WHITE PAPER

Addressing FFIEC Cybersecurity General Observations

With AlienVault Unified Security Management (USM)

"Cybersecurity threats continue to represent significant potential operational risks to financial institutions. Cyberattacks are expected to increase in frequency and severity as worldwide interconnectedness grows and the capabilities to conduct cyberattacks become more sophisticated and easier for criminals or terrorists to obtain."

This was a sobering quote from the National Credit Union Administration (NCUA) in 2016. Banks and credit unions have long been receiving guidance from the FFIEC to help protect data sought after by criminals and nefarious insiders. For instance, in November of 2014, the FFIEC issued observations to clarify what it believed are fundamental requirements the financial service industry must follow to protect systems and data. In many ways, the core of their guidance was that security is no longer a nice-to-have but essential. Additionally, securing systems and data is more and more becoming a business obligation that is capturing attention from the boardroom. Boards of directors and audit committees are asking executives tougher security questions and at the same time scrutinizing additional capital expenses. In other words, the message is: adhere to the requirements, but don't spend a lot of money in the process. Faced with tighter fiduciary responsibilities alongside an increase in attacks, this is no small challenge. It's certain now that regulatory oversight has placed cybersecurity as a key business area of focus.

AlienVault Unified Security Management ™ (USM) Provides a Comprehensive Solution

Applying the FFIEC's cybersecurity observations can prove to be a difficult challenge for many in the financial services industry. Organizations lagging behind are turning to solution providers to help get up to speed in a hurry. Which solution is right for the organization might be difficult to answer, as there are competing requirements: Providing all-inclusive visibility, avoiding the challenges of integrating multiple products , and finding a solution that is unified, simple, and affordable.

Named one of Deloitte's fastest growing companies, AlienVault meets these requirements by providing a unified solution that accelerates and simplifies threat detection and response for IT teams with limited resources. Its built-in security capabilities and integrated threat intelligence help many banks and credit unions comply with FFIEC cybersecurity guidelines. A short list of the essential security capabilities for financial services provided by the AlienVault Unified Security Management (USM) platform include:

ESSENTIAL SECURITY FEATURES FOR FINANCIAL SERVICES INCLUDED IN USM
Asset discovery to detect unknown systems on your network
Vulnerability Assessment to identify likely targets by attackers
Network and host-based intrusion detection to detect malicious activity on your network

ESSENTIAL SECURITY FEATURES FOR FINANCIAL SERVICES INCLUDED IN USM
File Integrity Monitoring (FIM) to detect changes in critical files
Security Information and Event Management (SIEM) to correlate security events from across your network
Integrated threat intelligence and response guidance to prioritize the most significant threats targeting your data, applications, and users
Compliance report templates for GLBA, PCI as well as custom reporting
Continuously updated detection capabilities that allow you to automatically detect emerging threats

AlienVault's USM Addresses the FFIEC Guidance

When regulators issue guidance, it becomes an easy benchmark for comparison. Organizations can simply go down the checklist to determine what actions have been taken and what items are outstanding. It is incumbent upon an organization to adhere to the minimum guidance. However, compliance does not necessarily equal security. It is in an organization's best interests to be forward-thinking and have a solution in place that is capable of a proactive, holistic approach to security.

AlienVault, recognized as a "Visionary" in the Gartner Magic Quadrant for SIEM, provides a unified security platform that makes it possible for organizations to get full visibility into their security program. The outline below illustrates where AlienVault is able to help financial services organizations in their efforts to apply the FFIEC tactical guidance and improve their security program.

Cybersecurity Inherent Risk

FFIEC General Observation: Risk and security posture assessments continue to be a key focal point for examiners and rightfully so. Where is the risk and what is being done to manage it? The FFIEC expects financial institutions to assess their activities and connections based on type, volume, and operational complexity. Is there visibility into connections being made, are they legitimately needed, hostile or not secure? Each connection represents an entry point for an attack to occur. Legacy protocols such as Telnet and FTP are still fairly common in the enterprise. Determining the source and destination, and more importantly the data transmitted, is vital. Once determined, organizations can then work with business units to secure application connections that can be used as an attack vector.

The FFIEC understands that attackers look to exploit products and services offered by the financial institution. Fraudsters will attack where the money flows – namely wire transfer or automated clearing house (ACH), online banking, ATMs, payment systems, and on-premise and cloud applications. In essence, identify the connections and the applications at risk where sensitive financial or credentialed connections exist.

AlienVault USM Capabilities: AlienVault USM provides a consolidated, single-screen view of all network activity including views by asset groups, such as in-scope PCI assets, which require special policies. This centralized view enables organizations to better understand their security posture, including the ability to pinpoint connections and validate their purpose so that corrective security changes can be made when necessary. This is part of the network discovery organizations can perform to create a baseline for further assessments in order to identify new connections which were not previously known. The USM platform will pinpoint the connections and their protocols to help users adhere to compliance mandates such as identifying insecure connections that are not allowed and require strict SSL/TLS or SSH for secure data transfer. Armed with this network inventory, teams are then able to take necessary action to reduce risks which may have otherwise been unknown. Figure 1 below illustrates the ability to view individual assets or groups of assets to assess your security posture.

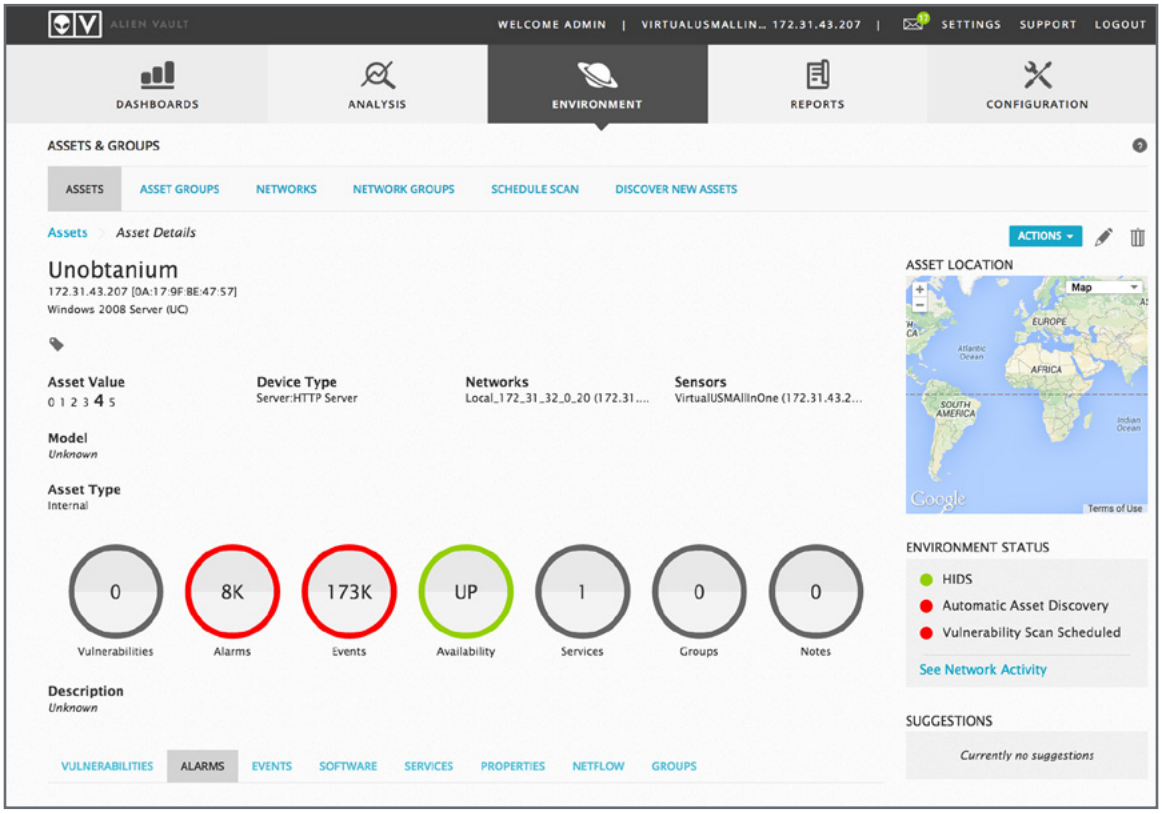

Figure 1: Granular detail on assets and asset groups

Risk Management and Oversight Observation

FFIEC General Observation: Regulation through the years has fast-tracked financial institutions into managing security risk better than other industry verticals. With security leaders encountering more board-level discussions, there's heightened sensitivity to roles and responsibilities and insight into what is occurring across the business. The oversight observation is mainly focused on governance and resources in order to effectively manage risk across the business. Management accountability for risk-based decisions factors heavily on the FFIEC's observation.

AlienVault USM Capabilities: Visibility into conformance to policies, activity, and the overall security posture is achievable with USM. The USM platform's central repository provides security leaders with a solution to pull back the data and report to boards and executive management on the state of the business across endpoints and networks. In particular, AlienVault has dedicated compliance reporting for GLBA, PCI, ISO 27001, FISMA, and others. These pre-defined reports, plus the ability to utilize over 2,200 report elements to build custom reports, ensure that users can measure and report on compliance, and make it easier to answer direct risk management and oversight questions they are asked. Figure 2 provides an example of AlienVault's executive dashboard, which users can customize to address specific compliance and governance needs.

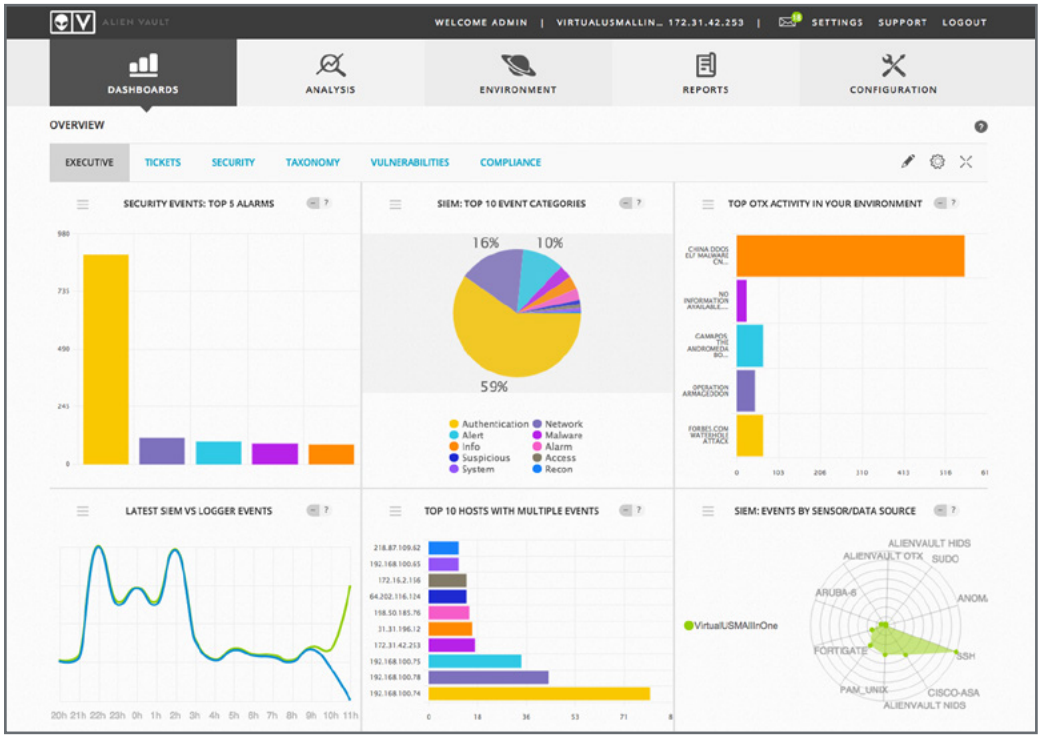

Figure 2: Dashboard View and Governance Oversight

Threat Intelligence and Collaboration Observation

FFIEC General Observation: Threat intelligence and collaboration continues to be a hot topic and for good reason. No one institution can go at this alone – it's strength in numbers. Sharing information with industry peers is vital. Just because the attacker is not directly attacking a specific financial services company now does not mean that organization won't be in the crosshairs for a future attack. The FFIEC expects organizations to gather, monitor, and analyze multiple sources of information on threats and vulnerabilities. Managing intelligence and collaborating with others across the globe increases awareness of threats and enables better risk management decisions to be made. This approach is more proactive and can be combined with log analysis to look for anomalies or trends. This activity links directly into the previous observation (risk management and oversight) to provide executive and board-level reporting.

AlienVault USM Capabilities: AlienVault USM includes built-in threat intelligence provided by the AlienVault Labs threat research team, supplemented by threat data from Open Threat Exchange (OTX). OTX is the world's first truly open threat intelligence community that enables collaborative defense with actionable, community-powered threat data. Over 37,000 participants contribute over 3 million threat indicators daily from more than 140 countries that identify malware hosts, command and control servers, botnets, and more. OTX enables teams to analyze seemingly harmless connections that when correlated with IP reputation data highlight potentially compromised communication. The AlienVault Labs team verifies and curates the data, ensuring that all is accurate and current. USM will alert users of communication with known bad actors and to emerging threats identified in OTX. While there are many subscription-based services available from intelligence firms, AlienVault provides this real-time threat data as part of its crowdsourced model. The OTX data is also integrated into the products of several OTX partners including companies such as Bit9, Centripetal Networks, HP, Risk I/O, ThreatStream, and many others.

The integrated threat intelligence saves IT teams significant amounts of time and effort, as they no longer have to create the correlation rules and conduct the threat analysis to receive prioritized alarms about malicious activity within their networks. Instead, IT teams can focus on responding the to threats identified by USM and reduce their risk profile. Armed with intelligence data, organizations are able to be proactive and if necessary involve allies, including law enforcement, a relationship expected to be in place by the FFIEC. AlienVault continues to receive accolades in the industry for the contributions and intelligence gathering available to their customers.

The AlienVault Labs team also publishes weekly updates to SIEM correlation directives, IDS signatures and more, based on their threat research and the global threat data available in OTX. This makes it possible for IT teams to detect the latest threats without needing the deep security expertise required to conduct detailed threat research themselves.

Figure 3 below shows the OTX activity map available in USM which identifies malicious actors attempting to interact with a network based on the IP reputation data from OTX.

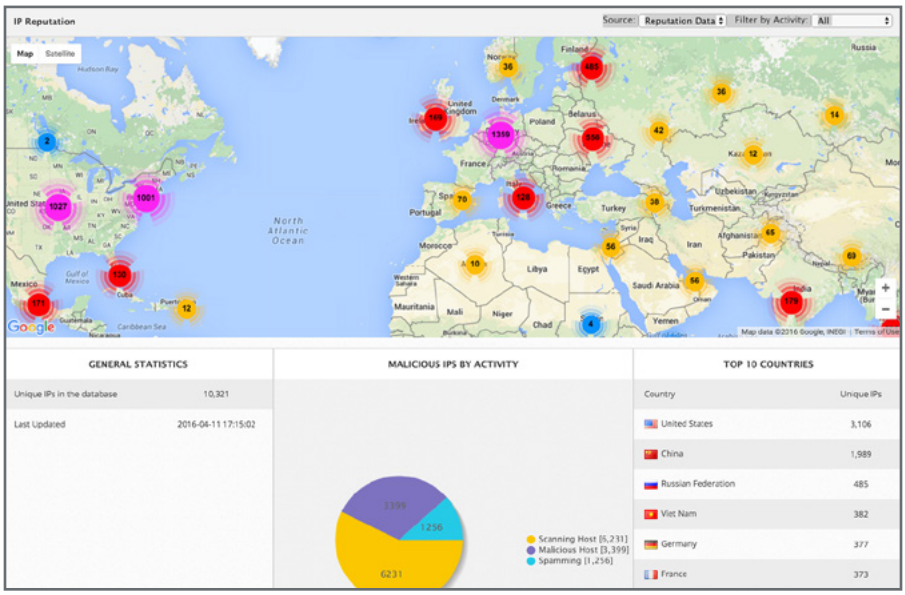

Figure 3: Open Threat Exchange Activity Map

Cybersecurity Controls Observation

FFIEC General Observation: The FFIEC asks: "What is the process for determining and implementing preventative, detective, and corrective controls on a financial institution's network?" The answer is that the process should include review to assess controls across assets and adapt to changes in the environment. An easy example to point to is asset inventory and vulnerability management. What (and where) are the assets and what vulnerabilities are present? For example, keeping an accurate inventory of endpoints and any vulnerabilities which may exist as well as their connectivity to and from networks is important for threat management. From here, organizations are expected to prioritize and reduce risk where it has the greatest potential for negative impact.

AlienVault USM Capabilities: The USM platform contains five essential security controls, all managed from a single management console:

- Asset Discovery
- Vulnerability Assessment
- Intrusion Detection
- Behavioral Monitoring
- Security Intelligence & Event Monitoring (SIEM)

These built-in, essential security controls and threat intelligence eliminate the need to deploy security point products and conduct independent threat research.

Look no further than the 2015 Verizon data breach investigations report (DBIR) to understand that "ten CVEs account for almost 97% of the exploits observed in 2014". With the asset discovery and vulnerability management capabilities built into USM, organizations can perform authenticated or unauthenticated scans to identify and prioritize vulnerability remediation. Teams can then take appropriate action to remediate their organization's greatest vulnerability risk and validate its success. Companies frequently get distracted focusing on the "next big thing" like Internet of Things (IoT) news, when in reality more time and attention should be dedicated to vulnerability management of systems and applications which are currently more likely to be attacked. Figure 4 shows an example of asset inventory and vulnerability management in USM.

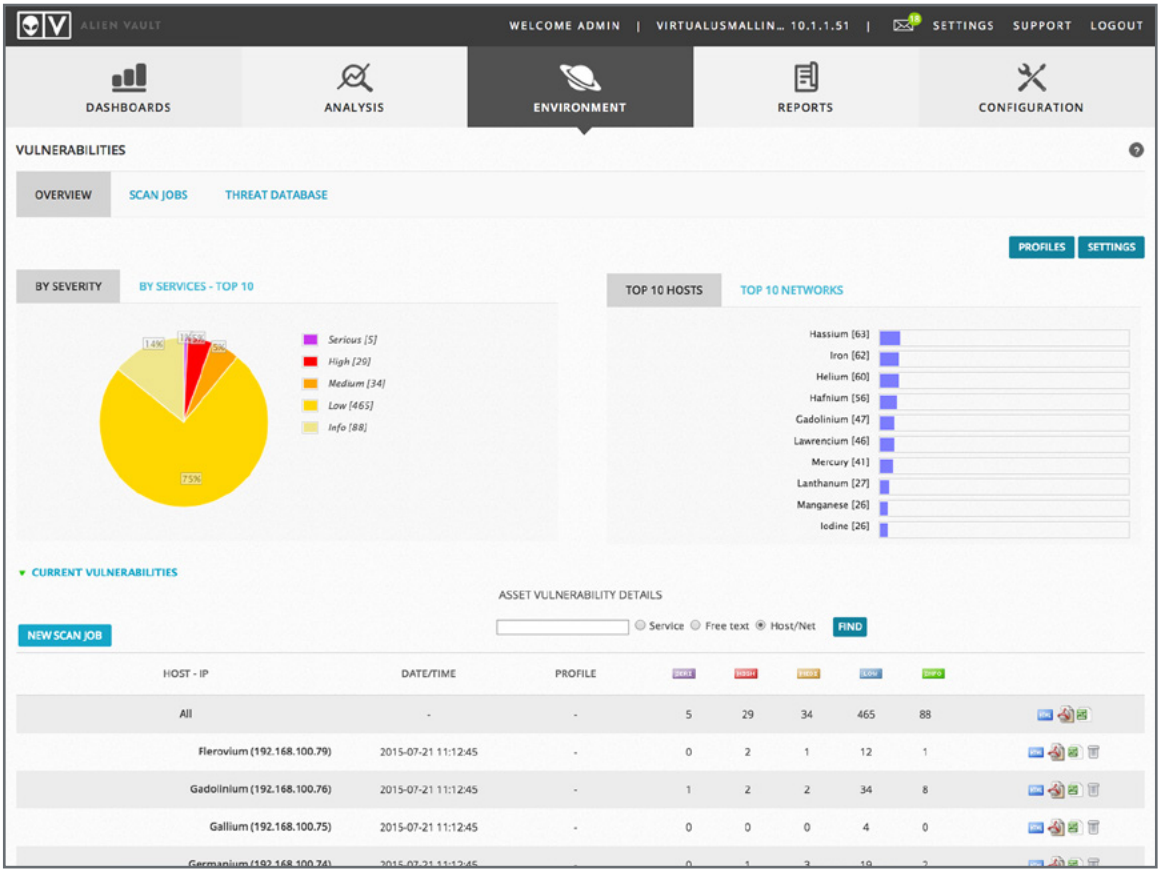

Figure 4: Host and Network Vulnerability Management

External Dependency Management Observation

FFIEC General Observation: External dependencies such as third-parties, business partners, customers, and financial service providers (e.g. loan origination solutions, payment processors, bank wires) can be an important source of risk. Every connection is an extension of the internal business, however an organization has much less direct control over external entities unless contractual language is in place. In other words, these dependencies can be the source of an incident. If and incident does occur, the financial institution still must manage the breach response.

AlienVault USM Capabilities: The USM platform's core capability is the analysis of activity across the network, including connections made to and from the network as highlighted previously. The advent of cloud computing and service providers has enabled businesses to create new services in a short period of time without any help from IT. USM's baseline collection can provide reporting on trusted connections and newly created relationships to identify sources of risk which may not have a solid process behind them. For example, VPNs, file transfers, back up sites, and managed services where the connection originates from outside of the company and terminates on the network (i.e. HVAC remote monitoring) are just a few. Figure 5 shows USM's capability to identify, group, prioritize and report on activity across the network, based on the attacker's intent.

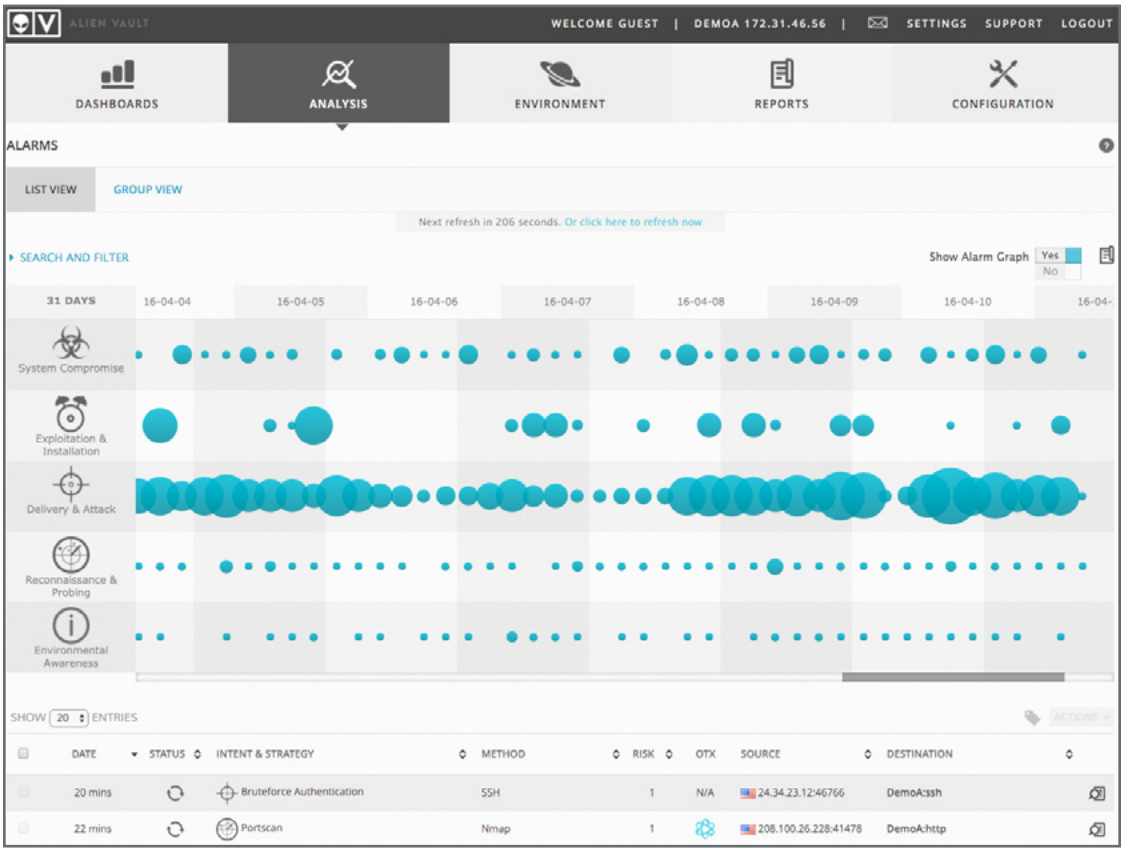

Figure 5: Network-wide Reporting of Suspicious Activity in the Kill-Chain Taxonomy

Cyber Incident Management and Resilience Observation

FFIEC General Observation: The FFIEC indicates, "cyber incident management involves incident detection, response, mitigation, escalation, reporting, and resilience." The statement sums up the expectation and the realization that incidents will occur. One parallel to incident management and resilience could be drawn to how disaster recovery and business continuity planning (DR/BCP) has traditionally been looked at. The resiliency component expects the business to be able to recover and operate the business when interruptions occur. Just like with DR/BCP, there's an understanding that at some point events will occur and the business must be able to identify and gain control of the situation so the business can still operate. Depending on the expertise of the personnel within the company, the ability to identify and recover may require an incident response retainer or professional services. Likewise, testing the ability to recover is an important aspect that should involve organizational leadership to ensure expectations are in line with what is most critical for systems and data recovery.

AlienVault USM Capabilities: The ability to detect network and endpoint incidents is a core competency of AlienVault USM. With data available from raw network log analysis and anomaly detection, along with correlation of security events from vulnerability assessments, IDS, file-integrity monitoring (FIM), and service availability monitoring, USM brings together the key data needed for effective incident detection, alerting and response.

This data is incredibly valuable and streamlined into a central repository to enable incident response teams to quickly limit the damage from an incident. Also, organizations who take part in third-party security incident response assessments can practice identification and eradication to reduce the dwell time of a successful attacker. Additionally, as the business becomes more focused on security, this data can be used in management and stakeholder tabletop exercises to identify gaps and set expectations around incident handling. Figure 6 illustrates host intrusion detection-based events built into USM.

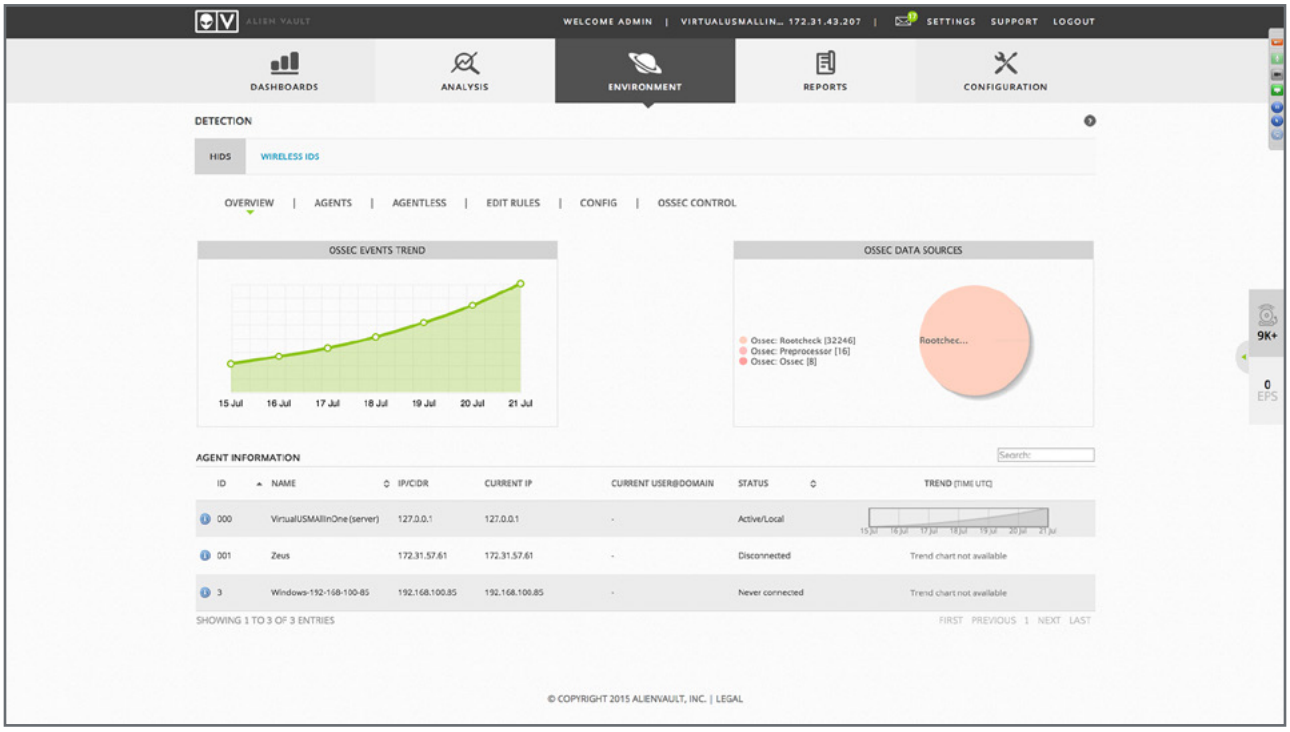

Figure 6: Intrusion Detection Activity

Beyond the FFIEC Observations

AlienVault provides additional capabilities designed to graphically map out risk areas and align with compliance requirements. AlienVault USM offers report templates designed for compliance requirements such as PCI and ISO 27001, in addition to the ability to create custom reports tailored to specific needs. The built-in reports can provide views of network connections, endpoint activity, compliance posture, vulnerabilities, vendor products, metric data, and dozens of other data views.

At a time where there is no shortage of security products on the market and with the landscape showing no signs of slowing down, security teams are looking for holistic solutions which do not take an entire security operations center (SOC) to manage. Advanced malware detection, vulnerability management, threat intelligence, and robust logging are required. AlienVault provides a powerful solution at a price point that is affordable for even small- to mid-sized organizations.

About the Authors:

Patrick Bedwell

Patrick Bedwell has 17 years of experience in the network security and network management industries. He is the Vice President of Product Marketing at AlienVault, responsible for creating and executing the go-to-market strategy for AlienVault's Unified Security Management products. Previously, Patrick was VP of Product Marketing at Fortient and has held product marketing and product management leadership positions at Arcot Systems, McAfee, SecurityFocus, Network ICE and Network General. Patrick earned an MBA with honors from Santa Clara University and a BA degree in English from the University of California, Berkeley.

Mike Saurbaugh

Mike Saurbaugh has spent nearly 20-years in financial services and for more than 12-years was the head of information security. Mike is a Faculty member with IANS Research, Research Director at securitycurrent, course developer and adjunct faculty at Excelsior College, and independent consultant with First Security Alliance, LLC. In technical and leadership roles, Mike has held positions in information security, eCommerce, technical operations and technology services. Mike has led and implemented security projects for online banking, PCI, SIEM, threat intelligence, data loss prevention, web security gateway, intrusion prevention, change management, vulnerability management, security awareness, and social engineering programs. Mike holds a Master of Science in Information Assurance from Walsh College and is an information security curriculum advisory committee member at two colleges. Lastly, Mike has advised stealth and up-and-coming security startups, and frequently conducts public speaking engagements in security.