emergency Response Team.

It is simple to use and usable to SOC analysts of all levels and CISOs, who can get summary reports and statistics illustrating the secure level of their infrastructure.

After the installation of THF Huntpoint and THF Sensor modules, you get all of the tools for threat hunting in your organization out of the box. In most cases, fast triage can be done without leaving THF Huntbox.

Depending on your use case scenario, THF can eliminate the need for a full-fledged SIEM and replace its functionality because it is built around the same ideas.

THF has a very mild learning curve. After you get used to the query language and event fields, you can get creative in your threat hunting endeavors pretty quickly.

THF supports battle-tested tools like Yara and Suricata that make it compatible with most threat intelligence sources, and enables you to make custom detection rules. It is carefully designed to reduce the number of alerts and, consequently, analysts' fatigue. This can sometimes come at the cost of reducing some automatic detections on endpoints related to red teaming techniques.

THF is a valuable tool for analysts and incident responders. It cannot replace human experts, but it will find anomalies and correlate them over various layers so they don't have to do it manually. The lack

of skillful analysts can be mitigated by using the THF in collaboration with CERT-GIB or other manager security services providers that employ THF as a security platform.

Group-IB runs an open partnership program for MSSPs around the world to deliver cutting-edge security services throughout the world.

We can recommend Threat Hunting Framework because it delivers on the promise of working on various layers (network, email system, files, endpoints, cloud) and providing actionable analytics from incidents/events.

The incident management capabilities are accessible and will be enough for most organizations. Group-IB Threat Intelligence & Attribution will enhance the threat intelligence and hunting capabilities in every organization, enable fast triage or more in-depth analyses, will save time and reduce the need for the integration of additional feeds.



Acronis

www.acronis.com

All-in-One Cyber Protection

With solutions for service providers, businesses, and home users, Acronis Cyber Protection Solutions help lower risk by protecting all data, applications, and systems – wherever they are.

- ✓ Automate your backup and recovery processes
- ✓ Prevent cyberattacks with advanced anti-malware, ransomware protection, virus scanning, vulnerability assessments, patch management, and more
- ✓ Streamline your endpoint protection management

[Learn More](#)

Trusted cybersecurity and the best
backup for complete cyber protection

AVTEST
The Independent IT Security Institute
Recognized Partner

VirusTotal

VB 100
VIRUS
BULLETIN

MRG Effitas
EFFICACY ASSESSMENT & ASSURANCE

ICSA labs

NioGuard
Security Lab





Navigating the waters of maritime cybersecurity

Brian Satira

Chief Hacking Officer, Redoubt Research

In January 2021, new International Maritime Organization (IMO) guidelines on maritime cyber risk management went into effect. Around the same time, the U.S. government released a first of its kind National Maritime Cyber Security Plan (NMCP), accompanying recent maritime cyber security directives from the U.S. Coast Guard.

For infosec professionals in sectors with a long history of cyber security governance, this may not seem earth-shattering news. But these measures are milestone developments in maritime cybersecurity.

Sea change in awareness

On June 16th 2017, the Maritime Safety Committee (MSC) of the United Nations' International Maritime

Organization (IMO) adopted a brief but significant resolution, MSC.428(98), “to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks”. The IMO committee had already approved an unreleased draft of guidelines for cyber risk management, MSC-FAL.1/Circ.3.

By the time those guidelines were published a few weeks later, the world’s largest integrated shipping and container logistics company, Maersk, had been devastated by a massive cyber attack. On June 27th, 2017, in ports around the globe, the company’s operations ground to a halt as the NotPetya malware ravaged IT systems. The fact that Maersk would later be assessed as “collateral damage”, rather than an intended target of the cyber-attacks, merely underscored how vulnerable and unprepared the maritime sector was.

The IMO resolution is referred to as “IMO 2021”, as it called for an implementation period that would expire on January 1st, 2021. Four years later, what progress has been made towards the goals of IMO 2021, and what challenges remain in maritime cyber security?

Dr. Gary C. Kessler, an independent consultant and practitioner in the areas of maritime cybersecurity, as well as the author of *Maritime Cybersecurity: A Guide for Leaders and Managers*, noted that PNT (position, navigation, timing) issues were just starting to become publicized in 2016, and that CEOs of maritime companies and ports did not look at cyberattacks as an existential threat. “The industry was just starting to talk about these problems five years ago, but it was far from mainstream.”

But now he told me that, in his opinion, the industry has reached a point of fully understanding that cyber is a major threat. “You can hardly have a meeting related to any aspect of the MTS without

some discussion of cybersecurity... IMO 2021 certainly was a wake-up call for the industry. More organizations and agencies have cyber plans.”

With respect to raising awareness on cyber risk, IMO 2021 seems to have been a success, though Maersk’s NotPetya nightmare may deserve some of the credit.

Standards, frameworks and guidelines, *al dente*?

In addition to creating awareness, IMO 2021 called for more detailed guidelines from maritime NGOs and [IMO] member governments. A profusion of new guidelines poured forth from an alphabet soup of organizations, including the:

- Baltic and International Maritime Council (BIMCO)
- Comité International Radio-Maritime (CIRM)
- Cruise Line International Association (CLIA)
- Digital Container Shipping Association (DCSA)
- International Chamber of Shipping (ICS)
- International Association of Dry Cargo Shipowners (INTERCARGO)
- International Association of Independent Tanker Owners (INTERTANKO)
- Oil Companies International Marine Forum (OCIMF)
- International Union of Marine Insurance (IUMI)

While this is better than not having any standards and guidelines, **Cris De Witt**, founder of operational technology cybersecurity company Cyber Mariner, described to me the resulting tangle as a kind of governance “spaghetti”. DeWitt, whose clients range from operators of offshore [oil and gas] to cruise ships and container vessels, thinks that “some of these standards organizations need to collaborate [so that] the end receiver of their dog food doesn’t have to comply with so many compliance regimes. It’s daunting what they have to do in this regard.”

In January, the U.S. government publicly announced its National Maritime Cybersecurity Plan (NMCP), which is divided into three parts:

1. Risks and Standards
2. Information and Intelligence Sharing
3. Create a Maritime Cyber Security Workforce

The Risk and Standards section addresses the issue of establishing guidelines for the sector in the U.S. It notes that “more than 20 Federal government organizations currently have a role in maritime security,” and that “common cybersecurity standards however, do not exist and are not consistent across Maritime Transportation Security Act (MTSA) and non-MTSA regulated facilities.”

Yet, after acknowledging the dilemmas created by bureaucratic overlaps and the aforementioned guideline “spaghetti”, the NMCP proceeds to call for the creation of a new reporting guidance for maritime stakeholders, a new framework for port cybersecurity assessments, and a new U.S.-led international port OT risk framework.

These guidelines would be in addition to the directives issued by the United States Coast Guard over the past year: Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities (NVIC 01-20) and Vessel Cyber Risk Management Work Instruction (CVC-WI-027(2)).

DeWitt remains hopeful that technical - rather than bureaucratic - solutions may be found. “On the horizon are tools that possibly negate the policy spaghetti, and ‘map’ one compliance regime to another in a way the worker bee, the FSO, ETO, Captain, IT person... can reasonably and practically implement.”

Cliff Neve, COO at MAD Security and a retired U.S. Coast Guard officer with 26+ years of experience,

frames the governance discussion in a different, blunter perspective.

“NVIC 01-20 is a start, and it’s moving the needle a little bit in industry on the policy and exercise side. The problem is that it’s not prescriptive enough. The job aids say nothing about firewalls, vuln scans, log management, event correlation, or anything else that actually results in a secure operating environment,” he noted.

“It’s almost as though the powers that be think that the Russians, Chinese and other adversary nation states are going to be deterred because someone has a cyber annex in their Facility Security Plan. I see people updating their documents but not making their systems more secure.”

Now hiring...

Ultimately, progress hinges on workforce development. There simply aren’t enough skilled personnel who, like Neve or DeWitt, have the unique combination of expertise in both maritime OT and cyber security necessary to bring organizations into alignment with best practices.

Chris Carter, a cybersecurity professional at a port facility in the U.S. Pacific Northwest, says that in his experience, only about half of deep water NW ports have dedicated, in-house IT staff, and he estimates that perhaps only half of those have dedicated cybersecurity personnel. Furthermore, he explains, the problem can’t be solved through outsourcing to general IT services firms, because ports would have to rely on MSPs that may not be versed on the aspects of maritime / port cybersecurity.

Dr. Kessler, who taught in the U.S. Coast Guard Academy’s new “Cyber Systems” program during its inaugural semester in 2019, echoed the challenge of workforce development.

"We are still waiting for maritime academies to recognize cyber as necessary coursework... Academia needs to take a lead and the institutions teaching the next generation of professional mariners have to be out there in front," he noted.

The NMCP addresses maritime cybersecurity workforce development and sets three priorities for the U.S. government.

The first sets a goal of producing "cybersecurity specialists in port and vessel systems" and calls for "investment, common training, and a sustainable career path to develop and incentivize cyber professionals". The second requires the U.S. Navy, Coast Guard, and Department of Homeland Security (DHS) to "pursue and encourage cybersecurity personnel exchanges with industry and national laboratories, with an approach towards port and vessel cybersecurity research and application."

"Priority Action 3", however, acknowledges that in the short-term, "Federal maritime cybersecurity forces exist, but are not sufficiently staffed, resourced, and trained to monitor, protect, and mitigate cyber threats across the maritime Sector." The plan, therefore, directs the U.S. Coast Guard to fill the gap by deploying "field cyber protection teams to support federal maritime security coordination of MTSA-regulated facilities and aid in marine investigations, as required."

Cyber threat intelligence: A cart before a horse?

The topic of cyber threat intelligence (CTI) occupies roughly a third of the NMCP. It also generates a significant divergence of opinion among maritime cyber security experts.

Carter, who also serves on the Board of Directors for the Maritime Transportation System

The topic of cyber threat intelligence (CTI) occupies roughly a third of the NMCP. It also generates a significant divergence of opinion among maritime cyber security experts.

Information Sharing and Analysis Center (MTS-ISAC), says that relationships he has established with members of the MTS-ISAC community, along with the contacts he was able to establish at DEF CON Hack the Sea, have become invaluable, and that they are finding successes working with each other.

"We are now seeing localized information exchanges launch that feeds into the larger MTS-ISAC, which will only better protect the maritime sector. I have personally shared half-million elements over five years," he noted.

Dr. Kessler, on the other hand, says that there's a need for better and more uniform information sharing of cyber intelligence.

"The ISAC/ISAO model is wonderful if you're a member. In the late 1990s, the ISACs freely shared information. Today, the model is that you have to pay to be a member. I fully understand that the ISACs need to be funded but the entire maritime transportation system is at risk, and that includes small operators, small manufacturers, and so on," he added.

In a section on "Information and Intelligence Sharing", the NMCP recognizes that "organizations such as Information Sharing and Analysis Centers provide a pathway to share information across the private and public sector coordinating Councils." It also points out, however, that "multiple private sector entities claim to be the information-sharing clearinghouse for MTS stakeholders. Overlapping

membership across cybersecurity information sharing organizations creates barriers to efficiently inform MTS stakeholders of maritime cybersecurity best practices or threats.”

An additional consideration is that not all organizations in the sector are at a sufficient state of cybersecurity maturity to leverage access to CTI. Organizations that do not have adequate understanding of their environment or capabilities to monitor their network and respond to events when they are detected are unlikely to benefit from access to third-party intelligence products. Those limited resources may be better dedicated to basic cybersecurity hygiene and workforce development.

Organizations that do not have adequate understanding of their environment or capabilities to monitor their network and respond to events when they are detected are unlikely to benefit from access to third-party intelligence products.

Leadership

Four years after NotPetya struck Maersk, and the IMO adopted MSC.428(98), the single greatest challenge facing cybersecurity in the maritime industry seems to be best summarized as “leadership”.

“Policy and regulation are good but any company that is waiting to be forced into implementing strong cyber defenses by regulators, legislators, and insurers is not competently managing their company,” Dr. Kessler noted.

Cliff Neve remarked that the single biggest challenge that his clients (including maritime clients) face is lack of leadership involvement in cybersecurity risk management. “I will be crystal clear that the problem my clients face is never technical: it is always a leadership or political issue.”



helpnetsecurity.com

Defending against Windows RDP attacks

Mike Jumper

CEO, Glyptodon



In 2020, attacks against Windows Remote Desktop Protocol (RDP) grew by 768%, according to ESET. But this shouldn't come as a surprise, given the massive increase in the number of people working remotely during the pandemic.

With enterprises resorting to making RDP services publicly available, hackers have taken notice. Some distributed denial-of-service (DDoS) attacks are leveraging RDP servers to amplify their effect, and malware like Trickbot is employing scanners to identify vulnerable open RDP ports.

When it comes to remote access, RDP is functionally rich and very useful. It's not inherently dangerous, but given its complexity, ubiquity, and position within the operating system, RDP has a large attack surface. If publicly exposed, vulnerabilities that emerge may be exploitable by

hackers to cause serious damage to an enterprise.

RDP needs to be well protected, and direct access should never be provided to an RDP server. Instead, access should be guarded behind a separate service with limited privileges to prevent malicious actors from gaining admin-level access.

RDP needs to be well protected, and direct access should never be provided to an RDP server.

The problem with public RDP

By its own nature, an RDP service must run with enough privileges to operate a machine as another user, including the administrator. If a cybercriminal

takes advantage of a vulnerability in the service and can execute arbitrary code, their code will inherit those privileges.

Like any sufficiently complex software, RDP has suffered from vulnerabilities. Probably the best-known vulnerabilities to date appeared in 2019.

Better known as BlueKeep (CVE-2019-0708) and DejaBlue (CVE-2019-1181 and CVE-2019-1182), they enabled an attacker to cause and exploit heap corruption to bypass the authorization layer and execute code on the server.

Patches were quickly made available. But while applying patches addresses specific issues, the primary concern for enterprise IT should be protecting against the unknown. As new vulnerabilities emerge, patches are not always immediately available or immediately feasible to apply. The system must be designed to mitigate future vulnerabilities *by design*.

Defensive RDP design

When designing an RDP deployment, make sure to adhere to the following two principles that limit the extent to which an unknown vulnerability can be exploited:

1. Defense-in-depth: Security should rely on multiple independent layers of protective services, not a single point of failure.

2. Principle of least privilege: Services and users should be given only the privileges that are strictly needed. If possible, tasks should be divided among multiple services so that the scope of privileged services is reduced.

Authorization should be performed independently by other services, not by the RDP server alone. Access to RDP services should only be possible

after authentication and authorization has already been performed. Typically, this means RDP should be deployed behind a secure gateway that serves as *the only means of accessing the RDP service*. Once a user has authenticated, the gateway should provide access only to those assets that the user needs. Likewise, privileges granted to the gateway and other publicly accessible services should be strictly limited so a successful attack cannot directly result in gaining admin privileges.

Organizations sometimes deploy a virtual private network (VPN) to overcome this challenge, and while that may be an acceptable short-term fix to secure RDP, there are significant long-term drawbacks. Providing general access to the private network using a VPN opens more of the network than is strictly required, violating the principle of least privilege. VPNs also have a reputation for being cumbersome to manage and scale. Given that many currently remote employees will remain remote even once COVID-19 restrictions have been fully lifted, this kind of administrative complexity is unlikely to be sustainable.

With RDP behind a secure, dedicated gateway, the network firewall can be configured so that outside access is possible only through the gateway. Likewise, all machines on the network that enable RDP should be locked down so that they can only be accessed via the gateway, ensuring that unauthorized access to one machine does not imply access to all others on the network.

In our new, remote-work world, RDP will undoubtedly continue to play a key role in enabling remote access to enterprise machines, both virtual and physical. And through a few relatively simple measures — consistent patching, isolating RDP behind a secure gateway and following the principle of least privilege — organizations can provide remote access without fear of providing new vulnerabilities for hackers to exploit.

Security world

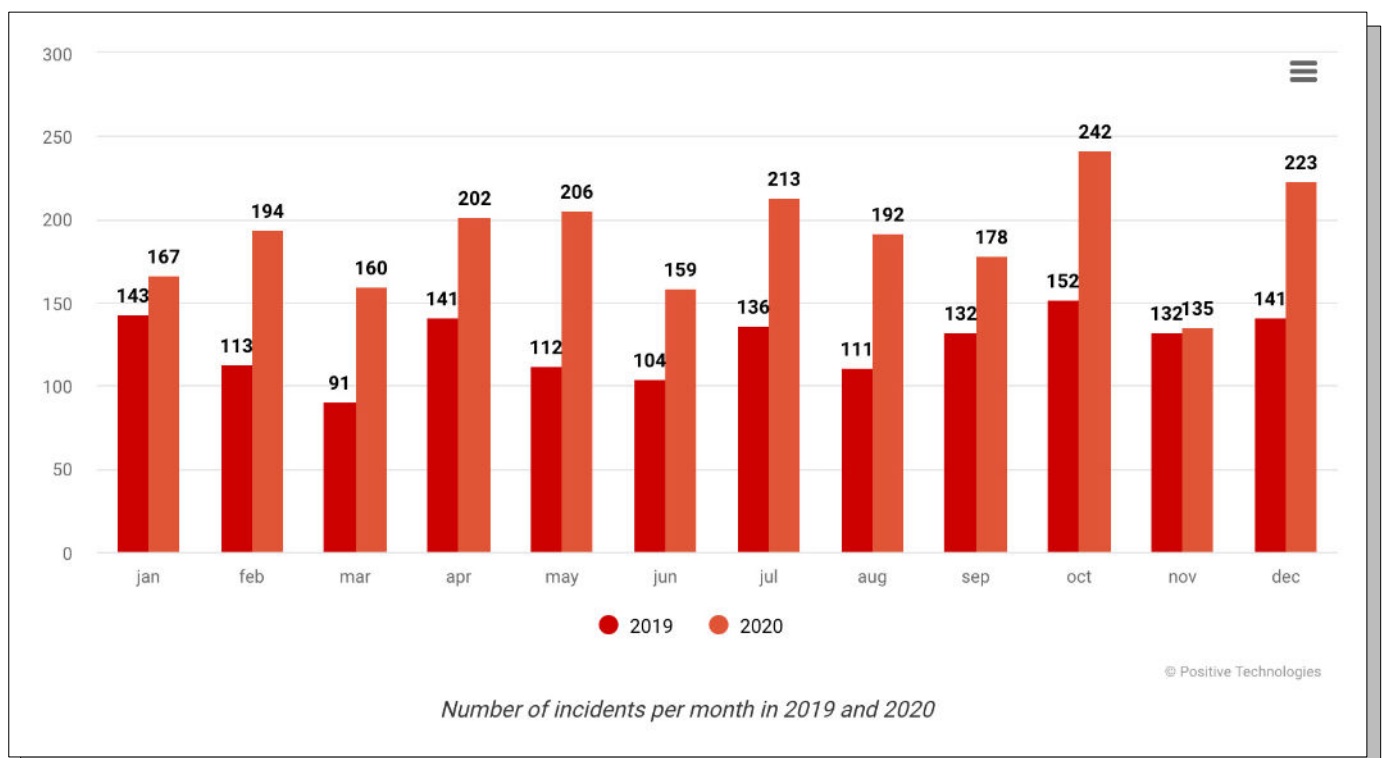
Malware-related attacks jump by 54%

Extensive analysis of cyberthreats in 2020 reveals a 91% jump in attacks on industrial companies and a 54% rise in malware-related attacks compared to 2019. Medical institutions ranked first in ransomware attacks, Positive Technologies reports.

The total number of incidents grew by 51% compared to 2019. Seven out of 10 attacks were targeted. The most popular targets were

government institutions (19%), industrial companies (12%) and medical institutions (9%).

In most cases, industrial companies were attacked by ransomware variants such as RansomExx, Netwalker, Clop, Maze, Ragnar Locker, LockBit, DoppelPaymer, and Snake (which deletes shadow copies before starting the encryption process, and has the ability to stop ICS-related processes).



Cyberattacks target the anywhere workforce, legacy security systems can't provide protection

VMware released a report based on an online survey of 3,542 CIOs, CTOs and CISOs in December 2020 from across the globe. The report explores the impact of cyberattacks and breaches on organizations and details how security teams are adapting to these challenges.

Close to 80 percent of organizations surveyed experienced cyberattacks due to more employees working from home, highlighting the vulnerabilities in legacy security technology and postures.

"The race to adopt cloud technology over the past year has created a once-in-a-generation chance for business leaders to rethink their approach to cybersecurity," said Rick McElroy, Principal Cybersecurity Strategist, VMware.

"Legacy security systems are no longer sufficient, organizations need protection that extends beyond endpoints to workloads to better secure data and applications. As attacker sophistication and security threats become more prevalent than ever, it's time to empower defenders to detect and stop attacks and implement security stacks built for a cloud-first world."

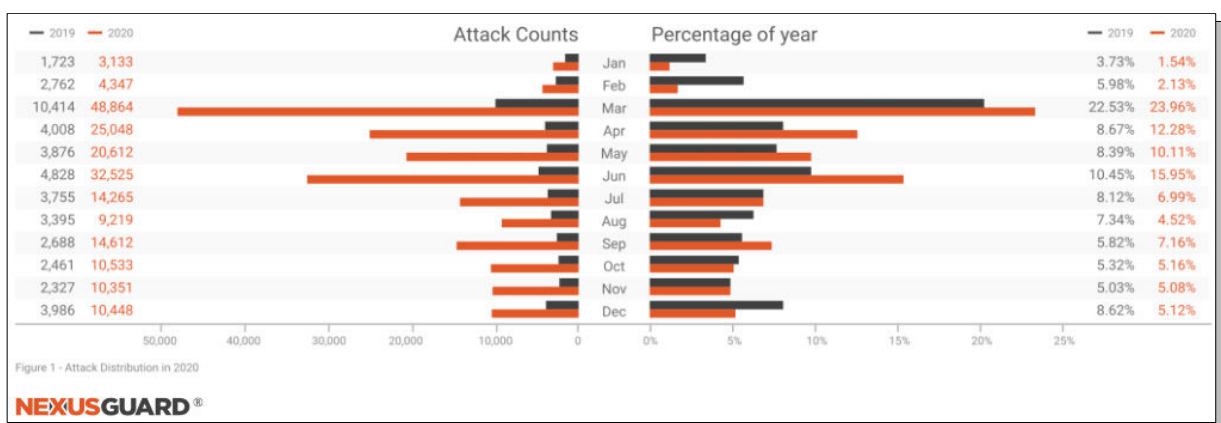
DDoS attacks increase 341% amid pandemic

During the pandemic, cyber attackers targeted industries providing connectivity, services and entertainment to populations forced to shelter-in-place, resulting in a 341% year-over-year increase in distributed denial-of-service (DDoS) attacks, according to Nexusguard.

The massive shift in online behavior and reliance

on connectivity strained communications service providers (CSPs) and internet service providers (ISPs) that provided the backbone for this remote work, including spikes in ransom DDoS (RDDoS) attacks to extort organizations for payment in exchange for staying online.

With lockdown and social distancing measures enforced across the world, 2020 saw an explosion in online gaming and dependence on the internet, which were attractive targets for attackers. Motivations for the attacks ranged from financial gains, political and economic benefits, revenge, cyberwarfare to even personal enjoyment.



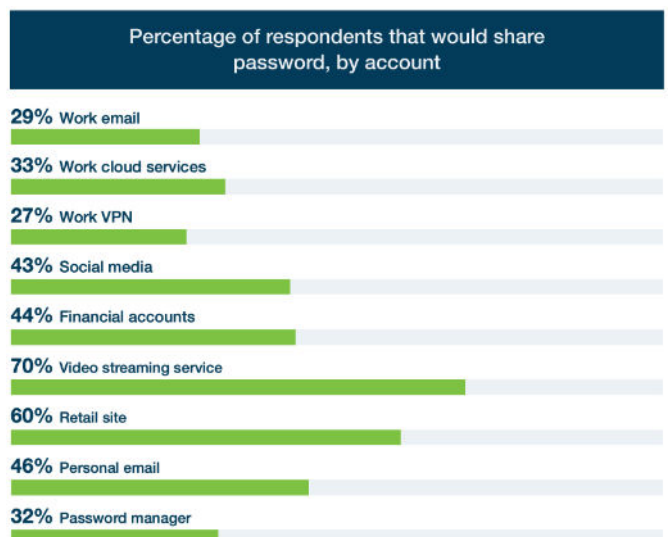
54% of all employees reuse passwords across multiple work accounts

Yubico released the results of a study into current attitudes and adaptability to at-home corporate cybersecurity, employee training, and support in the current global hybrid working era. The report surveyed 3,006 employees, business owners, and C-suite executives at large organisations (250+ employees), who have worked from home and use work issued devices in the UK, France and Germany.

Data shows that since the start of the pandemic employees have been engaging in poor cybersecurity practices on work-issued devices, with business owners and C-level executives proving to be the worst culprits. At the same time, enterprises are falling short on cybersecurity best practices that need to be implemented for out-of-office environments.

Less than a quarter of respondents admit to even implementing 2FA since the start of the pandemic and even then, many are using less secure and less user-friendly forms of 2FA like mobile authentication apps and SMS one-time passcodes.

“The research shows that many organizations are still finding their feet in these new, mostly virtual, work environments, and while this flexibility can deliver new opportunities for businesses and employees, they shouldn’t ignore the growing cybersecurity risks that come with it,” said Stina Ehrensvärd, CEO, Yubico.



Data privacy management software market to grow steadily

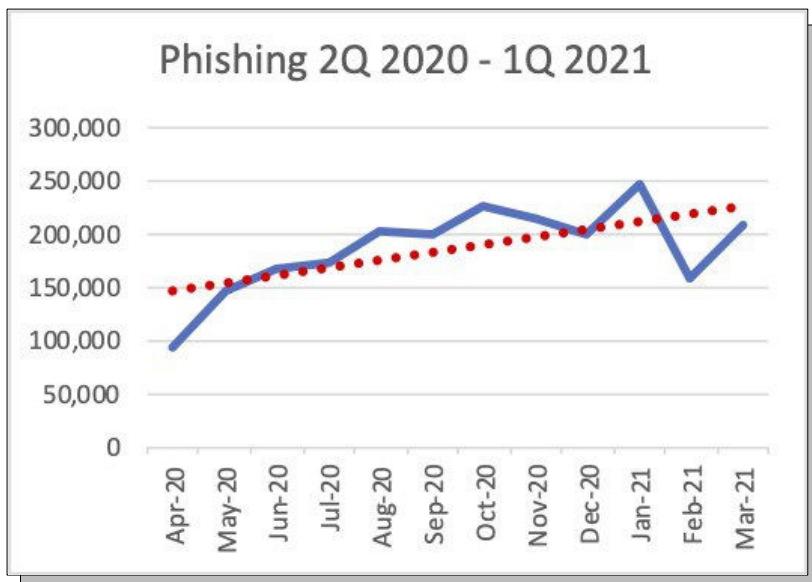
The data privacy management software market saw soaring growth in 2020 with worldwide revenues up 46.1% year over year.

IDC expects this growth to continue over the next

several years, driven by the further expansion of data privacy regulatory regimes worldwide. It is estimated that data privacy management software revenues will nearly double between 2020 and 2025, reaching nearly \$2.3 billion in 2025 with a five-year CAGR of 14.3%.

“It feels like a broken record when discussing data privacy regulations because every year data privacy regimes continue to grow in jurisdictions around the globe. But as repetitive as it can be, it is still the truth,” said Ryan O’Leary, research manager, Privacy and Legal Technology at IDC.

Phishing maintained near-record levels in the first quarter of 2021



The APWG's new Phishing Activity Trends Report reveals that phishing maintained near-record levels in the first quarter of 2021, after landmark increases of 2020 in which reported phishing websites doubled.

The number of reported phishing websites peaked in January 2021 with an all-time high of 245,771 before declining later in the quarter. Still, March suffered more than 200,00 such attacks, the fourth-worst month in APWG's reporting history.

"The APWG's members are reporting more confirmed phishing attacks," said Greg Aaron, Senior Research Fellow at the APWG. "There are, however, many more attacks that are not reported in our data repository. That means these numbers are the floor, and that the situation out on the Internet is worse than the mounting numbers indicate."

Higher encryption adoption driven by rising data breach threats

Security and IT professionals in the Middle East are demonstrating a rising desire to secure critical applications and data, driving higher encryption adoption for newer use cases like containers and IoT platforms, as well as for email and private cloud infrastructures.

This and other findings are highlighted in the Entrust study, a multinational survey by the Ponemon Institute. The study reports on the cybersecurity challenges organizations face today, and how and why organizations deploy encryption.

According to respondents from the region, the most important feature associated with encryption solutions is support for cloud and on-premises deployment. The adoption of encryption for private cloud infrastructure is up 8% over the past two years and Bring Your Own Key (BYOK) management support was cited an important feature of cloud encryption solutions by 42% (vs. 34% globally), making this the 4th straight year that this was above the global average.

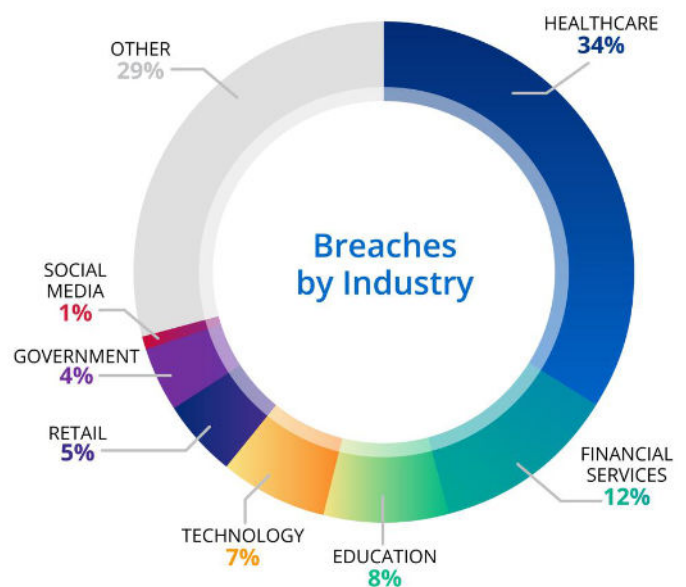
Unauthorized access accounts for 43% of all breaches globally

There has been a 450% surge in breaches containing usernames and passwords globally, according to a ForgeRock report. Researchers also found unauthorized access was the leading cause of breaches for the third consecutive year, increasing year-over-year for the past two years, accounting for 43% of all breaches in 2020.

Questionable yet common security practices, like sharing or reusing passwords, gave bad actors an easy path to gaining access to personally identifiable information (PII), such as date of birth and Social Security Number information, which is found in one-third of all breaches.

"For too long, usernames and passwords have been the backbone of providing people secure access to their digital lives. The findings in our identity breach report reveal that it's time for change," said Fran Rosch, CEO, ForgeRock.

"The surge in breaches involving usernames and passwords at an astounding 450% clearly emphasizes the need to adopt a strong digital identity and access management solution that offers the ability to go passwordless. It also gives companies a much better chance at reducing data exposure, as well as lowering their reputational and financial risk."



Operation HAECHI-I intercepts \$83M in online financial crimes

Amid an exponential increase in online fraud, an INTERPOL-coordinated operation codenamed HAECHI-I mobilized more than 40 specialized law enforcement officers across the Asia Pacific region.

Over six months of coordinated intelligence collection and joint operations, police were able to intercept a total of \$83 million in illicit funds transferred from victims to the perpetrators of cyber-enabled financial crime.

The operation focused particularly on five types of online financial crime: investment fraud, romance scams, money laundering associated with illegal online gambling, online sextortion and voice phishing.

Biometrics for banking and financial services market to reach \$8.9 billion by 2026

The turn of next decade is expected to be more challenging for banks and financial institutions as security breaches become more sophisticated with technology advancements.

Money laundering has become more widespread representing about 2%-5% of global GDP. One of the measures being actively pursued by banks is biometrics, since the technology assists in the creation of secure banking environment by

reducing instances of identity fraud, establishing audit trail of transactions, and protecting financial data.

The shift towards biometrics is also being driven by the inability of traditional security measures such as PINs, passwords and tokens to effectively offer protection, particularly against the growing sophistication of intruder attacks.

Business leaders now feel more vulnerable to cyber attacks

45% of business leaders claim that their company has experienced more network security incidents as a result of the pandemic, according to a new survey from Telia Carrier.

Geographically speaking, 55% of US and 49% of UK respondents have experienced the most severe impact to their network security due to these attacks (suggesting that their businesses are more of a target than those in continental Europe) which, in turn, has resulted in a clear majority of respondents (60%) increasing their investment in this area.

COVID-19 has also had an impact on the sense of vulnerability among business leaders, with 51% of them feeling more vulnerable to cyber attacks since the pandemic. In keeping with the other trends identified, the US and UK again appear to feel the most vulnerable.

Remote working security concerns still lingering

Despite being over a year into remote working and looking ahead to likely shifts to hybrid remote/in-office working models, 82% of businesses still remain concerned about the security risks of employees working remotely.

This is just one of the key insights from a study conducted by 451 Research, which reveals that managing security risks is undoubtedly getting more challenging, with 47% of businesses seeing an increase in the volume, severity, and/or scope of cyber-attacks in the past 12 months.

Globally, malware (54%) is the leading source of security attacks, followed by ransomware (48%), and phishing (41%). Yet, when it comes to how attacks occur, the message is clear: internal threats and human error are still of great concern to industry. A third of businesses stated that malicious insiders (35%) and human error (31%) are the greatest risks to them, followed by external attackers (22%).



Ask anyone who has been around the cybersecurity world long enough and they'll tell you just how much evolution the industry has undergone in the past few decades—particularly from the perspective and position of the Chief Information Security officer (CISO).

The role of CISO first emerged as organizations embraced digital revolutions and began relying on new data streams to help inform business decisions. As technology continued to advance and became more complex, so too did threat actors who saw new opportunities to disrupt businesses, by stealing or holding that data hostage for ransom.

As the years have gone by and cyberattacks have become more sophisticated, the role of the CISO

The evolution of the modern CISO

Heather Gantt-Evans

CISO, SailPoint

has had to advance. The CISO has evolved from being the steward of data to also being a guardian for availability with the emergence of more destructive and disruptive attacks. The CISO also must be highly adaptable and serve as the connective tissue between security, privacy and ultimately, consumer trust.

The changing threat landscape

Some of the latest and most consequential cyberattacks, such as the SolarWinds hack and those against the European medical agencies, Facebook and most recently the Colonial Pipeline have presented a critical question to many leaders that is yet to be answered – “What does it take to be a CISO in today’s threat-riddled economic landscape?”

Answering this question is a lot more complex than it was even just a year ago. While it’s true that cybercriminals were modernizing their strategies before 2020, the pandemic opened numerous new pathways to spread malware. As work-from-home mandates forced millions around the globe to remain remote, nearly overnight, IT departments were stretched thin trying to ensure connectivity to networks. In parallel, this proved to be a gleaming opportunity for cybercriminals to pounce on nearly every industry, flooding them with cyberattacks.

Given the fluid complexities brought on by COVID-19—including remote work and rapidly-accelerated digital transformation plans—the attack surface for cybercriminals nearly doubled as employees began conducting work from home on potentially unsecured home Wi-Fi networks and personal devices. In fact, nearly 50% of people working from home have fallen for phishing scams since the pandemic began.

As threat levels continue to rise, we’ve seen a plethora of new attack styles unfold. From double

extortion in ransomware and complex supply chain attacks, to a greater willingness among threat actors to collaborate and conduct more damaging and aggressive attacks.

As threat levels continue to rise, we’ve seen a plethora of new attack styles unfold.

For CISOs, this vast attack surface means their jurisdiction is no longer confined to company offices, and they now must think about cybersecurity in much broader strokes. The focus of the CISO in 2021 and beyond must consider securing cloud, IoT, WFH, BYOD, and so much more as technology continues to shift and grow.

Adaptability is key

With remote work primed to remain a mainstay in societal patterns, and growing interest in a “work from anywhere” mentality continues, the onus to be adaptable has never been higher for CISOs.

For CISOs, there’s a fine balance between continuing to make progress on strategic initiatives that will reduce risk and improve security maturity, while also being adaptable enough to stop and pivot as needed.

For CISOs, there’s a fine balance between continuing to make progress on strategic initiatives that will reduce risk and improve security maturity, while also being adaptable enough to stop and pivot as needed. Further, as businesses adapt to meet the growing needs of the customer, the business needs to do so with CISOs in mind in order to stop and ask the right questions to enable secure-from-the-start—such as, “Will this new technology we’re onboarding potentially open up

new security gaps?” or “Does branching into new sectors open our business up to new areas of attack?” and “Could we expose our customer base to threats by switching CRM platforms?”

To be able to answer these questions, CISOs need to be able to adapt across three major areas that are constantly shifting and inherently intertwined: the needs of the business and customer, the current threat landscape, and risk calculation and prioritization. For example, many CISOs are certainly taking heed from the SolarWinds attacks to ensure proper risk prioritization around product security.

Where we go from here

For today's CISOs, the key is to continue leading with the same level of diligence as they are right now, never letting their foot off the gas—because those looming in the shadows of the dark web certainly aren't slowing down. There is no going “back to normal” for cybercriminals who have gotten a taste of how much damage and chaos they're able to create. As CISOs look ahead, they must begin planning their identity-defined security strategy now – as the traditional perimeter security approach is no longer sufficient to defend against the threat landscape. As a result, emerging best

practices have developed, such as zero trust and other strategies recently released by NSA.

Businesses must consider their approach to cybersecurity and take actionable steps toward implementing a “cyber resilience” framework.

Businesses must consider their approach to cybersecurity and take actionable steps toward implementing a “cyber resilience” framework. From there, executive leadership, business continuity, crisis management, disaster recovery, cybersecurity, legal and communications, should be prepared from a worst-case scenarios perspective, ensuring proactive preparedness around the coordination and communications required for a business to successfully respond to a cyber attack.

CISOs also need to embrace information sharing and collaboration in order to take their organizations from being one step behind cybercriminals to being two steps ahead at all times.

+ HELPNETSECURITY



Ransomware attribution: Missing the true perpetrator?

Historical focus solely on attribution has made way for consideration of the human and financial toll that ransomware can have, not only to an organization but also to wider society.

Raj Samani | Chief Scientist, McAfee





Understanding the cloud shared responsibility model

Ameesh Divatia

CEO, Baffle

Over the past year, we witnessed an unprecedented transition to the cloud as companies had to quickly adjust to the almost instantaneous move to a remote work environment. But in many cases, they prioritized practicality over security to avoid business disruption, leaving many organizations vulnerable.

A significant reason for these vulnerabilities is that many organizations rely on default security offerings from their cloud providers, which are often provided as do-it-yourself toolkits and guidelines, leaving the actual configuration to the user.

In a cloud-first environment, organizations now operate under a shared responsibility model with

While the concept of a shared responsibility model is relatively easy to understand, implementing it requires a great deal of coordination.

cloud providers, which lays out what responsibilities belong to the cloud provider and what responsibilities belong to the user. While the concept of a shared responsibility model is relatively easy to understand, implementing it requires a great deal of coordination.

In many instances, a shared responsibility model dictates that cloud providers are responsible for the security “of” the cloud, and organizations are responsible for security “in” the cloud.

The differentiation can be a little confusing. Think of it this way: A home security provider can install a protection system, but it is up to the homeowner to identify where the sensors are located and ensure that it is armed before leaving the house. Similarly, a cloud provider protects the cloud’s infrastructure to reduce intrusion risk, while the organization protects the data if a breach occurs.

The challenge grows more complex when you consider that most organizations are working in multiple cloud environments. According to Accenture, 93% of organizations are operating with a multi-cloud strategy, utilizing an average of 3.4 public clouds and 3.9 private clouds per organization.

A cloud provider protects the cloud’s infrastructure to reduce intrusion risk, while the organization protects the data if a breach occurs.

Not only are companies constantly analyzing and assessing their own security posture, but they must also do the same for their cloud providers.

As companies rely more heavily than ever on the cloud, organizations must create an environment that addresses their responsibilities under a shared responsibility model. The following steps can help prepare organizations to protect their data at all times:

Identify sensitive data

Use advanced data discovery methods to find sensitive data in their repositories before moving them to the cloud.

Privacy regulations must be top of mind due to the rapidly expanding scope of what is considered sensitive. For example, IP addresses and geolocation information are now regarded as sensitive in addition to personally identifiable information (PII) such as Social Security numbers and birth dates.

Like any service, cloud service providers should have quantifiable evidence that demonstrates a commitment to cloud security.

Determine the usage of data

Identify the purpose of collecting data to comply with privacy regulations such as GDPR and CCPA. Next, they should map out how they will process the data and if they will need to share it with a third party. The critical element is to make sure that this data does not land into unauthorized hands, which can result in hefty fines.



BYOK enables encryption or tokenization of sensitive data records so that only the data owner has access to them.

Assign access control

Outline who is allowed to access that data for processing. Using dynamic masking tools, it is possible to create customized views for individuals based on their persona. For example, an application developer needs a different view than a data scientist who accesses the same dataset in the cloud.

Research the cloud provider's security qualifications

Like any service, cloud service providers should have quantifiable evidence that demonstrates a commitment to cloud security.

Conduct due diligence in researching their industry-specific, cloud security certifications, and if they publish regular reports associated with compliance and audits.

Cloud computing is an accepted reality of doing business.

Seek out advanced protection

Transitioning data repositories to the cloud brings many advantages in terms of scale and availability, but it does require giving up control of where the data resides.

Organizations should always be asking, "Can the cloud service provider see my data?" Or, more

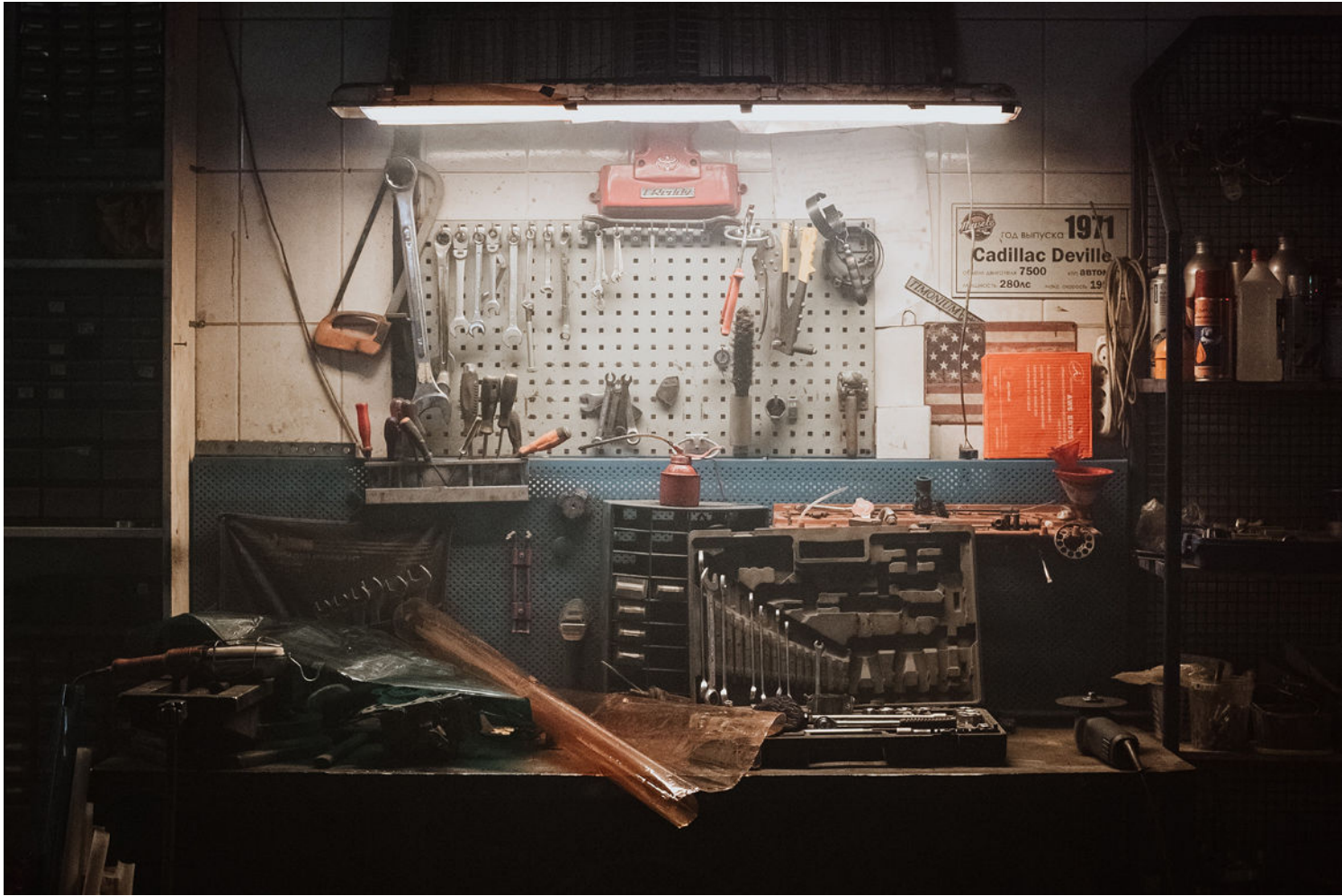
importantly, "Can someone impersonating my cloud service provider's administrator see my data?" Bring Your Own Key (BYOK) is an increasingly standard technology solution that helps organizations maintain control of their data on infrastructure that they do not own.

BYOK enables encryption or tokenization of sensitive data records so that only the data owner has access to them. These methods prevent the cloud service provider from ever being able to see the data. And if someone pretending to be the cloud service provider's administrator exfiltrates the data, all they will get is encrypted data, rendering the breach useless.

Traditional "at rest" encryption methods require data to be deposited in the cloud and in the clear before the protection kicks in. Adopt techniques where the data protection task is built into the data movement task, thus eliminating that vulnerability.

Cloud computing is an accepted reality of doing business. As such, understanding the shared responsibility model outlined by a cloud provider and taking the necessary steps to protect data throughout its lifecycle, in transit, at rest, and in use, should be top priorities before any cloud migration.

In doing so, organizations will reduce the risk of costly breaches and non-compliance, while unlocking the many benefits the cloud has to offer.



Why is patch management so difficult to master?

Juan Pablo Perez-Etchegoyen

CTO, Onapsis

This question has plagued IT and security departments for years. Each month these teams struggle to keep up with the number of patches issued by the myriad of vendors in their technology stack. And it's not a small problem. According to a Ponemon Institute report, more than 40% of IT and security workers indicated they suffered a data breach in the last two years due to unpatched vulnerabilities.

To get a better handle on the never-ending cascade of patches, let's first address some of the problems organizations face today.

Top patch management pitfalls

Each vendor, platform, and application has its own approach to patch management. For example,

when we look at SAP, their patches fall into two categories: automatic and manual.

Automatic patches don't require a system restart, which means IT teams can push patches into production without disrupting business operations. Manual patches, on the other hand, require a system restart. These patches are often tricky to implement and require IT teams to sync patching with maintenance windows, which could be weeks or even months away. These updates also need to be added to development, quality assurance and production environments, adding even more time for the patch. The problem? Hackers aren't waiting that long.

Automatic patches don't require a system restart, which means IT teams can push patches into production without disrupting business operations.

A recent study showed that some hackers are attacking vulnerable platforms within 72 hours of an issued patch. IT teams need to move quickly, which brings up the next pitfall. A record labor shortage with skyrocketing unfilled security positions has left enterprises shorthanded. And while some mission-critical business applications have a dedicated team, like SAP and BASIS administrators, security procedures for many applications are left to general IT and security staff who are already spread thin.

With hundreds of patches coming in every month, some updates can fall through the cracks, be deprioritized, or left unassigned.

With hundreds of patches coming in every month, some updates can fall through the cracks, be deprioritized, or left unassigned. This is especially

true for teams using outdated methods to track patches like spreadsheets and email.

Five steps towards better patch management

How can teams keep up with this never-ending issue? Businesses need to take five critical steps to drive alignment and establish a well-oiled patch management process.

These steps include leveraging automation, streamlining workflows, adopting advanced analytics, and more. These processes can alleviate patch management pitfalls, support staff, and up-level an organization's overall security posture.

1. Understand the problem and achieve buy-in:

Patch management is a team program. IT and security teams need to chart a map highlighting the full scope of applications within their business, the criticality of each system, and who is managing each vendor's updates.

With tightening security budgets, it's essential to showcase the growing, complicated web of applications and patch management processes to leadership in order to achieve buy-in for financial allocation and staff resources to fix this very solvable problem.

2. Automate: To replace spreadsheets and manual tracking, businesses should consider investing in third-party solutions that automate the scanning of a company's entire application landscape. These offerings can aggregate unpatched vulnerabilities, highlight priority patches and chart a roadmap to a level of manageable risk. Smart companies will also consider adopting workflow offerings that integrate with automation solutions to help streamline the remediation process.

3. Implement compensating controls: Complete coverage and immediate response to security


patches are not always possible. That's why it's essential to implement compensating controls that can help organizations "buy time" while patch prioritization, implementation, and testing kick in. There are different types of compensating controls, but one of the most common ones is enabling real-time visibility to assess whether security vulnerabilities are being exploited or not.

Complete coverage and immediate response to security patches are not always possible.

4. Analyze key trends: With the support of automation, businesses can move beyond identification and remediation to focus on trend analysis. As critical patches are resolved, security teams can quickly generate reports that show leadership where their business stands regarding unpatched vulnerabilities. The team can then establish a risk baseline the company is comfortable moving forward.

5. Establish an ongoing process: Every company is different, and the patch management process will reflect these differences. Whether that's the number of tools they leverage, the level of risk they're willing to accept, and how they apply these patches. One thing that's the same across every company, patch management is an ongoing process. It's essential to develop a patch management workflow that works for your organization, stays up to date on Patch Tuesdays' news and never forgets older vulnerabilities.

Automation technology promises to help streamline the monotonous job of tracking and applying patches, so security teams can focus on managing edge cases and more advanced issues. With a never-ending influx of patches, these five steps can help enterprises chart a course to better patch management.



DISCOVER WHAT
MATTERS IN THE WORLD OF
INFORMATION SECURITY TODAY

 **HELPNETSECURITY**

helpnetsecurity.com

Preventing security issues from destroying the promise of IoT

Patrick MeLampy

Juniper Fellow, Juniper Networks

Internet of Things (IoT) devices fall into various categories. Some, such as those located in a hospital setting, are very sophisticated, with advanced operating systems and encryption and certificate capabilities built in. Other examples of note are Ring doorbells and Nest thermostats.

The promise of IoT, however, is that sensors will become much less expensive to integrate and maintain, and therefore they will become far more ubiquitous. As IoT devices become more numerous, less capable, and less personalized, they create a Pandora's box of security concerns. In industrial settings, where devices are everywhere, the prevailing belief for many years was that these IoT sensors would be on an air-gapped network, automatically countering many safety concerns. However, with all the data

collected now being directly forwarded to data scientist repositories in public clouds, this is no longer true.

The need for specialized routing

Industrial IoT (IIoT) sensors need specialized routing for many reasons. The primary reason is to provide security and segmentation across the WAN or public internet. Separating these devices from all other traffic is essential, as these devices may not be trusted - and to top it off, the information they are collecting may be proprietary. If these devices and the data they carry were left with the other general traffic traversing the network it could create additional security problems, as well as make it tougher to provide the specific security needed to protect this type of traffic. Other reasons



IoT sensors need specialized routing include traffic engineering, path redundancy and load balancing - all critical aspects to managing the effectiveness, efficiency, and uptime of the network.

Many industrial applications combine sensors with process controls. In this case, the network with the largest number of sensors may also be used to control any critical processes. Separating, protecting, and guaranteeing process control traffic travelling on the same wires as the IoT traffic is essential. While the IoT traffic is typically data - which is important in its own right - the process control traffic is even more critical to maintaining operations. Separating them protects the ability of each to operate successfully and for a security issue on one not to necessarily affect both.

Isolating IP address requests

In addition, IoT devices often need IP addresses, and they often use Dynamic Host Configuration Protocol (DHCP) to obtain these. When there are large numbers of devices, it is essential that the edge routing equipment can isolate these requests, handle them locally and provide a secure source Network Address Translation (NAT) as required.

IoT devices may use Network Time Protocol (NTP), Domain Name Server (DNS) or other network services to obtain information. These must be guaranteed to be secure, while the protocols themselves are not. As such, providing local NTP or DNS secure relay services is essential. Providing localized DNS resolution for IoT endpoints may also be advantageous.

Router security

IoT devices will typically be the initiators of all communication. These same devices should be invisible to others and be unreachable by all. To do this, the router must be capable of understanding

the directionality of client/server communications, and then be able to enforce this.

IoT devices that are low-cost rarely can perform high-grade encryption. The routing equipment must be capable of authenticating and encrypting IoT flows between the sensors and the data centers they are connected to.

Full visibility is needed

Many IoT devices may need power from Ethernet switches. When managing these devices, it is very beneficial to have a single management/control plane for the Wi-Fi, wired, and secure edge routers. When an organization has full visibility into its operations through a single pane of glass, understanding the health of sensors is far easier.

Some IoT devices generate so much data that pre-processing the data is required prior to upload. In these cases, the smart edge routing device should be able to host or co-reside with containers for data processing applications.

Finally, most IoT devices will be connected to Wi-Fi networks. Having a tight integration with Wi-Fi networks is essential to ensure that security is maintained. Having Wi-Fi insights into IoT connectivity issues is essential in running a large network.

The promise of artificial intelligence (AI)

From finding bad cables, locating bad IoT sensors, diagnosing connectivity issues and more, AI can perform the same sequence of tasks as human operators, only much faster. When planning a large IoT network, consider learning about how AI can be applied to the network to help automate some of the maintenance, control and security needed to make the IoT strategy a successful one.

Industry news

Bayshore Networks expands its Security Gateway portfolio with the release of NetWall 10GB USG

NetWall 10BG USG for IT and OT is a high-speed hardware and software solution that creates a secure network segment when installed, shielding and isolating critical assets and sensitive networks from cyberattacks and misuse.

The entire NetWall family supports real-time file and data replication outside the electronic perimeter to corporate business systems such as ERP, MES, PLM, PIM and others. NetWall can securely transfer control systems data, logfiles, database records and other pertinent data to IT data centers, security operation centers (SOCs) and cloud-based data storage.



Qrypt Cloud Entropy Portal secures cryptography through the cloud

This virtual EaaS solution provides fast access to high-quality Quantum Random Number Generators (QRNG) hardware.

The Cloud Entropy Portal democratizes the availability of quantum safe random numbers for any application, especially cryptographic key generation.

Perfect randomness is essential for both classical and Post-Quantum Cryptography (PQC), which requires vastly larger key sizes – up to full one-time pad systems.

ReversingLabs Malware Lab: Detect, classify, analyze, and respond to malicious files

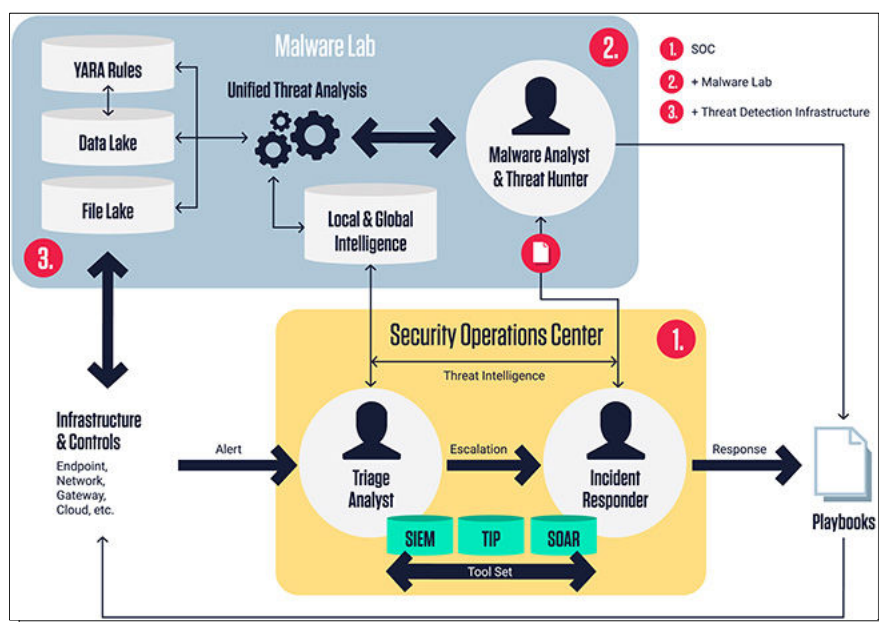
Designed to support modern security organizations increasingly delegating malware analysis to specific security operations (SOC) or development security operations (DevSecOps) experts, the ReversingLabs Malware Lab solution equips these teams with a unified threat analysis engine and console to rapidly detect, classify, analyze, and respond to malicious files and associated Indicators of Compromise (IOCs).

“Organizations are struggling to validate the effectiveness of their internal security controls and to respond to ever increasing quantities of actionable alerts. Homegrown and other complicated solutions have proven that responders are spending more time managing and integrating disparate technologies than addressing important alerts and incidents,” said Mario Vuksan, CEO at ReversingLabs. “At its heart, all SOC workflows, no matter how automated, require human analysis to provide context and inform their final decision. ReversingLabs Malware Lab is uniquely positioned as a commercial solution to give the highest quality of insight and decision

support. Moreover, it is easy to deploy and integrate, while providing the industry’s most advanced file analysis and indicator enrichment across a wide span of threat vectors.”

Despite advances in layered security approaches, organizations are still struggling to sort through fragmented event data to achieve complete risk assessment and visibility. Organizations are transitioning their security programs to get more clarity in the face of a rapidly evolving threat landscape by establishing a malware analysis service. Such services centralize the analysis of suspected threats and the investigation of malware.

As a result, all alerts can be addressed and more proactive postures can be delivered within their defenses. In fact, a recent ReversingLabs survey of information security professionals reveals that nearly 40 percent of respondents agreed that their organization could improve security with a more formalized threat hunting and malware lab program.



Protegrity Data Protection Platform introduces dynamic data masking and monitoring capabilities

Version 8.1 of Protegrity's platform introduces dynamic data masking and monitoring capabilities, providing customers with multiple data-protection methods all within a single data store.

The company also introduced: enhanced support for language-preserving Unicode tokenization; the Protegrity Cloud API, which allows businesses to easily embed data-protection capabilities into cloud ETL workflows; and a redesigned logging architecture to provide more granular auditability

over data-privacy initiatives.

"Companies need to use their data to drive innovation yet keeping data secure often delays access, which can significantly impact mission-critical AI, ML, and analytics initiatives," said Rick Farnell, President and CEO of Protegrity. "Our latest platform innovations provide expanded choice and control over data-protection methods – effectively expanding the tools available to safeguard data in a way that accelerates innovation."

RSA introduces Outseer, a spinout of its Fraud & Risk Intelligence unit

RSA Security announced the transition of its Fraud & Risk Intelligence business into a new standalone company serving a worldwide customer and partner community.

The new organization, Outseer, is led by CEO Reed Taussig who joined the RSA Fraud & Risk Intelligence business in late 2020 and is a veteran of the fraud prevention and digital identity industry.

Satori selected as finalist for RSA Conference 2021 Innovation Sandbox

Satori, a DataSecOps company revolutionizing data access, security and privacy for the modern data infrastructure, has been named one of 10 finalists for the RSA Conference 2021 Innovation Sandbox Contest for its work democratizing and protecting sensitive data in the cloud using a SaaS-based transparent setup.

Since 2005, the RSAC Innovation Sandbox has served as a platform for the boldest young cybersecurity companies to showcase their groundbreaking technologies and compete for the title of "Most Innovative Startup." The competition is widely recognized as a catapult for success, as the top 10 finalists have collectively seen over 50 acquisitions and \$8.2 billion in funding since the start of the contest. Satori will have three minutes to pitch the panel of judges before a question-and-answer round.

Waterfall Security Solution enhances support for OSIsoft PI

Waterfall Security Solutions, the global leader in OT security, announced an upgraded version of the OSIsoft PI connector for Waterfall's Unidirectional Security Gateway product line.

The continued increase in cyber attacks, a trend accelerated by the global COVID-19 pandemic, is driving cybersecurity concerns in industrial enterprises. With OSIsoft PI servers most often at the heart of both IT/OT integration and IT/OT security efforts, the upgraded connector makes truly safe IT/OT integration even easier for PI users and administrators.

The completely rewritten and upgraded connector supports the latest versions of OSIsoft PI Server software, functions, and access libraries. The connector includes support for PI Asset Framework, PI collectives and PI identity authentication. Waterfall's unique and innovative features in the connector include database backfill, clustered high availability, unlimited point counts,

support for data and event synchronization, high throughput, and an easy-to-use web GUI for configuration, monitoring and troubleshooting.

Point synchronization and database aggregation, which are the most popular features for unidirectional PI Server replication, continue to be supported in the new release. Point synchronization pushes PI point and attribute changes automatically to enterprise replicas. Systematic point renaming eliminates name conflicts when combining many plants' PI Servers to an enterprise server.



Gigamon ThreatINSIGHT Guided-SaaS NDR improves SOC and incident response effectiveness

ThreatINSIGHT Guided-SaaS NDR, which redefines how SaaS-based security solutions are delivered,

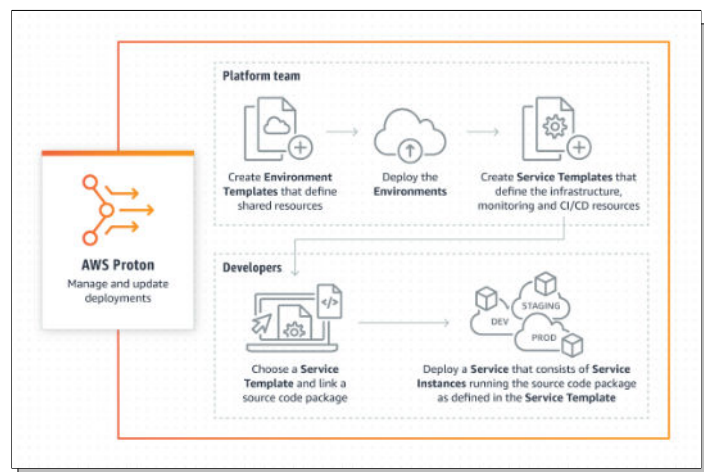
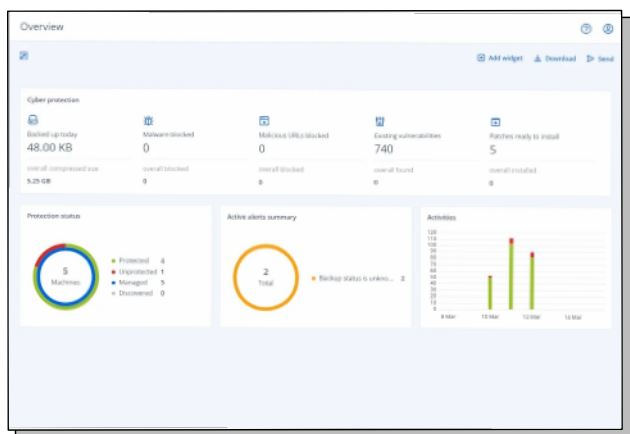
arrives at a critical juncture in threat defense as exponential growth in infrastructure complexity, and ever-increasing cyber threat activity, is negatively impacting InfoSec team's ability to efficiently do their jobs, ultimately contributing to high burnout rates.

ThreatINSIGHT alleviates the three most common problems that continue to plague SOC analysts and incident responders. They are often working in the dark without foundational visibility to observe adversary movement, leading 69% of IT and security practitioners to cite network visibility as the top reason for SOC ineffectiveness.

Acronis Cyber Protect Cloud's protection pack blocks email-borne threats

Acronis released a new advanced protection pack for Acronis Cyber Protect Cloud. Powered by the solution from Perception Point, the new Advanced Email Security pack enables service providers to enhance and extend their cybersecurity capabilities by detecting and stopping all email-borne cyberthreats before they can reach their clients' end users.

The native integration of Acronis Cyber Protect Cloud with Advanced Email Security means MSPs can use one solution to extend their cyber protection services to protect their clients' Microsoft 365, Google Workspace, Open-Xchange mailboxes, or on-premises mail server. Advanced Email Security intercepts all email-based threats, including spam, phishing and spoofing, business email compromises (BECs), advanced persistent threats (APTs), and even the zero-day malware attacks that are behind 80% of breaches.



AWS Proton: Fully managed application delivery service for containers and serverless

With AWS Proton, a customer's infrastructure team creates standard application stacks defining the architecture, infrastructure resources, CI/CD pipeline, and observability tools—and then makes these stacks available to their developers.

Developers can use AWS Proton's self-service interface to select an application stack for use with their code. AWS Proton automatically provisions the resources for the selected application stack, deploys the code, and sets up monitoring so developers can begin building serverless and container applications without having to learn, configure, or maintain the underlying resources.

There are no upfront commitments or fees to use AWS Proton, and customers pay only for the AWS services used to create, scale, and run their applications.

CyberArk Identity Security Platform enhancements secure risky access and broaden identity protection

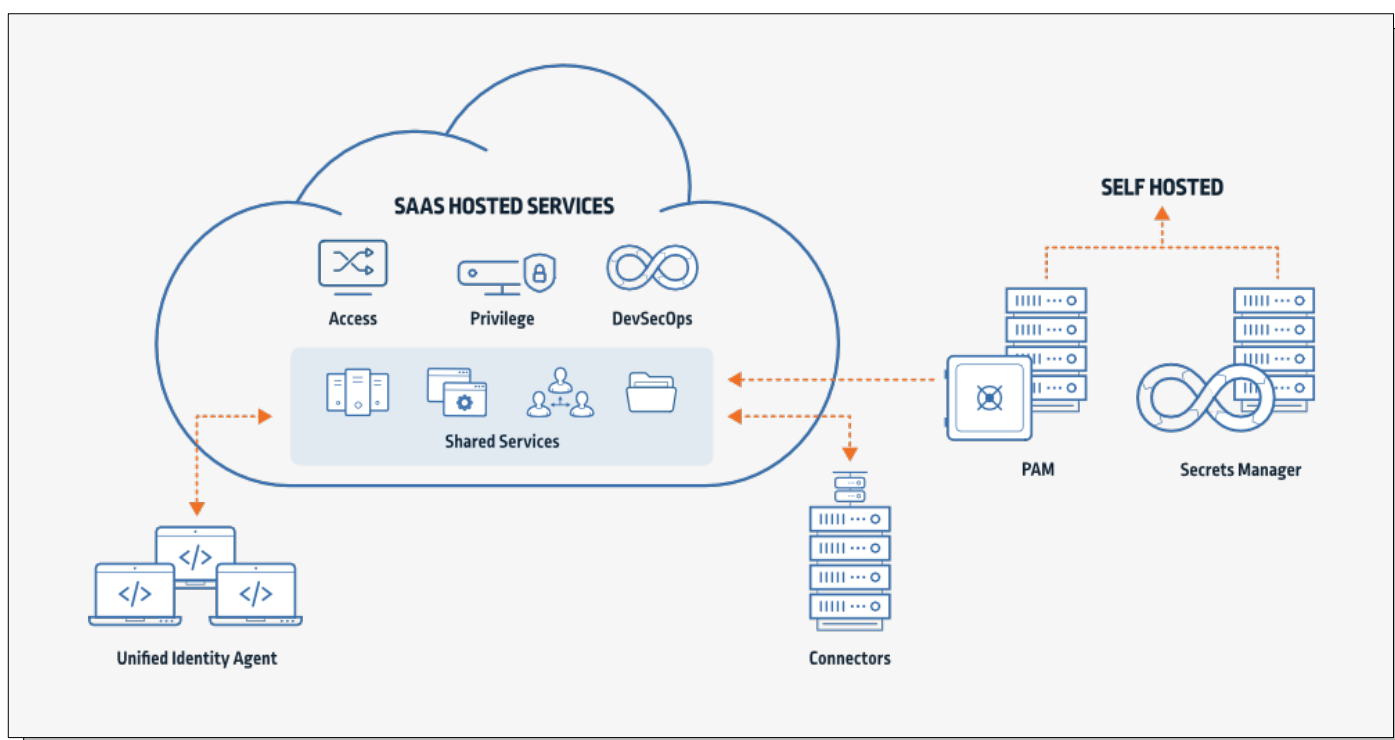
CyberArk announced major advancements to the CyberArk Identity Security Platform to help secure high-risk access and broaden protection across cloud and hybrid environments.

Global organizations of all sizes can benefit from CyberArk's set of cloud-delivered products and shared services to achieve a zero trust-based approach to protecting human and machine identities.

Centered on privileged access management, the CyberArk Identity Security Platform provides customers with a unified and holistic approach to securing access for any user, across any type of application or system, from anywhere, using any device.

"CyberArk is a critical component of our Identity and Access Management strategy, which enables us to deliver on our company's digital transformation goals," said Tony DeAngelo, assistant vice president, information security, Encova Insurance.

"And like many organizations, we're becoming more cloud-oriented, causing our CyberArk footprint to continue to grow and evolve as managing Identity Security and privileged access for our organization and partner organizations becomes even more vital," DeAngelo concluded.





Despite a positive (and significant) decrease from over 4 million unfilled cybersecurity jobs in 2019, there is still a staggering 3.12 million global shortage of workers with cybersecurity skills.

You may find this somewhat inevitable, given that IT innovation changes things so quickly and business will always, as a result, be playing catch up. However, I argue that we have the tools to tackle the gap and might have done so already were it not for our grave misunderstanding of the challenge.

Many thought leaders have approached the skills shortage from a cumulative perspective. They ask “How on Earth can companies afford to keep re-training their teams for the latest cyber-threats?”

Reformulating the cyber skills shortage

Aare Reintam

CTO, CybExer Technologies

The challenge, to them, emanates from the impracticalities of entry level training becoming obsolete as new challenges emerge.

Of course, the question of ongoing training is very important, but I believe it has misled us in our evaluation of the growing disparity between the supply and demand of cyber-professionals. What we should be asking is “How can we create a generation of cyber-professionals with improved digital skills and resilience to tackle an enemy that continually mutates?”

How can we create a generation of cyber-professionals with improved digital skills and resilience to tackle an enemy that continually mutates?

Defining the relationship between people and tech is of the utmost importance here. Cybersecurity is not merely a technical problem, it's a human problem. This is a critical intersection. People are not the weakest link in an effective cybersecurity defense strategy, but the most crucial. However, technology is the apparatus that can properly arm us with the skills to defend against attacks.

The silver bullet

The only thing we can be certain of is that cyberattacks are taking place right now and will continue to take place for the foreseeable future. As a result, cybersecurity will remain one of the most critical elements for maintaining operations in any organization.

There is a growing appetite for reform in cybersecurity training, particularly among higher education institutions (e.g., with the UK's top universities now offering National Cyber Security Centre (NCSC) certified Bachelor's and Master's

Programs). It is in the interest of the British government that this appetite continues to grow, as the Department for Culture, Media & Sport reported there were nearly 400,000 cybersecurity-related job postings from 2017-2020.

In addition, Covid-19 has been a significant catalyst in increasing uptake and emphasis on cyber skills since the steep rise in the use of digital platforms in both our work and personal lives has expanded the surface area for attacks and created more vulnerability.

Overall, though, young people remain our best hope for tackling the global cyber skills gap, and only by presenting cybersecurity to them as a viable career option can we start to address it. This is the critical starting point.

Once we do this, the next important step is to give universities and schools the facilities to offer sophisticated cyber training.

Empowering the next generation

If we're being honest, professors and CTOs are often concerned with providing their students and employees with a theoretical understanding of cyber security; that is, what the motives behind attacks might be, the means they use to carry out attacks, and the potential losses involved. While this provides a great theoretical background for cyber-training and may encourage vigilance, it is not always helpful in practical terms.

Young people remain our best hope for tackling the global cyber skills gap, and only by presenting cybersecurity to them as a viable career option can we start to address it.



By encouraging young people to take up courses in computer science or cybersecurity, whilst also supporting their learning via military and enterprise-grade platforms, the next generation of professionals will be well equipped to enter the workforce. Giving young people access to the best resources in the field is the only way to ensure they will play an active part in closing the skills gap.

Cyber range technology enables the user - be that a university, business, or government - to generate a realistic, capable and credible virtual environment which requires trainees to respond to cyber-attack simulations in real-time.

The standardization of cyber training practices for teens right through to experienced consultants will empower workers of all calibers to take an active role in reformulating their own organizations' training strategy, strengthening it and enabling seamless integration between teams.

Cyber range technology has emerged as the frontrunner when it comes to inciting this kind of bottom-up stability in cyber security. Cyber range technology enables the user - be that a university, business, or government - to generate a realistic, capable and credible virtual environment which requires trainees to respond to cyber-attack simulations in real-time.

Within the simulated network, users learn to cope under high levels of stress, locating and exploiting vulnerabilities on various network systems. This helps them develop the skills to identify, monitor and resist cyber-attacks.

Cyber ranges can mimic your IT systems and provide sophisticated training in the form of task-driven Capture-The-Flag (CTFs), live-fire exercises,

or a combination of both (threat hunting). They are available in open-source, and can be deployed quickly through the cloud, making roll-out to anywhere in the world a smooth process.

Cyber ranges can mimic your IT systems and provide sophisticated training in the form of task-driven Capture-The-Flag (CTFs), live-fire exercises, or a combination of both (threat hunting).

This technology is already the gold standard for governments, but its real disruptive capability lies in its deployment to higher-education institutions and even high schools. Here, students can hone their skills and prepare for tackling real cyber-attacks.

Simplifying the problem

The key to solving the cyber skills gap lies in mobilizing the next generation of (already) tech-savvy young people, and simply shifting our focus towards helping them develop cyber-skills *before* they enter the workplace.

The key to solving the cyber skills gap lies in mobilizing the next generation of (already) tech-savvy young people.

By taking a two-pronged approach, and bringing together a change in focus, supported by the newest and most sophisticated technology on the market, we can start to implement a real, viable strategy for tackling this immense challenge - before it's too late.



Certified Information
Systems Security Professional

An (ISC)[®] Certification

YOUR SKILLS Have Never Been MORE IMPORTANT

The cyber world needs your expertise. But the security leaders of tomorrow require a broad set of skills that job experience alone does not arm you with.

The globally recognized Certified Information Systems Security Professional (CISSP) credential help you prepare for real-time incidents and stand out as the expert employers are looking for. Download the white paper to discover the 9 key characteristics of effective leaders in the field.

Are you ready to stand out as an expert?

GET YOUR COPY



CISSP tops "The Next Big Thing" list as the #1 certification survey respondents plan to earn in 2021.

Cybersecurity industry analysis: Another recurring vulnerability we must correct

Pieter Danhieux

Chairman/CEO, Secure Code Warrior

I have spent my career finding, fixing, discussing, and breaking down software vulnerabilities, one way or another. I know that when it comes to some common security bugs, despite being in our orbit since the 90s, they continue to plague our software and cause major problems, even though the (often simple) fix has been known for almost the same length of time. It truly feels like Groundhog Day, where we as an industry seem to do the same thing over and over and expect a different result.

There's another little problem, however. We're not getting realistic advice, nor the fastest solutions, to combat the non-stop onslaught that is the modern threat landscape. Of course, each breach is different in its own way and there are numerous attack vectors that can be exploited in

vulnerable software. Feasible generic advice will be limited, but the best practice approach is looking more flawed by the hour.

To this end, I do have to wonder why so much of the commentary and analysis around cybersecurity has omitted solutions that truly address the root cause of so many vulnerabilities: humans. Gartner's most recent Hype Cycle for Application Security report, and Forrester's The State of Application Security 2021 report - both bibles for security experts that undoubtedly help to shape their program and potential product adoption - are almost entirely tools-focused. A report by Aberdeen back in 2017 showed just how unruly the average security tech stack had become, with CISOs managing hundreds of products as part of their security strategies; four



years later, we're grappling with more risk, more vulnerabilities, and more additions to growing tech stack beasts.

Security tooling is a must-have, but we need to look wider and restore balance to the people component of security defense.

Automation is the future. Why should we care about the human element of cybersecurity?

Virtually everything in our lives is powered by software, and it's true that automation is replacing the human elements that were once present in so many industries.

Virtually everything in our lives is powered by software, and it's true that automation is replacing the human elements that were once present in so many industries. It's a sign of progress in a world digitizing at warp speed, with AI and machine learning hot topics keeping many organizations future-focused.

So why, then, would a human-focused approach to cybersecurity be anything other than an antiquated solution to a technologically advancing problem? The fact that billions of data records have been stolen in breaches in the past year, including the most recent Facebook breach affecting over half a billion accounts, should indicate that we're not doing enough (or taking the right approach) to make a serious counter-punch against threat actors.

Cybersecurity tooling is a much-needed component of cyber defense, and tools will always have a place. Analysts have been absolutely on point in recommending the latest tools in a risk mitigation approach for enterprises, and that will not change. However, with code quality (and, by definition, security) difficult to manage at the volume of code production, tools cannot do the job

alone. To date, there is no single tool that will:

- Scan for every vulnerability, in every language: framework
- Scan at speed
- Minimize the double-handling caused by false positives and negatives

Tools can be slow, cumbersome, and unwieldy. Above all, however, they only find problems - they don't fix them, or recommend solutions. The latter requires security experts, who are thin on the ground and overworked, wading through the trash to find treasure in endless penetration testing and scanning results.

The fact is, according to the IBM Cyber Security Intelligence Index Report, human error plays a role in 95% of all successful data breaches. Almost half of those directly relate to software vulnerabilities, many of which could be alleviated if there was stronger adherence to secure coding and awareness in the early stages of the SDLC. However, for this to happen, a sharper and more relevant focus on education for developers - in addition to making it intrinsic to their workflow - is key.

Whether we like it or not, humans are deeply ingrained in the software development process, and cybersecurity is overwhelmingly a human problem. Tools won't be a catch-all to correct a fundamental flaw in our approach, but they can play a key supporting role in reshaping human solutions.

What if we just built better tools (and lots of them)?

Security tooling is improving all the time. SAST/DAST/IAST tools have come a long way, improving in speed and intelligence, and RASP should be a serious defensive consideration in many application environments. Firewalls, secrets managers, cloud and network security

applications: all no-brainers.

Humans can always strive to make better tools, but the innovation is not keeping up with the security and data protection needs of the digital world we live in.

Humans can always strive to make better tools, but the innovation is not keeping up with the security and data protection needs of the digital world we live in. Tools are, for the most part, built with robots in mind. They might be there to assist developers and the security team in scanning, monitoring, or protecting code, but interaction is very limited, and very few solutions aim to elevate security awareness or improve core skills that can lead to better security outcomes.

In fact, more than half of enterprises don't even know if the tools are working for them, nor are they confident that they could avoid a devastating data breach. That's a very poor sentiment, and in a tools-obsessed industry lacking support for a different approach, tends to solidify the status quo and the problems within.

How can an organization leverage a human-led approach to security?

There is no question that staying ahead of the trends in application security technology is beneficial and can even help prioritize upgrades or consolidations in a bloated tech stack. But to forgo targeting the root cause of vulnerable software - us humans - is going to keep us on the losing side of the cybersecurity battlefield.

If we want to get serious about decreasing the number of code-level security vulnerabilities, then developers need to be given the foundations to succeed in sharing responsibility for security. They need relevant, hands-on education and on-the-job

upskilling, and functional tooling that doesn't disrupt their workflow, or make security a chore to develop. Ideally, some tools would be developer-centric, built with their user experience front-of-mind.

If we want to get serious about decreasing the number of code-level security vulnerabilities, then developers need to be given the foundations to succeed in sharing responsibility for security.

To this day, no formal security certification program exists for developers, but every company can benefit from benchmarking and growing secure coding skills, killing common vulnerabilities early and often, and before that big tech stack has to lurch into action and slow everything down.

A team of security-aware developers is a hidden treasure for any organization, but like anything worth having, it will take time and effort to implement an effective dream team.

A team of security-aware developers is a hidden treasure for any organization.

Winning developers over to care about security and view secure coding as a foundation of code quality, takes an organization-wide commitment to put security first. And when entire teams are switched on to the positive impact they can play in eliminating common vulnerabilities as code is written, there isn't a tool on Earth that can compete.

For CISOs and artificial intelligence to evolve, trust is a must

Anne Hardy

CISO, Talend



Artificial intelligence (AI) is no longer the future - it is already in use in our homes, cars, and pockets. As AI continues to expand its role in our lives, an important question has emerged: What level of trust can—and should—we place in AI systems?

That is the very question that the European Union (EU) Commission has set out to answer with its newly proposed EU Artificial Intelligence Act. “On artificial intelligence, trust is a must, not a nice to have,” said Margrethe Vestager, the Executive Vice President of the European Commission for A Europe Fit for the Digital Age, in a press release. “With these landmark rules, the EU is spearheading the development of new global norms to make sure AI can be trusted.”

While we can all agree with Margrethe, the new regulation alone will not solve the problem. For any law to have absolute power and durability, it takes a team of trustworthy people to enforce the rules and drive greater technology awareness. Within organizations, leading the enforcement and education will ultimately fall onto the Chief Information Security Officer (CISO).

Traditionally, a CISO evaluates business opportunities against security risks that can potentially compromise long-term financial rewards. With the rise of new technology and its subsequent regulations, the role of the CISO is expanding to ensure company compliance with regulations like GDPR and education of employees

on personal data requirements to keep everyone safe.

Questioning the technology status quo

With concerns rising from consumers and citizens and the increasing need for more ethics and trust, we need to put limits to ensure sound and fair use of AI technologies. The new EU Artificial Intelligence Act is beneficial because it will dictate the rules and force companies to examine the societal implications of rapid technology adoption.

We must find a balance between technology benefits and risks. With the emergence of AI-enabled applications, traditional surveillance is transforming into smart video with new use cases that transcend what we consider surveillance today. Unfortunately, under the pretext of protection, camera operators risk exposing everyone within sight. We tend to overlook what data is collected or if it is secure for the greater good.

Any technology use and innovation must be transparent and explainable.

In 2020, amidst the Covid-19 disruption, France launched its contact tracing application, but its adoption was incredibly low because most citizens questioned the technology used and how the data was collected and stored. It forced the French government to rethink its approach and launch a new, "enriched" version of the application.

Stories like this one are not unique. Remember what happened when this novel coronavirus caused the UK government to eliminate teacher-predicted grades and switch to using an algorithm based on schools' past performance? Or the Apple Card, which favored men over women because of a lack of gender data?

We must take a 360° approach when using any

technology. To fully leverage AI, we need to look at the infrastructure in place, the algorithms involved, the quality of the data we have, who has access, and security protocols. The approach must include greater transparency on the data used and education for the people impacted by the technology. Whether the focus is new methods of working, new technologies, or some other type of change, the story is always the same. It takes time and effort but, in the end, building trust is the only way to launch and sustain a successful digital transformation.

CISOs at the crossroads

The role of the CISO is evolving at a fast pace. Regulations are constantly changing the way business is executed. Twenty years ago, the job was basically to manage the firewall and secure the perimeter. You didn't have to know much about what you were protecting if you knew which technology solutions would do the best job of keeping the bad guys out of your business.

The world today is drastically different. Digital technologies have infused every part of business and decision-making processes, raising the level of risk and, therefore, the importance of the CISO role. We see unexpected coupling, like CISO and Legal, because both positions intersect on data governance. The CISO supports business growth and ensures operations and data are secure using all technologies available at our fingertips.

The future CISO role will guide an organization through a rapid transformation and continuous marketplace disruption. As we look for the most meaningful ways to make data-based business decisions, AI, machine learning, and robotic process automation will inevitably be a part of this process. The EU Artificial Intelligence Act lays the foundation for a sustainable digital economy, and the CISO will institute this data-driven future on trust.

Quantum computing is imminent, and enterprises need crypto-agility now

Todd Moore

VP of Encryption Solutions, Thales

Nearly 100 years ago, the first quantum revolution ushered in the technological advances that have made our modern life possible. Advances in quantum physics led to the development of the transistor, laser and atomic clock, which formed the building blocks for innovations like semiconductors, GPS, medical imaging equipment, and optical fiber communication.

Today, we are nearing the arrival of the second quantum revolution. While the first quantum revolution used principles of quantum mechanics to develop new applications, the second revolution will enable engineers to manage the quantum mechanics themselves, controlling quantum systems at an individual level. The anticipated breakthroughs in quantum computing could define the next hundred years in the same way that the first quantum revolution shaped the 20th century.

But while quantum computing will lead to advancements that we cannot yet predict, it will also undoubtedly cause challenges for enterprises and their ability to secure information and communications. Current cybersecurity practices rely on classical encryption algorithms that are vulnerable to attacks from quantum computers. As quantum technology continues to advance, the security industry must develop post-quantum cryptography tools that cannot be broken by quantum computers.

The promise and challenge of quantum computing

The second quantum revolution will exploit the most advanced and nuanced properties of quantum physics; mastering these technologies has become a top priority for leading government



entities and corporations. In particular, large organizations with critical systems have recognized the importance of preparing for the security implications of quantum computing. The second quantum revolution has the potential to render current cybersecurity practices obsolete. Harvesting today's encrypted data for future post-quantum attacks has already started. Fortunately, there are steps organizations can take today to begin preparing for the quantum revolution and the emerging threats associated with it.

Governments, enterprises, and cybersecurity firms have spent the last five years anticipating the challenges of quantum security threats. The key technology for quantum-resistant solutions will be post-quantum cryptography, as these tools will enable businesses to practice crypto-agility and deploy algorithms that cannot be broken by quantum computers.

Race to develop quantum solutions

According to the National Institute of Standards and Technology (NIST), leading engineers predict that large quantum computers capable of breaking all existing encryption solutions could be developed within the next twenty years. To prepare for this threat, NIST initiated a plan to solicit and standardize at least one quantum-resistant public-key cryptographic algorithm. Over the past five years, leading engineering teams have worked to develop the algorithms which will serve as the backbone for the future of cybersecurity. NIST has identified finalists (including Thales) for the standardized post-quantum cryptographic algorithm for public key encryption and digital signatures, with the winning solution(s) to be chosen in 2022.

Pursuing crypto-agility

While there is never a silver bullet or guaranteed protection in cybersecurity, the challenges

presented by the processing power of quantum attacks can only be addressed through crypto-agility. In addition to providing vital protection against quantum hacking tools, crypto-agility will enable enterprises to lay the groundwork for future threats and solutions. Crypto-agility enables businesses to take a flexible approach to deploying new algorithms, as the new solutions do not require significant alterations to system infrastructure. In the event that the original encryption fails, updated algorithms can be deployed in the same manner. In the long-term, this approach means that enterprises can keep pace with the increasing power of computing without needing to make regular changes to their infrastructure.

Quantum computing threatens to upend the concept of trust as it relates to data ownership, data processing and communication. Crypto-agility will allow enterprises to ensure that only those able to access data assets are those who have been trusted to do so. With so little time until the onset of new cybersecurity threats, businesses and organizations must act now to protect their most important information.

The way forward

The second quantum revolution will represent a sea of change in cybersecurity threats and the tools used to protect our data and communications. Post-quantum technologies will play a vital role in securing data and communications in both backbone networks and at the edge. The security industry must come together and act quickly to develop solutions based on post-quantum technologies across the entire value chain and full set of use cases. Without the industry's recognition of this threat and support for post-quantum computing, we're putting organizations and their critical data at risk.



Crystal Eye XDR The X Factor in Your Security Program



Crystal Eye XDR allows you to reduce gaps in visibility, prioritize alerts and simplify investigations, all backed with Red Piranha's MDR team to enhance your security capability.

Security teams can no longer fight the advanced cyberthreat detection and response battleground on their own. They need help. Between managing multiple complex security tools, triaging thousands of alerts and dealing with decentralized data, it's hard to stay on top of the real threats that require attention and noise. That's where MDR comes in.

– Adam Bennett,
CEO of Red Piranha

With the proliferation of advanced cybersecurity attacks and the expansion of the cyber defence battleground CISOs, Security Managers and IT teams must work harder than ever before to secure their organisation's vast attack surface area across hundreds if not thousands of attack vectors. Most internal security departments can't keep up with the ever-expanding and complex workloads. Additionally these teams lack the dedicated resources required to effectively protect, detect, and respond to threats promptly across the entire organisation.

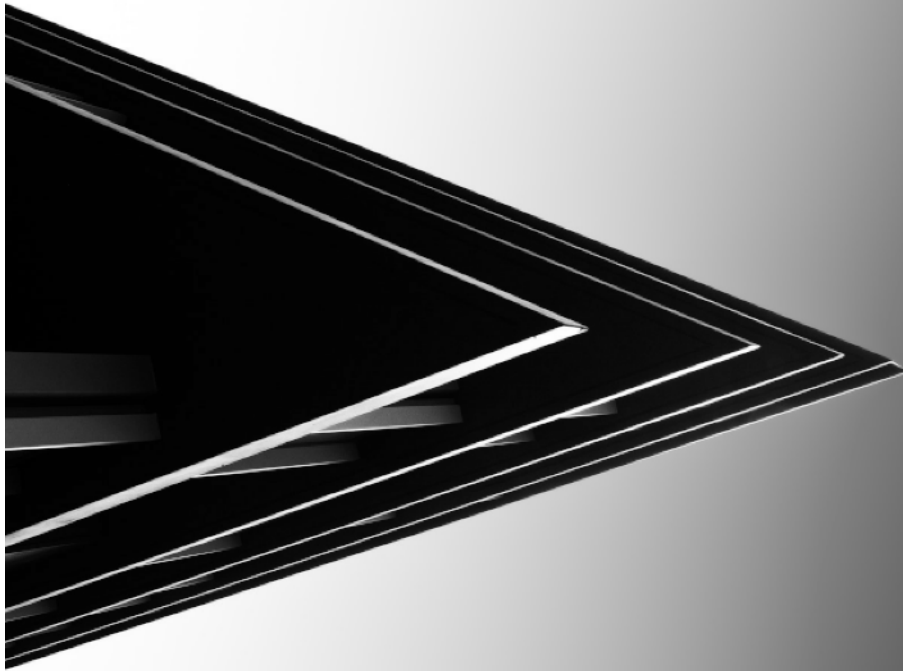
Red Piranha's Crystal Eye XDR (Extended Detection and Response) can play a vital role in reducing the burden on your security team by providing a single unified platform that intelligently and intuitively protects, detects, and responds to threats across your entire digital footprint. Allowing for the quick identification of real threats from the noise and initiate a rapid response strategy to minimize the overall impact felt by your business. All from one comprehensive and unified platform.

We provide a fully integrated Security Management (Managed Detection and Response) service to complement the XDR's capabilities. Our certified security analysts within our 24/7/365 Security Operation Centres (SOC) are available to investigate and resolve any security incidents in real-time across your network and help coordinate rapid response activities.

Our Security Management service enables your team to focus on what matters most to you while letting us handle threat detection and response. We'll be an extension of your internal team, your partner against cybercrime and a key player in strengthening your overall security posture.

Learn more at: redpiranha.net/MDR





When the adversarial view of the attack surface is missing, digital transformation becomes riskier

Mike Heredia

VP EMEA & APAC, XM Cyber

Digital transformation has become a competitive imperative in most industries. Organizations that fail to make this shift successfully - or in a timely fashion - are at grave risk of falling behind their competitors.

Yet a change of this magnitude requires diligent preparation and careful execution. Cybersecurity is one area that is often overlooked in the race to transform, and the consequences of this omission can be ruinous, both financially and reputationally.

As these initiatives have been fast-tracked, security standards have sometimes fallen by the wayside. A surprising 82% of IT leaders told the Ponemon Institute that their digital transformation initiatives were responsible for at least one data breach. One reason for this is that digital transformation has lots of uncontrolled change. Roughly 63% of IT

A surprising 82% of IT leaders told the Ponemon Institute that their digital transformation initiatives were responsible for at least one data breach.

leaders told the Ponemon Institute that they are not confident in their ability to operate securely in such contexts.

While an 82% breach rate may be understandable to some degree given the complexity of such large-scale shifts, it is also unacceptably risky. Even the most innovative processes and technologies don't mean much if a company cannot protect its business-critical assets.

The seven key challenges when pursuing digital transformation

Let's take a closer look at some of the key challenges that security organizations face when navigating this transformation:

- There is an increase in complexity and scale of the environment. Hybrid multi-cloud creates heightened complexity. Add to this the dynamic nature of cloud computing and the amount of fast-paced change needed to execute the strategy, and it becomes very problematic for security teams to manage as the attack surface is in a state of constant flux.

Using a compliance-based, box-ticking approach and relying on manual processes to manage policy is suboptimal in a dynamic environment.

- The traditional policy-based model of security does not extend easily to the cloud. Using a compliance-based, box-ticking approach and

relying on manual processes to manage policy is suboptimal in a dynamic environment. Compliance has not been an effective benchmark in traditional environments, and it is unlikely to be so in a dynamic environment.

- Defenders struggle to deal with the rapid, uncontrolled pace of change associated with digitalization. A CISO may raise concerns and be dismissed as an impediment to timely progress when highlighting legitimate concerns.
- Security posture confidence is often driven by vendors like AWS and Azure who use native tools to provide a "security posture score." Look carefully: The reality is that they are aligning configuration to policy standards – the onus of managing the configurations, controls and policies still falls on the end user.
- Operational security processes become split as separate processes are often set up to manage cloud environments, thus fragmenting the security of organizations. Split processes will really struggle to understand lateral movement. The attackers don't care about the different environments; they are simply thinking in terms of compromising critical assets wherever they are.

Traditional penetration testing and red teaming will not scale to meet the modern needs of an organization.

- Traditional penetration testing and red teaming will not scale to meet the modern needs of an organization. The approach lacks a continuous and comprehensive understanding of the attack surface, so can never adequately scale to meet the needs of a dynamic cloud environment.
- The adversarial view is missing. Defenders lack insight into the ways that cloud environments can

be compromised, as well as the mechanics and risks of lateral movement.

How attackers exploit these challenges

Attackers don't think in terms of compliance and controls. They will use all the available technical weaknesses, as they become available, to exploit critical assets. As processes fail or security tools become badly configured, attackers seize the opportunity to take the next step on the journey towards critical assets. Traditional approaches based on compliance and policy management are the perfect scenario for attackers, who wait patiently for a process to become deficient and a control to be misconfigured.

Traditional approaches based on compliance and policy management are the perfect scenario for attackers, who wait patiently for a process to become deficient and a control to be misconfigured.

There are many technical weaknesses that attackers can compromise within cloud environments, including:

- Unpatched servers
- Remote access
- Misconfigurations
- Insufficient credential, access and key management
- Open ports
- Overly permissive access rights
- Lack of multi-factor authentication
- Insecure storage containers
- Insecure APIs
- Inadequate change control

This lends itself to a wide range of attack techniques:

- Account hijacking
- Credential theft
- Credential stuffing
- Server-side request forgery
- Brute force
- Insider threat
- Ransomware
- SQL injections
- Cross site scripting
- Wrapping attacks
- Inside-out attacks

Organizations need to get back to basics and start thinking like an attacker to answer the fundamental questions, "How can I be attacked?" and "What can I do to prevent this?" These just happen to be very hard questions to answer in the context of hybrid environments without automation.

It is therefore imperative that organizations have a continuous view of how all the technical weaknesses chain together to allow exposure of the critical assets, and what opportunities are available for attackers to move laterally between environments. A silo-based approach managing individual technical weaknesses can never achieve this.

Why attack-centric exposure prioritization de-risks digital transformation

To avoid the scenarios outlined above, it is important to make cybersecurity a key lens from which to view almost all aspects of a digital transformation. CISOs must ensure that the security perspective is embedded within every part of the transformation process; organizational decision-makers must provide sufficient resources to support a secure and successful transformation and not view the CISO as a blocking agent, slowing down progress.

Part of this support includes choosing the right

software tools to help manage cybersecurity during this transition - tools that provide the adversarial perspective on a continuous basis. This attacker's perspective then needs to be wrapped into operational processes so that as the (proverbial) windows and doors become open, they are quickly closed before an attacker can exploit the gap.

An attack-path management platform provides continuous and safe attack simulation of the entire hybrid environment.

An attack-path management platform provides continuous and safe attack simulation of the entire hybrid environment. It highlights all exploitable attack paths across the hybrid environment and highlights lateral movement opportunities between cloud and traditional environments.

Such platforms also provide the necessary insight to drive cost-effective, prioritized risk mitigation. Adversarial-focused risk reporting for corporate boards helps provide much needed quantification, resolving the disconnect that is sometimes present between CISOs and the business side of the organization.

Finally, the right platform will include integration with the operational and technology ecosystem so that detect and response processes have the

Before the attack path is closed down, it needs to be monitored!

attacker's context. Before the attack path is closed down, it needs to be monitored!

Integrating these tools will ultimately provide better control over the true risk of compromise within hybrid environments and enable a more proactive approach, allowing security teams to close exposures as they appear.

Red team effectiveness will increase due to the expanding capacity and coverage, and security operations will improve because of the reduced detection and response times.

The takeaway

Ultimately, successful digital transformation requires buy-in from leaders and their teams, support from the C-suite, and a careful and well-thought-out plan. Having the adversarial perspective of the hybrid environment empowers business leaders to understand and manage exploitable risks. This provides them with the confidence to accelerate transformation and gives security teams the insight needed to dramatically reduce the chances of compromise.



HELPNETSECURITY

Mitigating third-party risks with effective cyber risk management

Third-party and digital supply chain attacks are on the rise, with third-party partners becoming an attractive target for threat actors for several reasons.

Dave Stapleton | CISO, CyberGRX

