AREA 1

splunk>

AREA 1 SECURITY & SPLUNK SOLUTION BRIEF

Integrated solution enhances phishing attack visibility and strengthens defense

Area 1 Horizon anti-phishing service detects and blocks phishing attacks

When integrated with Splunk, security teams can:

- Get deep insight and visibility into phishing email detected and blocked by the Area 1 service
- Quickly and effectively uncover related advanced threat activity organization-wide
- More efficiently investigate and respond to incidents
- Provide visibility into threat actor behavior and trends
- Facilitate and customize threat reporting

PHISHING ATTACK VISIBILITY AND DEFENSE

Phishing is the threat that most often breaches cybersecurity defenses. One of the biggest challenges that security teams face is how to quickly, effectively detect and respond to phishing attacks and minimize damage. Fortifying a Splunk deployment with early visibility to new phishing campaigns and infrastructure helps security teams more effectively find and defend against phishing attacks.

INTEGRATE AREA 1 SECURITY WITH SPLUNK TO IMPROVE PHISHING DETECTION AND ACCELERATE RESPONSE

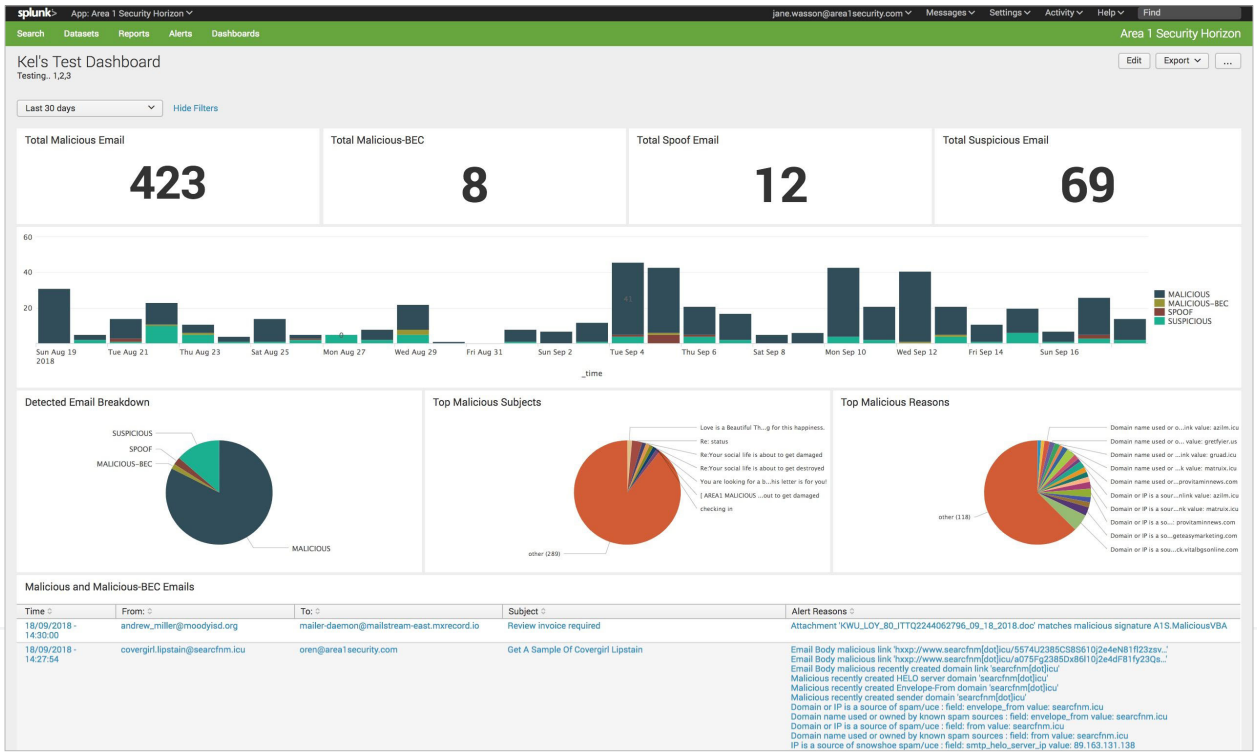
Integrating Splunk with the Area 1 Horizon anti-phishing service provides early, in-depth visibility to phishing detections. This insight into emergent phishing sites and payloads is key for detecting, investigating, and responding effectively to advanced threats.

INCREASE THE EFFECTIVENESS OF ADVANCED THREAT DETECTION

Area 1 proactively hunts for and exposes phishing campaigns and infrastructure in the wild, detecting malicious sites and payloads an average of 24 days ahead of industry benchmarks. The Area 1 Horizon™ anti-phishing service uses this early visibility, plus innovative predictive analysis techniques to add a layer of security to customer networks. This aggressively detects and blocks phishing across all attack vectors, including email, web, and network, to protect customers from cyber breaches.

By ingesting Area 1 phishing detections and threat indicators into the Splunk platform, security teams gain deep insight into attempted phishing attacks, plus early visibility into phishing campaigns and infrastructure.

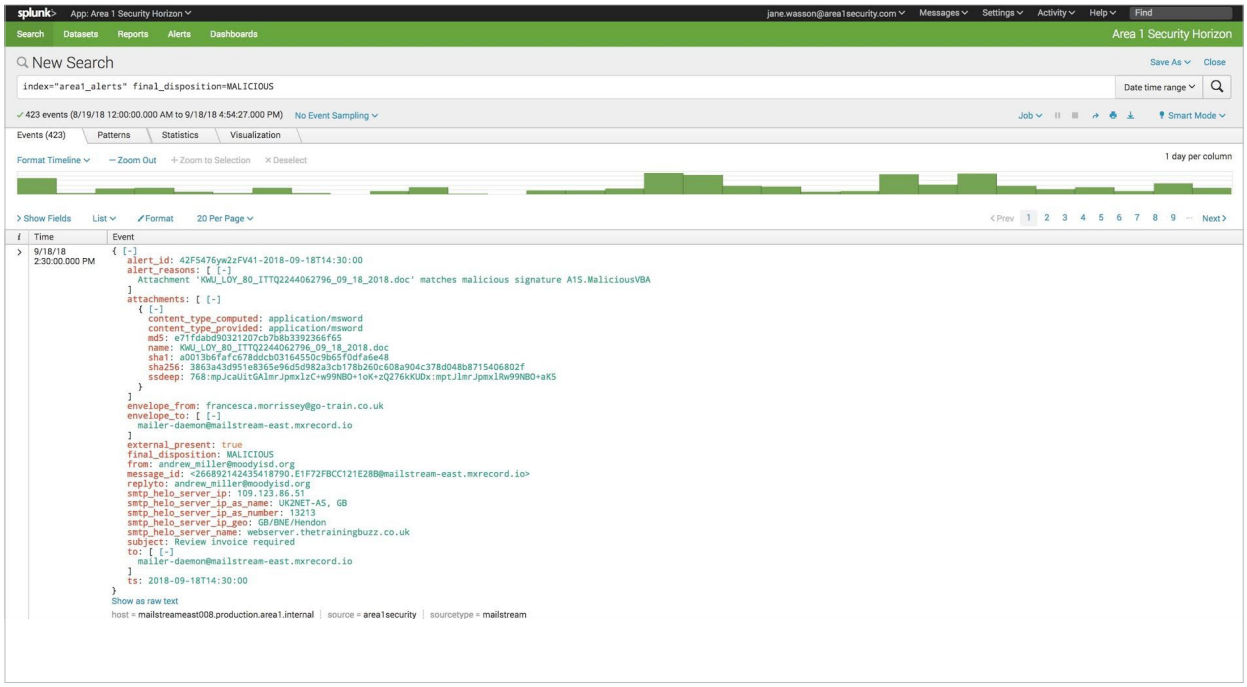
A dashboard provides an at-a-glance view of phishing email detections, including targeted users, email subject and the reason for detection. Drilling into detections reveals in-depth details regarding the attributes of a phishing email, and it's associated threat indicators. Teams can correlate the Area 1 detection information with other Splunk aggregate events to more effectively locate and defend against hidden advanced threat activity across the organization.



SPLUNK DASHBOARD FOR AREA 1 PHISHING DETECTIONS

IMPROVE EFFICIENCY OF INCIDENT INVESTIGATION AND RESPONSE

Splunk search queries facilitate uncovering the history of an incident to speed response and remediation. Because Area 1 provides early insight to phishing campaigns and infrastructure, security teams that integrate the Area 1 anti-phishing service with their Splunk platform are armed at the earliest phase of the attack cycle with the in-depth information necessary to research and remediate an incident. This also lets them more efficiently detect and prevent similar attacks. Area 1 phishing detections include threat indicators such as malicious domains, IPs, URLs, file hashes, and email addresses that can be used to investigate attacks and configure security policies to prevent follow-on incidents.



SPLUNK DRILL-DOWN FOR AREA 1 MALICIOUS EMAIL DETECTION

In-depth and historical information for threat indicators includes threat type, threat actor if known, domain WHOIS information, timestamps of indicator discovery, and other items associated with the indicator, such as malicious URLs and files. Using the Area 1 threat indicators and the Splunk query function, security teams can uncover additional users or systems that may have interacted with malicious domains, IPs, links, or downloaded malicious files. Queries can also identify any related lateral breach activity. The integration of Area 1 detections and threat insight with Splunk helps security teams more efficiently investigate and respond to a breach.

Also, when the Area 1 Horizon service integrates with the Splunk platform, if a malicious email is detected by Area 1, the email content can be accessed via Splunk as needed for further investigation or to retain for evidence.

VISIBILITY INTO THREAT ACTOR BEHAVIOR & TRENDS

Area 1 Security tracks threat actors and provides in-depth information about their activity. This includes real-time visibility into attack campaigns and infrastructure, who the targets are, and how and when they attack.

Integrating the Area 1 service with Splunk adds continuously updated threat actor information. This helps security teams visualize threat activity, motivations, and techniques to stay current and better understand and defend from attacks.

CONSOLIDATE REPORTING

By integrating the Area 1 Horizon service with Splunk, security teams can report on real-time and historical phishing attack activity. The team can use a common, familiar interface and easily include phishing attack detection and threat indicator data in reports, such as weekly or monthly roll-ups of significant events or weekly metrics.

ABOUT AREA 1 SECURITY

Backed by top-tier investors, Area 1 Security is led by security and data analytics experts from NSA, USCYBERCOM, Cisco/IronPort and FireEye, who realized the pressing need for a proactive solution to targeted phishing attacks. Area 1 Security is working with organizations that implement the most sophisticated security infrastructures. These companies include F500 banks, insurance providers, retail organizations, and health care providers. Our mission is to preempt and stop targeted phishing attacks at their very outset and significantly improve the customer's cybersecurity posture.

To learn more, please visit www.area1security.com.

ABOUT SPLUNK

Splunk Inc. (NASDAQ: SPLK) turns machine data into answers. Organizations use market-leading Splunk solutions with machine learning to solve their toughest IT, Internet of Things and security challenges.

Join millions of passionate users and discover your "aha" moment with Splunk today: www.splunk.com.