Solution Showcase

Enterprise-class Network Security Analytics

Date: July 2016 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: Enterprise CISOs face a true conundrum. Traditional security technologies like antivirus software, firewalls, and SIEM are no longer adequate for preventing, detecting, and responding to security incidents, but many organizations remain perplexed about what to do to combat this situation. New and innovative security analytics tools have great potential but organizations are still unsure where they should be applied. Based upon ESG research, leading enterprise organizations understand that networks act as a common denominator for cyber-adversaries, so they tend to start by collecting, processing, and analyzing massive amounts of network security telemetry in order to improve cybersecurity efficacy and efficiency. Arbor Networks can help here with a combination of Spectrum network security analytics and ATLAS threat intelligence.

Overview

According to ESG research, 67% of IT and cybersecurity professionals working at enterprise organizations believe that the threat landscape has gotten worse over the past two years.[1] This belief is based upon a number of factors including:

- **An increase in targeted attacks.** In the past, most security attacks were based upon broad-based phishing scams, Internet worms, or generic viruses. These attack vectors persist, with the discovery of more than 1 million malware threats. This volume masks the fact that an increasing number of these malware attacks target a single organization in order to penetrate their networks, compromise systems, and conduct what's come to be known as an advanced persistent threat (APT) that can ultimately result in data exfiltration and massive damages.
- **Highly-visible data breaches.** The parade of publicly disclosed data breaches continues unabated. According to the privacy rights clearinghouse (privacyrights.org), there have been 94 data breaches in 2016, exposing nearly 3 million records. Organizations breached in 2016 include MySpace (over 360 million records), Equifax (431 thousand records), and beautifulpeople.com (1.1 million records). There is no reason to believe this situation will improve anytime soon.
- **Day-to-day experience with security incidents.** In a recent ESG research survey, 68% of the enterprise organizations surveyed had suffered one or several security incidents over the past 24 months. These security incidents had numerous ramifications—47% of those organization said that a security breach required significant IT time and personnel for remediation activities, 36% said that a security breach had disrupted a business process or critical operation, 36% admitted that a security breach caused disruption of a business application or IT system availability, and 33% claim that a security breach resulted in lost productivity.[2]

[1] Source: ESG Research Report, *Cyber Supply Chain Security Revisited*, September 2015.
[2] Source: Ibid.

Why Consider Network Security Analytics?

Enterprise CISOs recognize that their organizations are under constant attack and are adjusting their cybersecurity strategies in response. For example, 70% of organizations are increasing their cybersecurity budgets in 2016.[3] Many firms are also bolstering prevention controls and exploring security analytics solutions to improve incident detection and response. Unfortunately, security analytics solutions often come with limited functionality or excessive overhead:

- **SIEM depends upon rule sets and staff resources.** SIEM systems were originally designed to collect, filter, and correlate log events from security and networking devices. This limits their effectiveness because:

  1. Log data provides information about individual nodes but it can be difficult or even impossible to trace activities across the network from Layer 2 through 7.
  2. SIEMs may ignore and throw away valuable historical data that could be needed for future cybersecurity investigations.
  3. Log data is one of many sources that can be used for security analytics. While some SIEMs interoperate with other data sources, there is little actual coordinated data analysis.

  SIEM systems were designed to churn through event data, map event data to custom rule sets, and then generate alerts for investigation. Unfortunately, this can be a time-consuming process that depends upon security analysts' familiarity and experience with SIEM tools. It also limits what they can do in terms of ad-hoc queries as part of security investigations.

- **Endpoint threat detection and response (ETDR) solutions can require ample time and advanced skills.** Some highly sophisticated organizations overcome the limitations of SIEM by collecting, processing, and analyzing endpoint behavior using ETDR tools. While this strategy can be effective, it minimizes the utilization of useful network security telemetry. Furthermore, ETDR projects can be extremely labor-intensive, requiring months to roll-out and fine-tune. Finally, ETDR requires advanced skill sets in areas like security analytics and forensics that many organizations simply don't have.

- **Threat management gateways can lack the right level of context.** Many organizations use an assortment of disconnected point tools and gateways (secure web gateways, NGFW, sandboxing) to block and detect exploits and malware on networks and systems. While these tools may provide incremental value, they tend to lack the right telemetry and intelligence to put individual security events into a broader context that can be used to piece together the history and scope of cyber-attacks. In truth, effective threat management demands a more holistic viewpoint across the entire network.

One way to overcome these limitations is to begin efforts around security analytics with a focus on the network. Why networks? As the old security saying goes, "the network doesn't lie." Regardless of the cyber-adversary, exploit technique, or malware variant, cyber-attacks flow across the network. Armed with the right network telemetry, security analysts can detect anomalous behavior and piece together the clues that indicate malicious activity in progress. It is ESG's observation that many highly regulated security-conscious organizations tend to invest in network security analytics projects before moving onto other areas.

[3] Source: ESG Brief, *2016 Cybersecurity Spending Trends*, March 2016.

Key Capabilities of Network Security Analytics Solutions

While network security telemetry can help organizations detect cyber-attacks at any phase of the APT "kill chain," CISOs must carefully assess network security analytics tools and choose solutions that provide comprehensive functionality to help them address growing cybersecurity requirements. ESG believes that the best network security analytics systems will offer:

- **Comprehensive network visibility.** Enterprise networks span across geographies and multiple tiers. As such, network security analytics should be able to collect, process, and analyze traffic at critical junctions across the network. Leading tools will do this by monitoring NetFlow/IPFIX telemetry while offering full-packet capture (PCAP) capabilities. By collecting, processing, and analyzing these types of network telemetry across the network, organizations have access to a record of every network connection, flow, and session that can help them detect attacks, piece together sequences of events, and prioritize where to point their scarce resources. It is worth noting that collecting and processing network telemetry for real-time and historical analysis depends upon a modern, scalable, and distributed architecture for data management and ample performance.

- **Tight integration with threat intelligence.** Aside from internal data derived from network traffic, network security analytics should be tightly integrated with threat intelligence feeds in order to compare enterprise network behavior with malicious "in-the-wild" activity. When a host suddenly reaches out to an unknown host, threat intelligence integration can help security analysts assess whether this is benign or suspicious behavior. The best threat intelligence will supplement basic indicators of compromise (IoCs) data points about malicious IP addresses, domains, and URLs, with detailed knowledge about the tactics, techniques, and procedures (TTPs) used in cyber-attack campaigns. Armed with this knowledge, security professionals can sort through massive amounts of network traffic to detect kill-chain actions based upon connections, packet metadata, or payloads. Threat intelligence can also be helpful for "hunters" who proactively look for signs of cybersecurity trouble.

- **An assortment of built-in analytics for anomaly detection**. These policies should also be applied to real-time telemetry to detect attacks in progress and historical data for retrospective remediation. Aside from native algorithms, the best network security analytics tools will allow users to develop custom rule sets to detect things like insider attacks or "low-and-slow" attacks on network-connected operational technology systems like HVAC equipment, manufacturing robots, or programmable logic controllers (PLCs).

- **Strong visualization and investigation capabilities.** In addition to detection, data visualization and underlying analytics must also be employed to tie detection to validation of the threat in the network. This includes workflows and built-in templates to quickly detail the timeline and exact connection points between the detected threat and activity in the network. For example, you must be able to confirm the malicious source, which hosts were involved, if/how it moved laterally throughout the network and finally, the connections to the external source via command & control interaction.

- **Role-based usability.** The best network security analytics should support a variety of cybersecurity roles and skill sets—from a junior SOC analyst tasked with triaging security alerts to highly experienced incident response personnel responsible for security investigations. This depends upon strong visual analytics tools to help analysts look at the data in a number of ways so they can spot anomalous needles in nonthreatening haystacks. It also depends upon the ability to query mountains of data while receiving high-performance responses.

- **Operational efficiency.** Too many threat investigation tools are homegrown, hard to use, and very time consuming and expensive to deploy. Storage and archiving requirements can expand dramatically after initial implementation, adding unexpected costs. Leading network-based approaches can be easy to deploy and operate in days, not months,

providing real value in a short timeframe. Advanced data collection and management methodologies enable deployments to scale readily without additional investment. Traffic analytics, data visualization, and intuitive workflows also make the network-based approach more easily embraced by the broader security organization.

Arbor Networks Spectrum

Best known for its leading DDoS products and services, Arbor Networks' Spectrum solution aligns well with the enterprise-class network security analytics functionality described above:

- Arbor Spectrum can collect, process, and analyze NetFlow/IPFIX and PCAP data to provide comprehensive visibility from L3 through L7 of the network stack. Furthermore, this information is presented to analysts through a visual analytics interface, enabling them to investigate, hunt, and pivot through vast amounts of network telemetry.

- Tight integration between the platform and Arbor's global visibility with ATLAS threat intelligence with native network telemetry to help analysts detect, visualize, investigate, and prioritize the most dangerous threats. ATLAS goes beyond basic IoCs, providing the SOC team with threat intelligence focused on attack campaigns. This viewpoint can help analysts identify and block malicious activities earlier in the kill chain process to minimize damages.

- Arbor Spectrum can be installed and configured for a production environment in rapid fashion. Once installed, the interface can be customized for individual members of the security team regardless of their skills or experience. Arbor Spectrum is also built for performance and scale, capable of capturing, processing, and analyzing massive amounts of data for real-time analysis. It is also built to query large repositories of historical data in rapid fashion for security investigations.

With a history in the service provider market, Arbor Networks has lots of knowledge about building high-performance, scalable products for network security. Enterprise organizations with large distributed networks can benefit from this experience by utilizing Arbor Spectrum for their network security analytics needs.

The Bigger Truth

Many enterprise CISOs realize that cybersecurity is in a state of transition. The security technologies used to protect networks in the past are no longer adequate, but many organizations remain unsure of what to do next.

ESG believes that new and innovative network security analytics solutions have the potential to level the playing field by collecting, processing, and analyzing massive amounts of data in real time while providing analysts with data visualization and query capabilities for security investigations. These benefits lead many leading enterprises to invest and focus on network security analytics and then support these efforts with other analytics projects over time.

Arbor Networks Spectrum is designed for today's enterprise security requirements. CISOs looking for help in this area could be well-served by evaluating how Arbor can help them mitigate IT risk, accelerate incident detection and response, and streamline security operations.