Stratecast | FROST & SULLIVAN

February 13, 2015

"Big Data" Analytics in Network Security: Computational Automation of Security Professionals

Stratecast Analysis by
Frank Dickson

Stratecast Perspectives & Insight for Executives (SPIE)
Volume 15, Number 6

"Big Data" Analytics in Network Security: Computational Automation of Security Professionals

Introduction[1]

The reality of today's Internet is that cyber threats are becoming increasingly more sophisticated. In the not too distant past, cyber-attacks were executed using rudimentary and standard malicious binaries, often referred to as viruses. Defending against these early malicious binaries was effectively accomplished by signature based antivirus Web and email content filtering platforms, which would rely on an actual pattern or static image of the binary.

Cyber criminals, many of whom are sophisticated, profit-maximizing members of organized crime, looked to increase the return on the investment that they had in their malicious code. The result was that the cybercriminal community discovered that they could continuously modify the way that their malicious binaries or executables appeared, such that signatures could no longer be applied effectively. The age of polymorphic malicious binaries was born.

Polymorphism can be very complicated or very basic. Simply put, polymorphism is the modification of the way the executable looks, without executing it. If the code of the binary looks different, the signature for the code will also be different, rendering signature based defenses, such as those often included in antivirus solutions, ineffective.

The moniker that has been given to this new form of malware is advanced persistent threat (APT). In reality, APT has become an umbrella term that includes polymorphic malicious binaries and other attributes. Essentially, APTs are the result of lessons learned by malicious actors from nation-state cyber-attacks, such as GhostNet and Stuxnet. These advanced attacks can be characterized as follows:

- Utilizes a type of advanced "zero day" malware
- Evades signature-based detection techniques
- Targets or focuses on specific individuals or organizations
- Aims to achieve a monetary or intellectual property gain, run like a business with a return on investment (ROI) objective
- Looks to penetrate and persist in an environment (network or endpoint)

In this SPIE, we discuss the role of signature based defenses in this new APT reality. We also discuss behavioral-based cyber defenses. Finally, we delve into one form of behavioral cyber defense: advanced security analytics.

---

[1] In preparing this report, Stratecast conducted interviews with representatives of the following companies:

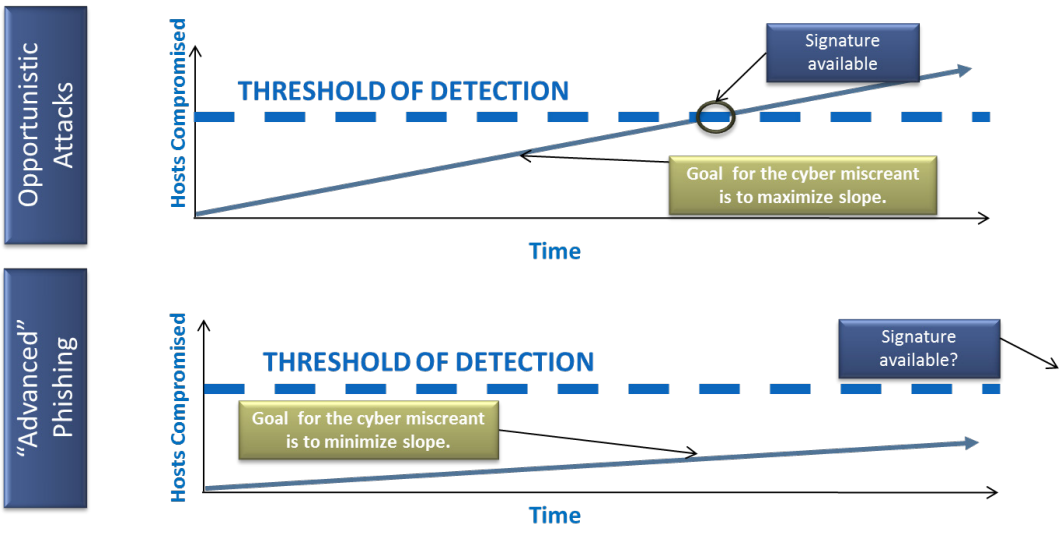
- Bit9/Carbon Black – Jeffrey J Guy; Director, Product Management
- Cisco – Bryan Palma, SVP Cisco Security Solutions
- Dell SecureWorks – Mark Wood, Director of Product Management
- IBM – Vijay Dheap, Global Product Manager - IBM Master Inventor, Big Data Security Intelligence & Mobile Security

Please note that the insights and opinions expressed in this assessment are those of Stratecast and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

Limitations of Signature-based Defenses

Traditional antivirus software is best used to combat opportunistic (untargeted) attacks, offering effective and efficient protection, following the creation of a signature. With "advanced" targeted "spear" phishing type attacks, cyber miscreants are selective with whom they target, saving the best advanced attacks for select targets. Thus, a malicious binary may not compromise enough hosts to hit the "threshold of detection" of the security companies that write signatures. Thus, there is a gap in protection.

Exhibit 1: The Use of Signature-Based Defenses in Opportunistic and "Advanced" Phishing Attacks



Source: Bit9/Carbon Black

Contrary to the hype, anti-virus is not dead. Traditional signature based defenses are effective tools to be use in a *set* of tools to provide security for endpoints. Using a combination of all the relevant technologies provides the highest possible level of security. Taking a "binary" approach that any one security tool is either 100% effective or 0% effective is folly.

Behavioral Cyber Defense

A different approach needs to be taken to address polymorphic APT attacks. The security community has responded with a completely different way of thinking as it relates to cyber defense—a complete paradigm shift, if you will—being proactive rather than reactive. The new thinking is to take a behavioral approach to detecting malware. Instead of trying to detect malware based on what it is (signature based), behavioral malware detection relies on what the malware does. For example, if the first action taken by an executable file is to modify or disable a notebook computer's Microsoft security center, this is a strong

The new thinking is to take a behavioral approach to detecting malware. Instead of trying to detect malware based on what it is (signature based), behavioral malware detection relies on what the malware does.

indicator that the executable is a malicious binary. The malicious executable would ideally then be quarantined, and security personnel notified. Sandboxing and the application of "big data" analytics to malware detection, as discussed next, are innovations resulting from this fundamental rethinking.

Sandboxing

The basic idea of sandboxing technology is to create an analysis environment in which a suspicious program is executed and the behavior of the program is observed, noted, and then analyzed in an automated manner. This approach is more effective than just looking at the appearance of the executable, because sandboxing goes beyond just the mere appearance of the binary, and observes what the binary does; and, therefore, it is much more conclusive in determining if an executable is malicious.

The same process or approach has occurred for JavaScript. Malicious JavaScripts that would compromise browsers via drive-by downloads are being identified by signatures. Cyber miscreants have therefore added obfuscation and polymorphism into the JavaScript exploit tool kits, to exploit vulnerabilities in browsers and browser environments.

In order to get around the problem of obfuscating, polymorphic JavaScript, a form of sandbox called "honey clients" was developed. Honey clients are browsers or programs that pretend to be browsers. The honey client executes suspicious JavaScript, and collects and analyzes the behavioral details in order to determine malicious activity. For example, if the JavaScript starts allocating incremental blocks of memory with the same structures, this behavior could be indicative of a heap spray attack. Therefore, maliciousness can be detected without a signature.

Network sandboxes, although powerful, are not a magic bullet. The cybercriminal community has not remained complacent. As sandboxing technologies have become more popular as a form of protection for enterprise networks, cyber miscreants have developed evasive binaries. These binaries use a number of techniques to identify if they are being analyzed in a sandbox, and will either stop executing completely or perform some benign action that seems irrelevant so that the sandboxes cannot detect the evasive binary as malicious.

"Big Data" Analytics

Another behavioral method of APT detection is the application of "big data" analytics to network security. Essentially, possible breaches are identified by detecting anomalous or suspicious activity on the network. For example, correlating traffic patterns to activity is one way to look for anomalous behavior. Establishing baselines for events coming from an IP or MAC address, and noting unusual application use or bandwidth is another way to detect anomalies.

In fairness, describing this methodology as "big data" analytics may be a bit sensationalized. Big data concepts have been part of security in several disciplines before the term "big data" was coined, as would likely be argued by many security professionals.

In fairness, describing this methodology as "big data" analytics may be a bit sensationalized. Big data concepts have been part of security in several disciplines before the term "big data" was coined. New concepts and principles are being applied, but seasoned security professionals would correctly argue that many of the activities are evolutionary rather than revolutionary. "Advanced analytics" may be a more appropriate term, so that term will be used for the remainder of this SPIE.

Advanced Security Analytics

An overly simplified description of advanced security analytics can easily be provided. Network and security log data is fed into a database and analysis platform, and combined with network flow and endpoint telemetry data. Covert and unknown malicious binaries are illuminated though the application of advanced analytics, which are directed by insights from security intelligence, identifying and investigating the questionable. Security intelligence, as the term is used in this discussion, refers to information received from a service or function that analyzes the cyber threat landscape *external* to the organization's network environment; and that provides in-depth information on emerging threats (such as malware, viruses, trojans, adware and other Internet security threats), zero-day vulnerabilities, and new exploit techniques. Exposing unknown malicious activity in the network utilizes three key methodologies:

- Anomaly Detection – Monitor network traffic, establish a baseline of what is normal, and detect anomalous traffic that is indicative of malicious activity
- Behavioral Analysis – Analyze traffic for known behaviors that indicate improper activity
- Flow Data Comparison – Monitor traffic flows for activity that is not congruent with legitimate known good patterns

This simplified description necessarily discounts the complexity of implementing and operating these advanced analytic solutions. By comparison, dieting (in order to lose weight) is conceptually simple: a person who consumes fewer calories than are burned loses weight. Needless to say, the implementation reality of serious weight loss is exponentially more difficult. Advanced security analytics is much the same.

Analytics = Computational Automation

Advanced security analytics is the automation of learned processes from skilled security personnel by powerful computational platforms. Analysts (humans) have the ability to use both inductive and deductive processes intuitively. Achieving that same result from analytics software requires that the software be programmed and taught, by humans, to perform certain operations. Simply put, analytics does not create; it automates. Think of it as digitizing a cyber-security playbook.

Simply put, analytics does not create; it automates. Think of it as digitizing a cyber-security playbook.

By thinking of security analytics as a form of computation automation, the "mystique and mystery" around advanced security analytics is removed. The process is illuminated to be security analyst (human) centric:

1) Search

   Search is the most basic step. Search allows the analyst to begin exploring and discovering the unknown. The first step in finding a solution to any unknown problem is search. The ability to search network and security data, either in the case of a suspected breach or after a breach has been detected (forensics), is a universal need for IT departments of all sizes.

   Historically, security professionals used Grep. Grep is a command-line utility for searching plain-text data sets for lines matching a regular expression. Originally developed for the UNIX operating system, grep principles are used for any command-line interface.

The problem with search is that it is manual and time consuming. Search is also cumbersome in that several correlations have to be considered. A search can start with comparative analysis of traffic flow, behavioral analysis, and analysis of which applications are being run. Standardization creates efficiency.

2) Reports

With problem solving success, repeatable queries become standardized reports. For example, who are the top talkers and who are the users? Viewed correctly, reports may identify patterns that require further investigation. Pattern detection is what is required.

Pattern detection can be brittle, though. Regularly used expressions (regex, regexp, or rational expression) can change. The current malady facing signature based defenses like traditional antivirus is that the signatures (or malware patterns) are constantly morphing as cyber security professionals combat an active adversary.

3) Heuristics

Once predictable patterns of compromise have been discovered, standardized approaches can come into play. These standardized approaches become rules.

Rules become the mechanism for depicting and automating rule engines. Rule engines are implemented to apply the rules (heuristics) optimally, allowing for greater portfolio of rules. Rules engines take analysis to the next level, enabling the analytics platforms that finally automate the discovery of malware. The more powerful the rules engine, the more correlation is achieved.

Several conclusions easily arise:

- The more powerful the rules, the more effective the analytics
- The greater the number of rules, the more effective the analytics
- The greater the computation power of the analytics platform, the more effective the analytics

By chaining rules together, synergies are created. For example, by chaining rules, an IT team can greatly reduce false positives and false negatives.

4) Algorithms

In security analytics, algorithms are the mechanisms that move analytics from being manual to automated, "weaponized analytics." Algorithms can blend data, processing power, and custom rules to achieve greater effectiveness and efficiency. Examples include machine learning and behavior anomaly detection.

Algorithms have to be tuned and tested for maximum efficacy in specific environments. For example, the Holt-Winters algorithm applies exponential smoothing to time series data. Time-stamping is important because data can be spoofed, and a time stamp creates an indelible aspect of an event.

5) Custom analytics

Standard analytics provide an effective starting point. However, analytics also need be to tuned and optimized for individual networks. Proprietary data sets may be used that are unique to individual companies, such as identity and access management data or DNS records, or even Twitter or Facebook data. Predictive and statistical analytics are involved. If an incongruity

involving the end-user, application, or traffic pattern occurs, an alarm can be sounded. The key to custom analytics is finding the unique data sets, analytic algorithms, and alerts that provide the optimal predictive analytics for the individual organization.

It's a Process

As can be inferred by the preceding discussion, advanced analytics is a process. Constant work needs to be done to increase the effectiveness of the analytics.

Constant refinement would be necessary even if the cyber environment were static. However, cyber miscreant actors never remain static. They are always improving; always trying new methods. Analytics solutions need to adjust constantly in order to continue thwarting the evolving cyber-attacks.

Implicit in the process is the value of the feedback loop. Information sharing throughout the process enables maximum translation of trained human deductive reasoning into automated analytic algorithms and processes.

The Practical Application of Advanced Analytics in Security

As in all analytics, tremendous importance is placed on selecting the correct datasets. Not all data yields similar results. Not all data sets incur similar costs.

Almost all security analytics solutions begin with log data. Log data—which comes from firewalls, intrusion detection and prevention systems, networking equipment, security software and other sources—is rich in value, and is plentiful. Also, most companies already maintain log data solutions, such as log management, for compliance purposes.

Network Flow Data

Network flow data provides another layer of value. An apt descriptor of flow analytics data is traffic metadata. This metadata allows for network anomaly detection and application layer (layer 7) anomaly detection.

Flow analytics allow better network visibility by correlating log data with flow analytics. Breaches like the one at the NSA have given rise to complaints that log data can be tampered with or modified. Flow analytics is one method that allows security professionals to determine if log data has been compromised.

Additional value can be created by importing other data sources. Vulnerability management and risk management systems are additional systems that provide meaningful data to augment flow analytics.

Full PCAP

The next step is to extend network security analytics to include full packet capture data (PCAP). Essentially, full PCAP utilizes an application programming interface (API) to allow network devices to deliver network traffic data to the analytics application. Full PCAP captures all Ethernet/IP activity, as opposed to filtered packet capture that only captures a defined subset of traffic data such as IP address, MAC address or protocol. As it is often difficult to know which attributes are going to aid in identifying future malware activity, full PCAP provides rich data for network forensics and analytics.

Given the rich data available in full PCAP data, indicators are necessary to make analysis efficient and effective. Inconsistencies from network flow data provide clear indications that payloads need to be examined, and which payload variables need to be further explored. The forensic value of the full PCAP payload can be critical in understanding the true nature of cyber-attacks.

However, utilizing full PCAP has a down side. The rich data comes with significant cost in the form of storage requirements and the skilled professionals needed to manage and utilize such data. As a result, before augmenting advanced analytics with full PCAP data, a thorough plan needs to be in place to maximize the return from the investment.

Illustrative Advanced Analytics Examples

Several examples of companies that have implemented advanced analytics solutions in various manners are included in this section. Based on these examples, lessons learned will be presented.

Cisco Managed Threat Defense

On April 22, 2014, Cisco introduced Managed Threat Defense, an on-premises managed security solution, comprised of hardware, software, security intelligence and analytics designed to monitor, capture, and analyze threats. This solution protects by capturing real-time streaming telemetry, and leverages Cisco's network of Security Operation Centers. A dedicated security team customizes the service to meet customer needs, and provides incident analysis, response, escalation, and remediation recommendations. Equally as important, the intelligence is not only provided to detect cyber-attacks but is also applied to prioritizing alerts, allowing security professionals to effectively apply their scarce time to the most critical threats. Customer data remains within customer data centers, allowing them to maintain control at all times. Additionally, as a managed service that provides incident tracking and reporting via a subscription-based business model, companies are able to move capital expenses associated with providing security to predictable operational expenses.

The Cisco approach utilizes the latest Hadoop enhancements to apply predictive analytics to detect anomalous patterns against each customer's unique network profile, thereby determining suspicious behavior. Flow-based security monitoring provides data such as bandwidth, application performance, and network utilization to augment traditional security data.

Managed Threat Defense is enabled by Cisco security technologies, including those developed in-house and others that Cisco has acquired. These technologies include ThreatGRID for context-driven analytics, Cisco Advanced Malware Protection, Sourcefire FirePOWER for threat detection, Cisco Cloud Web Security for email and Web content security, and network security products such as firewalls and intrusion prevention systems.

Dell SecureWorks Advanced Endpoint Threat Detection

Dell SecureWorks has taken an innovative approach of combatting advanced threat actors not only at the network perimeter but also at the endpoints. The approach begins with two key inputs: endpoint sensory information from a lightweight, "always-on" client from Bit9/Carbon Black; and threat intelligence from Dell SecureWorks' Counter Threat Unit. The resulting Advanced Endpoint Threat Detection (AETD) service provides clients with early warning of possible endpoint compromise, innovative and complete insight into the security posture of their endpoints, and provides opportunities for security teams to accelerate incident response efforts and disrupt miscreant efforts sooner in the "kill chain." A kill chain describes stages of a targeted cyber-attack.

AETD utilizes the endpoint sensors to collect telemetry about endpoint state such as file system changes, registry changes, network connections, binary executions, and execution events. The sensors provide the telemetry data to an analytics console, where Dell SecureWorks Counter Threat Unit endpoint intelligence and other intelligence feeds are applied to detect potential threats on endpoints based on compromise patterns. Alerts are escalated to an advanced analyst team in the Dell SecureWorks SOC for deeper investigation.

The Advanced Endpoint Threat Detection service both improves the detection of malware and makes the improved intelligence elegantly actionable for the customer's security teams. The service has three key product objectives:

- Improve security visibility, providing advanced insight sooner than most other solutions.
- Speed detection of targeted threat activity and enable earlier disruption of miscreant efforts earlier in the "kill chain."
- Reduce time and cost for resolution by providing the exact details of the compromise, and recommended steps for remediation.

Advanced Endpoint Threat Detection adds efficacy to network security by providing visibility into endpoint security posture while simplifying the provisioning of cyber breach remediation.

IBM QRadar

Historically, log data and log management have been a necessary burden for security teams to prove compliance and to initiate post-breach forensic investigations. However, information gathering is not just a passive security activity. In recent years, the reimagining of log management and SIEM capabilities has improved pre-exploit strategies, and augmented perimeter defenses. For IBM, the goal is to provide SIEM and data packet capture as part of an integrated cyber security defense approach. IBM created a distributed, multi-level architecture, and persistently integrated new technologies around its IBM QRadar Security SIEM.

The IBM Security QRadar SIEM—part of the QRadar Security Intelligence Platform that includes SIEM, Vulnerability Manager, Risk Manager and Incident Forensics—is an appliance designed to handle 20,000 events per second. The SIEM is available as both a physical and virtual appliance, which is critical in heterogeneous networks. All SIEM data is federated locally, which eliminates the possibility of a single-point failure or a bottleneck. As the customer's needs expand, IBM offers event collection, processing and console appliances to add capacity. Scaling upward, the highly distributed architecture also makes it possible for the IBM Security QRadar Risk Manager to correlate several million events of NetFlow data centrally and in real-time. QRadar Incident Forensics provides the starting point for data exploration and insight, as well as speeding up incident response.

The IBM Security QRadar SIEM provides a comprehensive topography of all endpoints on the network, including devices, servers, span ports, switches, and routers. When the topographical representation of the network is coordinated with the IBM Security QRadar Risk Manager, new capabilities result.

For example, SIEM can be used to establish baselines for events, monitor for unusual applications, and detect network and application anomalies. Another native capability on the IBM SIEM is behavioral profiling, which enables the SIEM to detect anomalous traffic activity from an endpoint,

such as a printer port communicating with a Russian IP address, or an unapproved peer-to-peer app running on the network. Under such conditions, the SIEM can send an alarm and notify intrusion detection and prevention systems of anomalous behavior. IBM calls this technology network behavior anomaly detection (NBAD). The same profiling capability is also important when new devices are added to the network. The SIEM will perform a new scan when a new server is installed. The scan will check for configuration errors, patch levels, and anomalous endpoints, based on existing log data.

Event correlation is another feature on the QRadar platform, analyzing both flow and event data. The risk management platform helps to determine threat severity based upon the maliciousness of the threat, the degree of anomalous behavior, and the value of the asset. The vision for the IBM QRadar Security SIEM is for data storage and capture to be "intelligent, integrated, and automated." The processes described can be viewed and acted on in one central console, and are transparent (automated) from the perspective of the security team.

A functional SIEM is not the result of continuous endpoint discovery. The IBM QRadar Security SIEM has an open-standard API. The IBM SIEM integrates with Active Directory and network authentication devices platforms. Leading Identity Access Management (IAM) platforms[2] can be integrated onto to The IBM QRadar Security SIEM.

Finally, the IBM QRadar Security SIEM's potential for integration is not just limited to security platforms. The IBM Big Data & Analytics platform is already leveraged to help specific market verticals like banking, healthcare, and telecommunications. Big data analytics combined with SIEM can be spun into actionable applications. IBM Navigator on Cloud is a cloud-based file sharing service, and, if integrated with SIEM, DLP processes can be automated. The IBM Enterprise Content Management (ECM) has a two decade legacy.

Q1 Labs serves as the central collocation point for information coming from QFlow sensors on global QRadar Security Intelligence platforms. Q1 Labs is not the only IBM internal integration. The SIEM is integrated with a direct feed into the IBM Security Network Protection XGS 5100 next-generation intrusion prevention system. The SIEM considers as many as five concurrent reputation feeds to see if there are new endpoints on the network, as well as feeds from X-Force IP Reputation data. Rules can be updated to include signatures from the IBM Security Trusteer Pinpoint Malware Detection Advanced Edition software.

The IBM Security QRadar SIEM can be integrated bi-directionally with traditional and next generation firewalls (NGFW), intrusion detection and intrusion prevention systems (IDS/IPS), vulnerability management (VM), SIEM, and mobile device management (MDM). The IBM Security QRadar SIEM is integrated with FireEye to provide advanced threat protection, and help fortify the sandbox technique used by FireEye. Integration with the Microsoft System Center Configuration Manager (SCCM) allows the IBM SIEM to pick up feeds from application virtualization, and from the Microsoft enterprise desktop virtualization.

The Security Analytics Value Equation

Based on the preceding discussion, value is created in a security analytics platform when talented and skilled security professionals mine relevant data feeds to discover the data points or sets that suggest

[2] Please see Frost & Sullivan Market Engineering Study, *Identity & Access Management (IAM) Global Market Analysis: IT Mega Trends Drive Growth and Opportunities in IAM Market*, http://www.frost.com/nec7.

malicious activity. That data, when combined with other data and illuminated with analytics, indicates malware. In essence, the resulting equation is simple:

$$Security\ Analytics\ Value = (Security\ Professionals)\ x\ (Data\ Feeds + Security\ Intelligence)\ x\ (Time)$$

Having represented the creation of analytics value into an equation, the resulting implications can help drive decisions. Some of the implications follow.

Product Development is Embedded in the Delivery

As was stated earlier, advanced security analytics is not a discrete product that can be delivered "in a box." Advanced security analytics is a constantly evolving service, being refreshed and improved as part of the service delivery. Product development, as a result, is often integrated as part of the delivery. Organizations that provide analytics as part of a professional or managed service have an advantage, as the analytics is constantly improved as a natural part of the delivery of services.

Some Organizations Have a Structural Advantage in Security Analytics

One third of the security analytics value equation is skilled security professionals. Clearly, the greater number of security professionals, the greater the value of analytics that can be created, assuming a standard level of execution among organizations.

Managed security service providers are dedicated to maintaining the security posture of their customers. The larger managed security services providers have organizations that exceed 1,000 employees. Scale such as this provides advantages over many security platform providers. As a result, managed security service providers have an advantage in productizing and delivering security analytics.

The SIEM providers also have scalability advantage; they just achieve scale differently. By utilizing their user community, SIEM vendors are able to leverage the combined expertise of thousands of users. The structural advantage that a company has is dependent on execution. A SIEM vendor with tens of thousands of users has little structural advantage unless it plans to utilize that user community and executes on that plan. This point may obvious, but it is worth noting.

Telecom operators, likewise, have an advantage. The advantage is not based on the number of security analysts but on the access to dats—data provided to them as the result of sitting in the catbird's seat of a backbone network. For example, Level 3 has network visibility that includes 40+ billion NetFlow sessions, 1+ million captured malicious packets and 85 terabytes of security event data, on a daily basis.

Flow-based security monitoring provides data such as bandwidth, application performance, and network utilization to augment traditional security data, enabling advanced analytics to not only block attacks but also predict them. For example, distributed denial of service attacks are preceded by "pinging and prodding" of Web sites and networks, as cyber miscreants perform pre-attack reconnaissance. The resulting digital breadcrumbs provide the foresight to anticipate attacks, and then ensure proper protection, thereby minimizing business interruptions.

Simply Connecting a Sensor to an Analytics Platform Does Not Create Value

Placing sensors within a network or on endpoints to collect rich telemetry is important, but value is not created at the moment that data is fed from the sensor to the analytics platform Data feeds are only one third of the equation. Skilled security professionals and time are the other two thirds. Skilled personnel have to be given time to create the analytics to capitalize on the value of the new data. The implication of the lesson is that there are no short cuts on the path.

To create analytics value, an organization must take a process approach. Simply "throwing money at the problem" will not provide superior analytics due the requirement of the time component. Companies that have made investments into advanced security analytics have a defendable competitive advantage as they have the benefit of time.

Companies that have made investments in advanced security analytics have a defendable competitive advantage as they have the benefit of time.

The Dell SecureWorks example is worth noting again. Its Advanced Endpoint Threat Detection service is not presented to the market as a stand-alone service. Dell SecureWorks offers the service as an addition to the Dell SecureWorks' Advanced Threat Services portfolio, augmenting its Advanced Malware Protection and Detection service and the Targeted Threat Hunting service with enhanced endpoint detection. The result is a solution of cyber security services designed to expand visibility and detection capabilities in the environment, to combat advanced attacks.

The Value of Security Intelligence Cannot be Overstated

The Analytics Value Creation equation separates "data feeds" from "Security Intelligence," as it is the opinion of Frost & Sullivan that these are separate and distinct. Security intelligence is not just another data feed, but is separate and unique.

"Data feeds," as the term is being used in this SPIE, refers to data collected from an organization's network environment. Such data includes log files, full packet capture data, network flow information, user information, endpoint telemetry, and other related data. The superset of network data sources is almost limitless.

Whereas, data feeds provide "what is examined," security intelligence provides the "where to look" and the "what is being looked for." To use a metaphor, if the goal is to visit Major League Baseball stadiums, security intelligence provides a map of how to get to "1060 West Addison Street, Chicago, IL" and a description of Wrigley Field. Without such security information, security professionals will be horribly inefficient as they wander, looking for network activity to automate in analytics.

Stratecast
The Last Word

"Big Data" analytics often carries a tone of mysticism as if an endless stream of data can be fed into a massive database and analytics platform, resulting in a magical illumination of intelligence. In network security, the corresponding assertion is that a blinding spotlight would be cast on malware, creating impenetrable defenses. The reality is a much different picture.

Security professionals prefer the term "advanced analytics" as it better reflects the tremendous investment of people, time and resources to create analytics that adds value. Analytics needs to be viewed as a service that is delivered as a service with on-going improvement, rather than an event.

Advanced security analytics is the automation of learned processes from skilled security personnel by powerful computational platforms. Analysts (humans) have the ability to use both inductive and deductive processes intuitively. Achieving that same result from analytics software requires that the software be programmed and taught, by humans, to perform certain operations. Simply put, analytics does not create; it automates. Think of it as digitizing a cyber-security playbook.

As advanced security analytics is human-centric, the approach to advanced security analytics is very different than the approach to which we are accustomed in traditional information technology (IT). In IT, the business value comes from the software purchased; the people required to administer the systems are often a tax on top. But in advanced security analytics, the value comes from the people; software is purchased to make them more effective. The difference is subtle, but critical, when designing solutions. Software does not provide the answers; it provides the tools and enables the data needed to discover answers.

Security professionals that are evaluating analytics solutions need to not only examine the effectiveness of the analytics solution in today's cyber environment, but also how vendors plan to continuously improve the analytics to deliver superior analytics in the future. Cyber miscreants are not static. With bring-your-own-device (BYOD), hybrid cloud environments, network function virtualization and software defined networks, the cyber environments are getting more complicated, not less. Security analytics services cannot be static either.

One final question to contemplate: Is the sophistication required to effectively implement selected cyber security defenses becoming increasingly out of reach for mainstream organizations? Tools that historically performed behavior analysis for threat detection, such as an IPS, are too limited in visibility, given the reality of today's cyber threat landscape. Many businesses are too resource-constrained to support expert analysts, data scientists, and "big data" solutions. Much like employing specialized accounting firms to help navigate the complexities of tax codes, employing security specialists, like managed security service providers, may be unavoidable at a point in the future.

Frank Dickson

Research Director – Information and Network Security

Stratecast | Frost & Sullivan

frank.dickson@frost.com

About Stratecast

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.

CONTACT US

For more information, visit www.stratecast.com, dial 877-463-7678, or email inquiries@stratecast.com.