#RSAC 2016

ISSUE 49.5, SAN FRANCISCO EDITION

MARCH 2016

CONNECT
TO PROTECT

RSA Conference, the world's leading information security conference, concluded its 25th annual event in March at the Moscone Center in San Francisco.

Keynotes, sessions and debates focused on the Internet of Things, industrial control systems, encryption, artificial intelligence and machine learning, crowdsourcing, healthcare, automotive, and more, with many reflecting current industry news. A record number of more than 40,000 attendees experienced keynotes, peer-to-peer sessions, track sessions, tutorials and seminars.

40,000 attendees

Phantom was named "RSA Conference 2016's Most Innovative Startup" by the Innovation Sandbox's judges' panel comprised of technology, venture and security industry thought leaders.

The inaugural Security Scholars Program brought together the brightest up-and-coming cybersecurity students from 10 participating public and private universities with leading experts, peers and conference attendees.

NETWORKING

"RSA Conference continues to be the premier security event, with each event seeing more attendees than ever before, and RSA Conference 2016 was no exception," said Linda Gray, General Manager of RSA Conference. "Our 25th anniversary marks not only a milestone in the conference's reach and impact in this important industry, but is also a testament to the work we as a community are doing together. We thank the cybersecurity community for its continued support, innovation, spirit and drive as we shape the future of our industry, together."

You Have the Data.
We Have the Indicators of Compromise.
We'll Find the Adversaries.

- Operationalize your threat intelligence data
- Focus your team on the threats, not your data
- Unify your security team response processes

Learn more at www.anomali.com/product.

FREE TRIAL

ANOMALI™
sales@anomali.com

Featured vendors

(IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Editor in Chief - mzorz@helpnetsecurity.com
News: Zeljka Zorz, Managing Editor - zzorz@helpnetsecurity.com
Marketing: Berislav Kucan, Director of Operations - bkucan@helpnetsecurity.com

Photography by RSA Conference and (IN)SECURE Magazine.

YOUR DATA WILL TRAVEL.

Shouldn't your security?

VERA

Secure confidential data with a single click. Track every access to data, anywhere it goes.
Dynamically change permissions, add watermarks, and revoke access, instantly.
Take back control of your data with Vera.

To learn more, visit vera.com/video

QUALYS RELEASES APP FOR SERVICENOW CONFIGURATION MANAGEMENT DATABASE

Qualys announced it has received certification of its application with ServiceNow. The Qualys App for ServiceNow CMDB is an application that synchronizes Qualys IT asset discovery and classification with the ServiceNow Configuration Management system. The app automatically updates the ServiceNow CMDB with any assets discovered by Qualys and with up-to-date information on existing assets, giving ServiceNow users full visibility of their global IT assets on a continuous basis.

Qualys collects real-time inventory information about IT assets by leveraging Qualys' Cloud Agent technology. Any changes made on the device are immediately pushed to the Qualys Cloud Platform and then synchronized into ServiceNow.

QUALYS

MINIMIZE YOUR ORGANIZATION'S THREAT EXPOSURE WITH QUALYS THREATPROTECT

Built on the Qualys Cloud Platform, ThreatPROTECT correlates data from vulnerability scans and active threat data from multiple sources into a single dynamic dashboard to provide a holistic and contextual view of an organization's threat exposure. With ThreatPROTECT, customers can visualize, prioritize and take action to minimize exposure from vulnerabilities related to the threats that matter most.

"In today's rapidly changing threat landscape, the most effective way for companies to protect themselves is to accurately identify assets, prioritize threats and take action to prevent a compromise," said Philippe Courtot, chairman and CEO for Qualys.

DB | NETWORKS®

DATABASE CYBERSECURITY

Non-intrusive deep protocol inspection, discovery machine learning, and behavioral analysis

- ☑ Database Discovery
- ☑ Application to Database Mapping
- ☑ Identify Credential Abuse
- ☑ Immediately Identify Database Attacks

TERBIUM LABS CLOSES $6.4M IN FUNDING FOR STOLEN DATA DISCOVERY ON DARK WEB

Terbium Labs announced has raised $6.4 million in Series A financing led by .406 Ventures, bringing the total raised to $9.7 million. Terbium Labs will use the new capital to expand its team and accelerate enterprise sales of Matchlight, a Dark Web data intelligence platform.

Making its public debut in June of 2015, Matchlight has quickly grabbed the attention of the security industry and CISOs at leading businesses and government organizations for its innovative approach to information security, offering much-needed private, proactive and automatic breach detection and response that is both affordable and reliable.

The average data breach takes more than 200 days to identify, giving adversaries months or even years to exploit a security incident and costing the global economy $450 billion annually. With Matchlight, organizations can discover in seconds to minutes when a compromise has occurred and take action, minimizing the damage, loss, and risk cause by a data breach

DISCOVER, CLASSIFY, PROTECT AND ANALYZE DATA WITH TITUS ILLUMINATE

TITUS launched its data discovery and classification tool, TITUS Illuminate. Already in use by large enterprise organizations, TITUS Illuminate examines and automatically classifies files discovered on-premise as well as in the cloud.

With TITUS Illuminate you can:

- Discover data in network file shares, SharePoint, as well as cloud shares such as SharePoint Online, OneDrive, Dropbox and Box to determine where sensitive data resides.
- Identify the business value of data so an organization knows what data it has and how it should be protected.
- Classify any file type based on the content (PCI, PII, PHI or intellectual property), context or file properties (author, location, etc).
- Apply content protection to files where they reside, quarantine files that are stored inappropriately, or flag files for follow-up where risks are identified based on the combination of content and location.
- Analyze data with built-in analytics and reports or through third-party business intelligence tools to help identify risk areas for the organization.
- Integrate with other security solutions such as DLP and ERM that can access TITUS metadata to enforce appropriate protection policies.
- Work seamlessly with TITUS Classification Suite to enforce rules on files in motion, ensuring the right people have access to the right information at the right time.

THREATQ

THREAT INTELLIGENCE PLATFORM

INDICATOR MANAGEMENT • INCIDENT ANALYSIS • ADVERSARY PROFILING

Malware Specimens

DETECTION SOLUTIONS

LEARN MORE AT THREATQ.COM

Logs / Alerts

Distribute Indicators / Signatures

SIEM
Deploy threat intelligence to enrich SIEM alerts. Provide indicator attribution to SIEM to prioritize incoming alerts.

Events are escalated

TICKETING SYSTEM
Collect incident details from a ticketing system to determine indicator and source validity.

Indicator/Alert metrics

Actor's indicators
Nested indicators

Alert metrics
Incident Annotations

ADVANCED THREAT PROTECTION
Automatically ingest malware analysis to deploy indicators and create an event around the identified attack.

THREATQ

LOG REPO
Perform a 'rear-view-mirror' search to identify prior successful attempts and determine indicators false positive probability.

INCOMING FEEDS
• Government • Private Community • Commercial • OSINT

EXPORT INTELLIGENCE VIA API
• XML • JSON • TAXII • PDF / PNG

OPERATIONALIZE CYBER THREAT INTELLIGENCE


Birds of a Feather
RSAConference2016
25th
Birds of a Feather


TITUS
Classify, Protect & Confidently Share


QUALYS
Michael McCaul at
RSA Conference 2016
Meet Author and Chairman of the
Homeland Security Committee.
See Agenda


ANOMALI
• Threat Intelligence Made Relevant
• Early Breach Detection
• Make Your SOC & SIEM More Effective
EXIT
ANOMALI

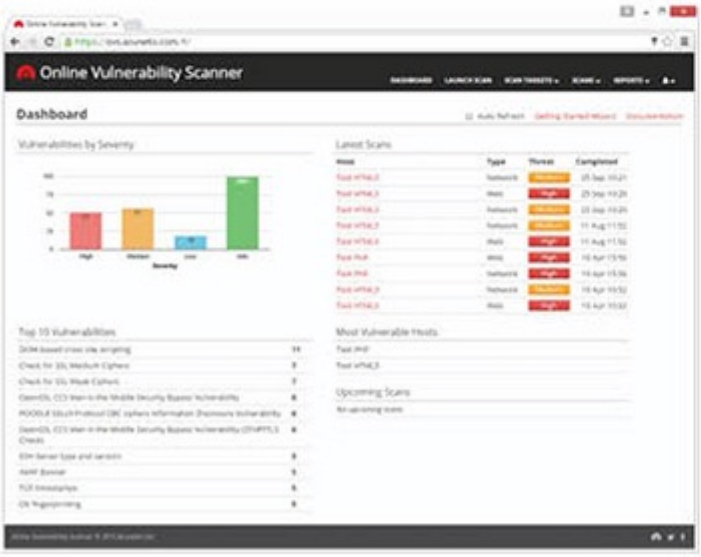

VERA
RSAConference2016
TechCrunch

acunetix

Is your website hackable?

Check with Acunetix Vulnerability Scanner

Hackers are concentrating their efforts on web-based applications - shopping carts, forms, login pages, dynamic content, etc. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases and also allow hackers to perform illegal activities using the compromised site. Firewalls, SSL and Hardened Networks are Futile against Web Application Hacking!



Audit Your Website Security with Acunetix Vunerability Scanner

Acunetix is available Online (OVS) and on Premise (WVS):

- Detection of SQLi & XSS Vulnerabilities (incl. DOM-based & Blind XSS)
- Checks for known vunerabilities in WordPress, Drupal and Joomla
- Full HTML5 & JavaScript analysis
- Advanced penetration testing tools
- Free network scanning of perimeter servers
- Automated scanning of password protected areas
- Compliance Reports.

Register Online or Download today!
www.acunetix.com

acunetix

REACH US ON
info@acunetix.com

+1 917 722 8550
+44 (0) 330 202 0190

www.acunetix.com

ENDPOINT PROTECTOR: FIGHT DATA LEAKAGE ON LINUX WORKSTATIONS

CoSoSys released Endpoint Protector DLP for Linux in Private Beta, enabling protection against data leakages for confidential data on organization's Linux workstations. Endpoint Protector already runs on Linux distributions like Ubuntu, OpenSUSE, RedHat and CentOS with device control features to block the use of specific portable storage devices and prevent data loss and data theft. With the recently announcement Endpoint Protector 4.4.1.0, the content-aware DLP module is also available for Linux.

The features include content filtering based on file type, predefined content (PII, credit card numbers, social security numbers, and others), and custom content with dictionaries of keywords and regular expressions.

With Endpoint Protector DLP for Linux, IT administrators are now able to constantly track user data transfers to portable storage devices and the cloud as well as block certain file transfers. Based on comprehensive reports provided by the solution, organizations can detect data security incidents as they happen. The intuitive management console enables the easy implementation of the DLP policies on Linux workstations, as well as on Windows and OS X, completing the data security systems.

BARRACUDA EXPANDS NEXTGEN FIREWALL PRODUCT LINE

Barracuda has expanded its next-generation firewall product family with the addition of the new Barracuda NextGen Firewall S-Series, which is designed to empower customers to connect thousands of machine endpoints, such as ATM machines or other remote devices, enabling new IoT applications and deployments.

Barracuda announced immediate availability of two new products in the S-Series: the Barracuda NextGen Firewall Secure Connector 1 (SC1) and the Barracuda NextGen Secure Access Concentrator (SAC). The Barracuda NextGen SC1 is a small appliance that includes firewalling, Wi-Fi, and full VPN connectivity. The Barracuda NextGen SAC is a virtual gateway – capable of running in Microsoft Azure environments or in private clouds – to optimize network traffic flow and centrally apply next-generation security functionality to deployed SC1 appliances. The Barracuda NextGen Firewall S-Series helps customers enforce proper access privileges, secure and centrally manage all communications, and quickly roll out thousands of devices to untrained staff in remote locations.

Klaus Gheri, VP Network Security, Barracuda, said: "Barracuda NextGen Firewall S-Series empowers customers to massively scale thousands of connected devices with powerful technology that is easy to use and affordable. The Barracuda NextGen Firewall S-Series launch further underscores Barracuda's aim to help customers optimize network traffic and better regulate application usage in highly distributed and hybrid environments."

HOW EFFECTIVE ARE ORGS AT DETECTING AND INVESTIGATING CYBER THREATS?

A new threat detection effectiveness survey compiling responses from more than 160 respondents around the world has provided valuable global insight into what technologies organizations use, what data they gather to support this effort, and their satisfaction with their current toolsets. Additionally respondents were asked what new technologies they plan to invest in and how they plan to evolve their strategies going forward.

According to RSA, a key insight from the survey was that respondents expressed deep dissatisfaction with their current threat detection and investigation capabilities.

CYBERSECURITY STILL SEEN AS A TECH ISSUE, NOT A BUSINESS IMPERATIVE

Cybersecurity is now front and center on organizations' boardroom agendas, but most CISOs have yet to earn a seat at the table.

According to a study by ISACA and RSA Conference, 82 percent of cybersecurity and information security professionals polled in the survey report that their board of directors is concerned or very concerned about cybersecurity, but only 1 in 7 (14 percent) CISOs reports to the CEO.

This gap between belief and actions at the highest levels of management is playing out in an environment where 74 percent of security professionals expect a cyberattack in 2016 and 30 percent experience phishing attacks every day.

RESEARCHER DEMONSTRATES HIJACKING OF POLICE DRONE

A security researcher has demonstrated to the RSA Conference crowd how he – or anyone, for that matter – can take over control of a drone used by the Dutch police and make it do anything the rightful owner can.

The hijacking – executed via a Man-in-the-Middle (MitM) attack combined with command injection – can be performed easily and very cheaply, researcher Nils Rodday says – you just need a laptop and a cheap radio chip connected via USB.

WHICH PASSWORDS TO AVOID FOR INTERNET-FACING SYSTEMS?

For the last year or so, Rapid7 has been collecting login credentials via "Heisenberg," a network of low-interaction honeypots that the company has set up to analyze login attempts by random, opportunistic actors.

The honeypots emulate the authentication handshakes of several protocols, but nothing more than that, so the motives of the "attackers" are unknown. But the recorded login attempts give insight into the top attempted usernames, passwords, and username:password combinations.

The recently released report that the company has compiled in the wake of this research has concentrated on login attempts coming through the Remote Desktop Protocol (RDP).

ONLY ONE IN FIVE ORGS SET UP TO SECURELY MANAGE USER IDENTITIES

As organizations seek to capitalize on digital opportunities through rapidly developing and hosting new services online, they frequently under-invest in adequate cybersecurity measures creating significant risks, in particular governing user access.

"Identity Crisis: How to Balance Digital Transformation and User Security?", a survey of more than 800 C-level executives in the US, UK, Germany, France, Benelux and the Nordics revealed that 62 percent believe it is very important or critical for their organizations to enable or extend access for users to digital services securely, yet only 26 percent have the technology in place to do so.

Next Generation MANAGED SECURITY SERVICES

SOLUTIONARY®

AN NTT GROUP SECURITY COMPANY


LinOTP
initiative
Twistlock
SECURITY, BUILT FOR CONTAINERS
VULNERABILITY MANAGEMENT AND RUNTIME PROTECTION FOR CONTAINERS
DEEP "DNA" ANALYSIS
PURPOSE-BUILT
AGENT-LESS
rasoo
VISIT US


IS YOUR WEBSITE
HACKABLE?
Check with Acunetix Vulnerablity
www.acunetix.com


cisco
intel Security


RSAConference2016
CRYPTOGRAPHERS'
PANEL


DARKMATTER
THREATQ


zscaler
Data Loss Prevention (DLP)
Device Control
Mobile Device Management (MDM)
ENDPOINT PROTECTOR

MICRO FOCUS | NetIQ

Identity-Powered Security

Balancing usability with reduced risk

- Identity and Access Governance
- Access Management & Authentication
- User Activity Monitoring

Contact
www.netiq.com

THREATSTREAM REBRANDS AS ANOMALI, REDEFINES THREAT INTELLIGENCE

ThreatStream changed its name to Anomali and launched two new products: Harmony Breach Analytics for mid-to-large enterprises, and the Anomali Threat Analysis Reports Service for small to medium sized businesses.

"SIEMs today can only ingest and correlate a small fraction of the 25 Million indicators of compromise we've curated that are currently listed as active. We see threat intelligence as the next 'big data' problem," said Hugh Njemanze, CEO of Anomali. "For perspective, hackers are automating the production of 18 million fraudulent domain names per day and the amount of active IoCs is currently growing 39 percent each month. This makes non-curated threat intelligence data far too noisy for use by incident response and security operations teams.

Harmony Breach Analytics and Threat Analysis Reports Service were purpose-built to find and focus an organization's attention on only threat intelligence that is relevant to their organization at any given moment."

Harmony Breach Analytics, built on the ThreatStream Threat Intelligence Platform, can work with your existing threat intelligence platform or completely replace it. It will read your organization's log data, cull the possible IoCs from it and compare them to Anomali's massive library of threat data in real-time. This approach focuses security operations, incident responders and threat analysts on actionable threats.

The Anomali Threat Analysis Reports Service allows an organization to simply and easily submit their raw log data to Anomali. The service strips out potential indicators of compromise from the data and looks for matches in Anomali's vast store of threat intelligence data.

The report provides threat analysis reports that are relevant and actionable. The reports generated provide security metrics for inbound and outbound threats and a view of all matches and live links for additional attacker information. These reports are available as a subscription and provide automated security situational awareness.

IT SECURITY NEEDS LESS WALL, MORE INTELLIGENCE

MEET CONTEXTUAL SECURITY INTELLIGENCE TO:

PREVENT APT ATTACKS
Privileged User Behavior Analytics uses real-time monitoring and five-factor statistical analytics to detect hijacked accounts.

SUPERVISE VIP USERS
Privileged Activity Monitoring helps you to superintend your sysadmins and outsource contractors without hindering their work.

UNDERSTAND IN REAL-TIME
Balabit CSI Suite™ combines advanced monitoring techniques with contextual information to provide a real-time CISO dashboard™.

GET COMPLIANT
Balabit CSI Suite™ is producing bullet-proof audit trails round-the-clock making audits and forensic investigations incredibly fast

BALABIT

PASSWORDLESS SECURITY FOR CONSUMER-FACING WEBSITES

iovation launched its new Customer Authentication service that allows consumer-facing websites to enhance security while streamlining and improving the customer experience.

The easy-to-integrate device authentication service eliminates friction by allowing consumers with “known devices” to bypass passwords and immediately access relatively low-risk but still confidential sections of their online accounts—like account balances, shopping records and activity histories. If needed, iovation’s device authentication triggers stronger “step-up” authentications like one-time passwords for higher risk actions like user and account changes, money transfers, or purchases.

Unlike competing algorithms that use only cookies or IP addresses or rely on algorithms depending on exact matches, the new Customer Authentication service offers greater elasticity for fewer false negatives while still identifying key device characteristics. This kind of SaaS-based device authentication is the first step along the road to “continuous authentication” that will validate not only logins, but still prevent man-in the-middle, man-in-the-browser and spoofing attacks at any point during a customer’s session.

BALABIT’S BLINDSPOTTER EXTENDS BEHAVIOR ANALYSIS WITH BIOMETRICS

Balabit, best known as “the creator of syslog-ng,” announced the release of Blindspotter version 2016.03. The new version of its User Behavior Analytics (UBA) solution features several new and unique machine learning algorithms that help security teams to quickly identify hijacked accounts or discover forbidden account sharing, thereby avoiding large-scale data breaches or compliance problems.

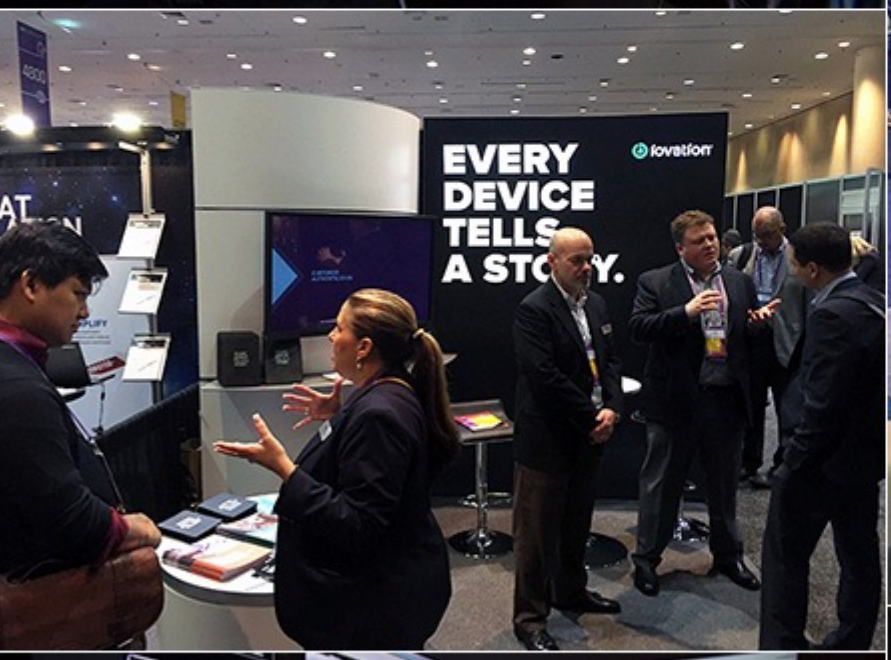
System accounts used by humans, shared accounts and personal accounts used by scripts are typical red flags of potential security risks for the company. When an attacker gains access to stored credentials used by a script, particularly if those are the credentials of a privileged account, this can lead to a large-scale data breach. Blindspotter is able to distinguish between human and automated activity and allows the security team to discover the misuse of personal or service accounts.

Based on the technology of Shell Control Box, Balabit’s market leading activity monitoring solution, Blindspotter has already been able to analyze commands issued in SSH and Telnet administrative sessions and find potentially risky activities. In v2016.03, this capability is extended to Windows users using RDP.


Twenty-five Years of Information Security Milestones
2000
2001
2002
2003
2004
2005
2006
2007


IoT Sandbox


Database Cybersecurity
NETWORKS
neustar


EVERY
DEVICE
TELLS
iovation


BALABIT
THE CREATORS OF
SYSLOG-NG
BALABIT
LOG
+
PAM

DB NETWORKS PARTNERS WITH CYPHORT AND SECURITY ON-DEMAND

Big news from DB Networks, a provider of database cybersecurity products. They partnered with Cyphort to offer customers full spectrum visibility from the desktop and network perimeter to deep in the database, and their Layer 7 Database Sensor has been chosen to power Security On-Demand's Database Threat Protection service.

"The combination of Cyphort and DB Networks provides enterprises with a comprehensive analysis of the kill chain," said Rami Shalom, vice president of product management at DB Networks. "Enterprises can now observe and mitigate risk throughout their entire infrastructure including risks effecting critical data assets, thereby focusing attention on the riskiest activities."

"Databases can be a blind spot for businesses. Many organizations lack policies and procedures for creating or copying databases. The result is a sprawl of undocumented databases. You can't protect what you don't know about. With this service, we offer unprecedented insights into database activity, vastly improving the ability to identify insider and external threats," said Peter Bybee, CEO of Security On-Demand.

IDENTIFYING ABUSE OF COMPROMISED CREDENTIALS IN REAL-TIME

DB Networks announced industry-first capabilities to non-intrusively identify compromised credentials in real-time by uniquely applying machine learning and behavioral analysis to every database communication. This powerful new feature is now available in its DBN-6300 and Layer 7 Database Sensor products.

Rather than inherently trusting specific clients, servers or users, the new approach identifies normal business flows and evaluates the risk and business context of any deviation. Doing this accurately and in real-time requires deep protocol analysis on large amounts of database communications to detect when an entity demonstrates a new behavior – indicative of an attacker using stolen credentials.

The cyber criminals' primary goal is to obtain privileged logon to gain access to sensitive and valuable data. Once they have obtained the proper credentials they can pose as the privileged insider and breach the databases. At that point they can access sensitive assets and setup a channel to exfiltrate an entire data set to an off-site server.

Once a compromised credential is identified it's critical to understand the scope of the incident. DB Networks assists security professionals with a security search tool to enable them to easily investigate any suspicious activity in the database tier. This powerful capability is extremely useful to understand the scope of activity that resulted from compromised credential.

TERBIUM LABS

Data Intelligence

A CISO wants to know the moment her data appears on the dark web.

The catch?

She can't share the data.

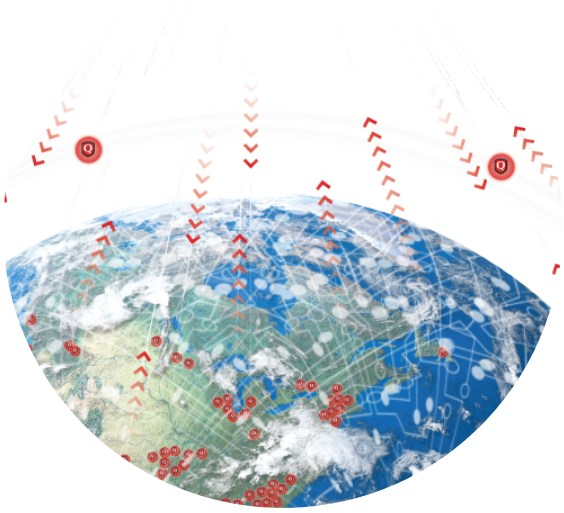
With Matchlight, she doesn't have to.

Matchlight finds your data on the dark web privately, within minutes.

TERBIUMLABS.COM

QUALYS DELIVERS SCALABLE, CLOUD-BASED PATCHING

Qualys announced an OEM partnership with HEAT Software to deliver a cloud-based patch management offering to its global customers. The partnership allows Qualys to embed HEAT Software's PatchLink technology within the Qualys Cloud Platform. The new combined offering allows Qualys to distribute patch management data via the Qualys Cloud Platform, enabling customers to detect and patch vulnerabilities on IT systems and endpoints via the Qualys Cloud Agents.



With the new patch management offering via a single cloud-based console, Qualys customers can automatically identify and patch heterogeneous operating systems, Microsoft security and non-security vulnerabilities, third-party applications and endpoint configurations—all seamlessly managed through a single cloud-based console.

QUALYS

QUALYS EXTENDS CLOUD AGENT PLATFORM TO SUPPORT LINUX AND OS X

Qualys announced the expansion of the Qualys Cloud Agent Platform. The Cloud Agent platform empowers organizations with flexibility and real-time asset inventory searches on a global scale, to effectively address the security and compliance of their IT assets, whether on premise, in the cloud or on mobile endpoints.

Qualys announced the availability of cloud agents for Linux and OS X, adding to the platform's existing support for Windows. Support for these operating systems is key to securing elastic cloud environments and endpoints where these operating systems are predominant. The Qualys Cloud Agent Platform combines the power of the Qualys platform with lightweight agents that are extensible, centrally managed and self-updating, allowing global businesses to continuously assess the security and compliance of their IT infrastructure and applications.


NTT Group
Security
Full life-cycle security services based on intelligence, technology and expertise.
SOLUTIONARY
dimension data
NTT Communications
NTT Com Security
NTT Group
Security


QUALYS
CONTINUOUS SECURITY
SEARCH, DETECT, RESPOND
CLOUD AGENTS IN ACTION
MEET RAMI MALEK,
CYBERSECURITY ENGINEER /
Qualys

PHISHING UNDERGROUND: EXPLOITING THE HUMAN VULNERABILITY

PhishLabs exposed the murky evolution of a thriving, sophisticated phishing underworld. Their report is based on more than one million confirmed malicious phishing sites residing on more than 130,000 unique domains, and the movement of more than 90 threat actor groups and organizations actively deploying spear phishing.

"Our research clearly shows that phishing attacks are the weapon of choice for adversaries across the spectrum," said John LaCour, Founder and CEO of PhishLabs. "Most successful hacks today start with a phishing attack. It is critical for organizations to understand the true risk of phishing and how they can fight back to protect their business."

SENIOR LEVEL PERCEPTIONS ABOUT SAP SECURITY

More than half of companies believe it is likely their company would have a data breach due to insecure SAP applications, according to a new Ponemon Institute study. This same group indicates their company's SAP platform has been breached an average of two times in the past 24 months, yet 63 percent indicate C-level executives tend to underestimate the risks associated with insecure SAP applications.

This perception gap is furthered by the limited visibility organizations have into the security of SAP applications and many do not have the required expertise to quickly prevent, detect and respond to cyber attacks – a problem which 60 percent of respondents say would be catastrophic or very serious and could lead to $4.5M average cost if systems are taken offline.

COMPANIES ARE REALIZING THAT SECURITY AND PRIVACY GO HAND IN HAND

50 percent of companies over the past two years have increased the involvement of privacy professionals on their information security teams to enhance the prevention of data breaches, a joint study by IAPP and TRUSTe has found.

The study polled 550 privacy, IT and information security professionals across the globe. The findings reveal a significant increase in privacy-related investments, with 42 percent of firms spending more on privacy technology, nearly keeping pace with increases in security tools.

The study also confirms the well-documented extent of the cybersecurity threat as 39 percent reported an incident in the last two years and increased their information security and privacy investments alike to address the growing threat.

HACKING HOSPITALS: CYBER ATTACKS CAN RESULT IN PHYSICAL HARM

Independent Security Evaluators (ISE) published a study that demonstrates security flaws to be pervasive within the healthcare industry.

The research found that adversaries could deploy cyber attacks that result in physical harm to patients. 100% of the hospitals investigated all had very serious security issues, suggesting broader implications across the entire industry.

"The industry today is focused almost exclusively on protecting patient records," notes ISE founder Steve Bono. "We set out on this research to determine what are the threats to patients lives, and how realistic are those threats." Bono explains the research impact, stating, "We found those threats to be very real, and worse still, the industry is ill-prepared to effectively deal with them."

Over the course of 24 months, the researchers investigated 12 healthcare facilities, 2 healthcare data facilities, 2 healthcare technology platforms, 2 active medical devices, and a host of other devices and applications. The research proved that remote adversaries can deploy attacks that target and compromise patient health.

TITUS Illuminate™

Discover · Classify · Protect · Analyze

TITUS Illuminate helps you define what and where your data is, who has access to it, and how to protect it.

Discover data at rest in network and cloud file shares

Classify files based on content and context

Protect files with encryption and remediation options

Analyze results to better understand your data

TITUS TITUS.com/illuminate

VERA SECURES $17 MILLION IN SERIES B FINANCING

Vera, a top 10 finalist for the Innovation Sandbox competition at RSA Conference 2016, has closed $17 million in Series B financing, led by Sutter Hill Ventures, with participation from existing investors Battery Ventures, Clear Venture Partners, and Amplify Partners. As part of the financing, Stefan Dyckerhoff, Managing Director at Sutter Hill Ventures will join the Vera board of directors.

To date, the company has raised over $31M in total funding. The injection of new capital will fuel the company's aggressive growth on its mission to become the trusted standard for securing and sharing all forms of business information.

"Vera is bridging a critical security gap by changing the way enterprises think about securing their data and we're excited to be part of this opportunity," said Stefan Dyckerhoff, Managing Director at Sutter Hill Ventures. "Vera is a leader among this new and exciting class of security solution providers. All of us at Sutter Hill Ventures are extremely impressed with how Vera has redefined information security and it's exciting to see the industry take notice."

THREATQUOTIENT WINS SECURITY START UP OF THE YEAR AWARD

ThreatQuotient announced its Threat Intelligence Platform (TIP), ThreatQ, was recognized as a Silver winner for Innovation in Enterprise Security at the 2016 Info Security Global Excellence Awards. The awards gala held during the RSA Conference acknowledged the winners amongst their peers for their advanced, ground-breaking products and solutions that are helping set the bar higher for others in all areas of security and technology.

"Today's threat intelligence analysts and operators are inundated by data and spend valuable time manually importing information," said John Czupak, President & CEO at ThreatQuotient. "Our job is to make theirs easier; and we are doing that by providing a seamless integration with existing security solutions to enrich and nurture indicators. The recognition of ThreatQ by Info Security is a further testament to our innovative approach to operationalizing intelligence."

ThreatQ is the only TIP that centrally manages and correlates unlimited external sources with all internal security and analytics solutions for contextual, operationalized intelligence in a single view. As a result, ThreatQ enables threat intelligence teams to return their focus to analysis, and improve their security operations by reducing the amount of effort traditionally exerted into combining data sources. Additionally, ThreatQ is the first TIP to provide Indicator Nurturing, which goes beyond enrichment to help customers tailor indicators of compromise (IOCs) more specifically to their infrastructure.

Twistlock

SECURITY, BUILT FOR CONTAINERS

PROTECT ANYWHERE

From Dev workstations to private cloud to public cloud

CRADLE TO SCALE

Integrated protection from images, registry, to production servers

DEEP "DNA" ANALYSIS

Intent, behavior, provenance of containers

PURPOSE-BUILT

Designed for the container environment

"Top 20 Cybersecurity companies to watch for 2016"
- DarkReading

"Breakout security companies to watch for 2016"
- Momentum partners

"Best Emergent Technology"
nomiee
- SC Awards 2016

www.twistlock.com Free trial: www.twistlock.com/demo contact@twistlock.com