opentext™ | Cybersecurity

Position Paper

360° Analytics for a Resilient SOC

Layered Analytics for Faster Detection and Increased Productivity

Elevate cyber resilience by sharpening SOC analysts' focus on what truly matters with contextual insights for known and unknown threat detection.

Table of Contents

Introduction

Every day a plethora of threats target your company. Finding and responding to those threats requires the ability to detect the signs of an attack at every point along the chain of actions that start with reconnaissance and could end with an impact to your company.

The first sign may be the anomalous use of a single set of compromised credentials or a convincing phishing attack, resulting in an attacker gaining access to a machine on your network. With attackers increasingly focused on big game hunting—looking for a large payday—the cyber actor may use the initial machine as a beachhead to compromise the network and move from machine to machine, identifying key data and critical systems.

Eventually, the attacker will take action—dropping a payload, such as ransomware, stealing data or intellectual property, or turning captured machines into a botnet for crypto-mining.

The failure to detect such threats early have a high cost. For many companies, the first time they realize that they have been compromised is when their data appears online, a third party notifies them of anomalous behavior, or computers in the office display a message: “All of your files are encrypted with RSA-2048 and AES-128 ciphers…”

The list of companies and organizations compromised in the past year is long, with many public incidents, such as:

- A community college in North Carolina
- The City of Baltimore
- A game developer in Europe
- A paper and packaging company

To be resilient, a security operation center (SOC) needs to adapt in the face of change and challenges, particularly in the ever-evolving cybersecurity space. Catching threats as early as possible improves the SOC’s ability to withstand and recover from both accidental and deliberate actions against the business and makes the business more resilient.

A Comprehensive Approach

While much of the discussion surrounding defenses against modern threats focuses on detecting and blocking the initial intrusion, a more comprehensive approach is needed. Companies need to not only detect the initial intrusion, but also need to focus on detecting attacker interest, the anomalies that indicate that intruders are already in their network, and also allow security analysts to seek out signs of specific attacks based on threat intelligence.

Like the proverbial blind men describing individual parts of the elephant without understanding the whole, security teams are only aware of the elements of an attack that their tools can “see.” A decade ago, real-time correlation using security information and event management (SIEM) technology was good enough to detect threats on its own,

but the volume of data has grown, allowing attackers to hide in the noise. While artificial intelligence and machine learning can help by highlighting anomalous activity, such automation does not know whether the anomalous behavior is good or bad. It lacks situational context.

Blending the two approaches and letting them work together to get faster, actionable insights, with context, helps with the real problem: Reducing the time a company is exposed to threats. A system that puts together different data sets can improve the chance of detecting—and prioritizing—the signs of an attack. This layered approach to security analytics results in better coverage of a company's attack surface and earlier detection of threats—before they can do extensive damage.

Layered analytics—which brings together correlation, behavioral analytics and threat hunting—helps companies minimize the impact of an attack. For vigilant companies with the right tools, today's threats are not single malicious incidents appearing out of nowhere, but a series of actions detectable at each step of the attack chain. Different technologies and techniques are better suited to analyzing, for example, log events, user actions, and anomalous traffic. Layered analytics brings these different types of analysis together, combining signals generated by potential threats, to allow earlier and more consistent detection of attacks.

Layered Analytics Sees the Entire Attack Chain

Combining different analytical approaches captures an attack at different points in the chain of events that can start with reconnaissance by the attacker and extend to payload deployment and impact. MITRE's ATT&CK Framework can be used to describe all the steps of an attack, and from the defender's perspective, all the points at which an attack can be detected and defenders can respond.

Take, for example, a ransomware attack, which consists of numerous steps[1]:

- Initial Access—Attackers gain access through phishing attacks, the use of previously stolen valid credentials, and exploitation of an unpatched vulnerability
- Persistence—The addition of boot-up or login scripts, hijacking execution flow, and abuse of the Office application startup sequence allows an attacker to keep control of the system.
- Lateral Movement—Attackers use open ports, remote-administration services, reusing sessions keys, or conducting internal spearphishing to spread throughout the organization.
- Exfiltration & Impact—Data may be encrypted for ransom, intellectual property might be exfiltrated, or operations could be impacted.

Layered analytics maximizes an organization's ability to detect and respond to an attack by catching the signs of an attack throughout the entire attack chain:

- The security-incident correlation engine in ArcSight ESM by OpenText™ brings together security events, threat intelligence, and log data to better detect threats and minimize false positives.
- The behavioral analytics and machine learning capabilities in ArcSight Intelligence by OpenText detects user and device behavior that departs from the expected normal activity.

1. MITRE ATT&CK Enterprise Matrix." MITRE. Web page. N.D. **https://attack.mitre.org/matrices/enterprise/**.

- The **big data analysis and search capabilities** of ArcSight Recon by OpenText™ supports extensive threat hunting and incident response activities.

Combining layered analytics, and not relying on a single approach, gives additional context to security analysts, allowing them to triage alerts more quickly, and reducing time to detecting actual threats.

Pre-Empting Threats: Catching Attacks in Real Time

The security events that indicate an attack or compromise frequently do not stand out from the noise. Looking through events for signs of attack can be subtle: A handful of failed login attempts, accessing an application from an unknown Internet address, attempts to connect to restricted corporate resources, and the use of tools or processes for the first time.

When these events are not correlated, a SOC analyst will be inundated with a plethora of seemingly unrelated alerts. Often, alert fatigue will set in. With the number of alerts produced by security information and event management (SIEM) systems, a single anomaly is often not enough to convince an analyst to prioritize a security event. With real-time correlation, a security analyst will quickly be presented with more context about a specific event.

Detecting Linked Events

A common technique following initial access, for example, is to execute scripts and malware. Common tools—such as PowerShell and the Windows Command Shell—are used to run command scripts without attracting notice. However, a remote login paired with running a command line interface (CLI), especially if the user rarely ever runs such a tool, can often be correlated to detect an attack as early as possible.

A series of failed logins before a successful login may rise to the level of anomaly depending on the organization's threshold. SIEMs often create rules that only alert analysts to failed logins if number of failures exceed a specific threshold in a certain period of time. By linking such events with subsequent behavior, defenders gain context: A series of failed logins, followed by a successful login, the execution of previously unseen processes, and a connection to an untrusted Internet address should rise to the top of the list of incidents to be investigated.

Correlation is only as good as the signatures provided to link together known events. While an organization can create their own signatures for the best fidelity, they often cannot keep up with the correlation signatures required to detect the most current threats. Any correlation engine needs to also include rules and signatures created using the latest intelligence.

Event Correlation Improves Chance to Detect Unknown Threats

While zero-day threats are uncommon, attackers are always searching for ways to evade detection. This often takes the form of changing a single step in their attack chain, whether obfuscating their malware or scripts to avoid analysis or lengthening the time between password attempts to confound threshold rules.

Costs of Missing Signs of an Attack

The longer an attack goes undetected, the more expensive it becomes. Organizations that deployed security automation—a proxy for the speed of detection and response—had an average breach cost of about $2.5 million, much less than the average breach cost of $6.0 million for companies with no automation deployed, according the 2020 Cost of Data Breach report, conducted annually by the Ponemon Institute.

The cost of a failure to detect, or understand, an attack can be seen in a recent, anonymous, incident revealed by the U.K.'s National Cyber Security Centre (NCSC)[2]. An organization that fell victim to a ransomware attack paid almost £6.5 million—more than U.S. $9.0 million—but failed analyze the root cause of the breach. The attackers came back two weeks later and reinfected their network. The victim paid a second time.

2. Technical Lead for Incident Management. "The rise of ransomware." National Cyber Security Centre. Blog Post. 29 January 2021. **www.ncsc.gov.uk/blog-post/rise-of-ransomware**.

Correlating the behavior of various entities—whether processes, devices or users—allows security operations to see through these attempts at obfuscation and gives organizations a better chance to detect and stop unknown threats. While the link included in the initial e-mail used in an Emotet campaign, for example, may fool any blacklist, a rule that correlates an e-mail message from an unknown sender with a link to an previously unknown domain could help identify a wide variety of phishing attempts.

Pre-Emptive Threat Detection
Companies are inundated with security events, often causing alert fatigue for security analysts. Pre-emptive threat detection uses automation, context, and intelligence to prioritize potential security events, reduce alert volume, and allow analysts to respond to true threats fast.

Unlike search-based security event technology, real-time correlation automates the detection of sequences of events to allow for real-time detection of threats.

People-Centric Threats: Detecting Behavioral Anomalies

Many attacker operations, such as ransomware campaigns, need to gain extensive access to a company to a work. Gaining access to and encrypting a single computer, or even using a worm to crawl through many systems, is less common than attackers taking a user-centric approach. Infecting a single system as a beachhead, using that user's credentials to move throughout the network, and raising privileges to gain further access are people-centric approaches common to ransomware.

While internal actors are less common, people-centric threats are prevalent. In 2020, more than a third of breaches (37%) stole or used credentials, and 27% of breaches targeted users with phishing[3].

Machine Learning Allows Detection of People-Centric Threats

The amount of information required to quantify the behavior of even a small organization would tax most security operations teams. While some organizations use rules to try to create their own "normal" profile for users—for example, connecting between 7 am and 6 pm and less than three login failures—such approaches can miss true threats and issue alerts for innocuous behavior.

Automating the process and using machine-learning to determine anomalous behavior is critical to catching people-centric threats. Unsupervised machine learning can determine which users behave similar to others in the groups and whether current activity matches their past activity.

SIEM Correlation Engine in ArcSight Enterprise Security Manager
By correlating events and anomalies in real time, the SIEM Correlation Engine in ArcSight Enterprise Security Manager by OpenText™ gives your security operations team more context about events in real time and greater visibility into potential malicious activity. The SIEM Correlation Engine can connect the dots and determine that malware may try to run because a user has fallen for social engineering.

3. "2020 Data Breach Investigations Report." Verizon Enterprise. PDF. pg. 7. May 2020.

People-Centric Focus Allows Fast Detection, Before Damage
The time to detect ransomware can have a significant impact on the amount of damage suffered by your organization. Automated machine-learning systems continually collect information on the latest events, allowing security operations teams to identify potentially compromised users in time to respond, before ransomware is deployed.

The technique also can take advantage of attackers' weak link: In almost every case, an attacker will not behave in the same way as the user. As long as the machine-learning system has visibility into would-be attacker's activity on the internal network, it can spot the anomalous behavior.

Combining different analytical methods into a layered approach, security analysts gain behavioral insights—not only to improve the identification of anomalous behavior—but allowing them to respond to the incident with assurance, because the layered analytical models can increase confidence in the identification of malicious behavior.

People-Centric Attack Mitigation
Insiders are a top threat to your organizations. While actual malicious insiders account for a minority of breaches, attackers usually target employees as the first step in an attack. A compromised device or stolen credentials can be used to disguise attacker access as a user's daily business.

People-centric attack mitigation focuses on the users who are typically targeted by attackers. Every user has a behavioral pattern that makes them difficult to categorize into specific roles, making simple rules not an effective way to create alerts. Instead, by analyzing event data and using extensive machine learning, ArcSight can identify the users that pose the greatest risk.

ArcSight Intelligence and Behavioral Analytics Powered by AI
Behavioral analytics is key to detecting threats early and limiting an organization's exposure to damaging attacks. **ArcSight Intelligence** uses behavioral analytics to determine the normal baseline behavior of every user, determine the level of risk those users present, and detect anomalous behavior. Using unsupervised machine learning, the system creates a digital fingerprint of each users, allowing potential anomalies to be identified in context.

Proactively Hunt for Threats

Historically, time has been the attacker's friend. While companies typically do not find an attacker for weeks, if not months, attackers often work much faster. In one attack in 2019, only eight days after an employee received an e-mail and opened the malicious Office attachment, attackers had compromised and encrypted nearly 200 endpoints and 30 servers, and then activated a ransomware payload[4].

When security operations centers (SOCs) need to analyze potential security events, their analysts require the ability to quickly search through the collected logs of a company's critical assets. This capability to hunt for threats can be the difference between identifying an initial compromise and having dozens, or hundreds, of systems encrypted for ransom.

4. Harpaz, Ophier, and Kuznets, Danielle. "IResponse To IEncrypt." Guardicore. Blog. 5 April 2019. **www.guardicore.com/2019/04/iresponse-to-iencrypt/**.

Often, indicators of compromise found by other organizations can be the starting point for analysts to hunt for threats in their own network. Mining analysis of high-profile incidents, such as the compromise of SolarWinds' software, can also be a good starting point to look for attackers in your own network.

Tools to Search for the Latest Threats

Threat hunting is a valuable way to apply the latest intelligence to your own organizations to find threats that might otherwise go unnoticed. Combing internal log data and external intelligence can result in proactive detection of threats before they blossom into ransomware incidents or data breaches.

However, giving security analysts the tools to hunt for threats among millions of security events requires a few capabilities:

- a centralized store of log data,
- an event storage format that allows for efficient searching, and
- the ability to integrate with third-party sources of intelligence and data.

Adding the power of layered analytics also allows threat hunters to enrich their investigations using behavioral analytics and historical data to dramatically increase confidence and decrease the time and effort necessary to identify threats and anomalous behavior. Augmenting the ability to efficiently search through data with the results of automated machine-learning behavioral algorithms can increase the power of a single analyst, allowing them to perform threat hunting more quickly and more accurately.

Regular Threat Hunting Reduces Attack Surface, Faster Response

In addition to reducing exposure time, organizations that regularly conduct threat hunting reduce their attack surface area, making it more difficult for attackers to infiltrate their networks. Regular threat hunting also helps create repeatable procedures for detection and response, speeding organizations' reaction times.

Threat hunting—and regular penetration testing, in general—can also help catch misconfigurations or other situations where a security measure has been implemented incorrectly or not completely.

Exposure Time Reduction

Knowing about the latest threats can reduce a company's cost to clean up the damage from a breach and limit an attacker's ability to do damage. From Winn Schwartau's book Time Based Security, costs are related to exposure time, which is the sum of the time it takes to detect a threat and the time it takes to react or respond to the threat.

Unfortunately, most companies are not winning this race against the attacker. The average time it took for a company to detect and contain a breach is 280 days, and companies that could detect and contain a breach in less than 200 days could save an average of $1 million[5].

Big Data Analytics and Threat Hunting through ArcSight Recon

With centralized log management, the ability to efficiently search through data, and integration with ArcSight and third-party security environments, **ArcSight Recon** can be used to proactively detect potential weaknesses before they are used by threats. By integrating Recon with **ArcSight Security Orchestration and Response (SOAR)**, the systems responds automatically to threats identified during threat hunting.

5. Ponemon Institute. "Cost of Data Breach 2020." Report. Web. **www.ibm.com/security/digital-assets/cost-data-breach-report/**.

Only a quarter of companies were able to stop ransomware before data is encrypted, and those who paid a ransom had roughly double the costs—$1.4 million—compared to those who refused to pay a ransom[6].

Conclusion

The key to catching complex threats early is to uncover signs of attack from as many parts of the chain as possible. By not relying on a single source of information, layered analytics can correlate subtle evidence of an attack into a single decision based on context. Real-time correlation allows organizations to use known threat details to automate threat detection. User and entity behavior analytics (UEBA) can determine what activity is normal in your organization and what should be considered an anomaly. And, threat hunting gives security teams the tools to use current indicators of compromise to take a second look at historical data.

Layered analytics supports the entire threat-intelligence lifecycle. ArcSight ESM operationalizes any intelligence on known threats by integrating it with the real-time correlation engine. ArcSight Intelligence allows user and device behavior to be analyzed for unknown or emerging threats by uncovering abnormal activities. And ArcSight Recon gives analysts a tool for proactively looking into evidence of threats.

No matter where you start in the analytical cycle, adding additional capabilities and analytical layers is simple. ArcSight's ESM, ArcSight Intelligence, and ArcSight Recon are tightly integrated to allow each product and its analyses to be used as context in the other analytical layers. In the world of a rapidly changing threat landscape and a threat data tsunami, layered analytics serve as a force multiplier for your SOC team so they can focus on what truly matters in elevating your organization's cyber resilience.

Next Steps

Learn more about each of the Layered Analytics products below:

- ArcSight Enterprise Security Manager (ESM)
- ArcSight Intelligence
- ArcSight Recon

In addition, see how each element of the Layered Analytics model detects threats based on MITRE's ATT&CK Framework.

- OpenText ATT&CK Navigator

6. "The State of Ransomware 2020." Sophos. PDF. pg. 12. May 2020.

Connect with Us

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.