White Paper

Security

Power of the Threat Detection Trinity

How to Best Combine Real-time Correlation, Insider Threat Analysis and Hunting to protect against cyber threats. Combine real-time correlation, detection analytics and hunt to cover and tighten your detection grid and reduce the attack surface.

MICRO FOCUS

Table of Contents

page

When all three of these approaches are combined into a threat detection trinity organizations can effectively defend against current multi-vector threats

Today, security operation centers (SOCs) face mounting challenges as the advanced threat landscape continues to evolve with attackers using higher levels of sophistication, organization and innovation. It's not only businesses that are losing millions of dollars each year due to security incidents, but home users as well. Symantec found that 64 percent of Americans were willing to pay a ransomware attack extortion fee with criminals demanding an average of $1,077 per victim . To make matters worse, not all attackers are external; in fact, insider threats often pose an even greater risk—some intentionally malicious, some caused by carelessness from employees, that can expose an organization to data breaches and hacks. Compounding the challenge of advanced threats, is the explosion of data and lack of skilled security personnel trained to respond to these threats.

How Can SOCs Stay Steps Ahead of These Advanced Threats?

Organizations must be both innovative and efficient with their security solutions to win this security battle. Because today's threats are often multi-vector attacks, traditional tools and approaches are not able to handle the evolving needs of SOCs today. Single solution approaches are not adequate to combat multi-vector, multi-layered threats. SOCs need real-time correlation, detection analytics and hunt tools to combat both known and unknown advanced threats. Real-time correlation identifies events of interest (EOI) and alerts SOC analysts to initiate their incident triage and investigation processes. Real-time correlation accounts for the fact that variables are constantly changing and can identify their specific relationship at every moment you need to react. Detection analytics use machine learning and analytics to uncover user behavior that might indicate insider threats or previous breach occurrences. Meanwhile, hunt and investigate tools demonstrate the proactive "hunt" against unknown threats. When all three of these approaches are combined into a threat detection trinity organizations can effectively defend against current multi-vector threats.

The Threat Detection Trinity, which combines real-time correlation, detection analytics and hunt, can cover and tighten your detection grid and reduce the attack surface. While each technique by itself is capable for their specific area, their combined power as the Threat Detection Trinity delivers a multi-layered approach for today's SOCs.

This report will cover current challenges, examine the power of the Threat Detection Trinity, and how Micro Focus® ArcSight Enterprise Security Manager (ESM), UBA and ArcSight Investigate are three distinct detection solutions that form the Threat Detection Trinity.

Current Challenges

ADVANCED THREATS AND MULTI-VECTOR ATTACKS

Multi-vector attacks wreak havoc on SOCs where cyber criminals combine a range of tactics, techniques and procedures deployed at various stages and points. Once case study still typical of multi-vector attacks today, was the "String of Paerls". The attack began with a phishing email containing a malicious Word attachment. Once opened, the malware penetrated and expanded laterally and then called backed to command and control servers on two separate domains in India and the UK. The third prong of the attack contained malicious executables that went to the cloud.

This attack shows an example of how organizations today struggle to combat attackers who are becoming more advanced, stealthy and tactical. The average annual loss per company in the US is $17 million[1] as SOCs try to keep pace with adversaries.

DATA INCREASING

Data is exploding and coming from various sources—IoT, the cloud, etc. IDC predicts worldwide revenues for big data and business analytics will grow from $130.1 billion in 2016 to more than $203 billion in 2020[2]. And, as many organizations known, criminals are targeting this valuable data. However, many traditional security tools were not designed to process today's volume and velocity of data.

LACK OF SECURITY PERSONNEL

SOCs face the challenge of personnel shortage to handle the volume and complexity of advanced threats. Senior security analysts are hard to find; and, in addition, entry and mid-level analysts often grapple with complex tools or are not experienced enough. Creating more obstacles is having the security analysts work on separate solutions (silos) and not properly communicate with each other for workflow efficiency. Another challenge is the "swivel-chair" syndrome impacting SOCs when lack of integration between solutions cause analysts to use multiple terminals, tools and solutions. The analysts must then "swivel" the chair between the separate solutions. Security analysts are already burdened and don't need these extra obstacles.

DISPARATE POINT SOLUTIONS

To combat threats, many organizations are investing in security, which is a step in the right direction. However, having too many separate security point solutions is not an ideal approach. Disjointed security controls may increase your IT complexity, create integration challenges, and these vulnerabilities may broaden your attack surface. As an example, one SOC may have a real-time correlation tool and then another separate tool just for detection. The challenge here is the lack of coordination between the two different solutions.

Overall, all these challenges reduce levels of visibility, coverage and control. SOCs must combat threats slipping through the gaps in the detection grid but often lack a unified detection view.

Current Challenges:

- Data increasing
- Lack of security personnel
- Disparate point solutions

1 *Micro Focus (HPE), "Intelligent security operations: an investigation guide"*
2 *IDC, "Double-Digit Growth Forecast for Worldwide Big Data and Business Analytics Market"*

Hunting with ArcSight Investigate:

- Intuitive Guided Search and Visuals
- Built-in Advanced Analytics
- Workflow Efficiency
- Automation of Tasks

The Threat Detection Trinity

Our security industry is at critical point where security solutions and advanced threats are in a heated battle. Point solutions are effective at solving specific and distinct challenges, but today's threats are often multi-vectored attacks. A new approach is needed—an actionable vision that is proactive, complete and powerful.

Fortunately, Micro Focus delivers the answers with the Threat Detection Trinity, which combines hunt via ArcSight Investigate, real-time correlations via ArcSight ESM, and detection analytics with ArcSight User Behavior Analytics. Combined, these three areas form a powerful Threat Detection Trinity to tighten the detection grid and reduce the attack surface.

Let's examine each specific area that forms the Threat Detection Trinity.

Hunting

Traditional hunt tools have not scaled to match the growing size of IT infrastructure and the amount of data being generation. Today Hunt teams need a solution that can empower them with sophisticated search, visualization and analytic tools to manually explore data for unknown threats and artifacts indicating a compromise has occurred.

Threat Detection Trinity: ArcSight Investigate for Hunting

ArcSight Investigate delivers next-generation hunt and investigation technology directly into the hands of all your security analysts. ArcSight Investigate taps into advanced analytics to fuel hunt and investigation while meeting the evolving needs of SOCs today.

Key capabilities and benefits include:

- **Intuitive Guided Search and Visuals**—An intuitive search interface understands search terms in security context and dynamically suggests relevant queries and delivers out-of-box visuals for security-specific use cases.
- **Built-in Advanced Analytics**—ArcSight Investigate takes advantage of Vertica, a high-performance analytics platform, to drive the analytical power of the investigative process.
- **Workflow Efficiency**—Response time to threats is critical. With ArcSight Investigate, security analysts improve workflow efficiency by providing a complete and real-time view of security events.
- **Automation of Tasks**—ArcSight Investigate helps your security analysts execute searches up to 10x faster than other investigation tools. Analysts can shift through large volumes of data collected over many years in minutes via ArcSight Investigate.

Hunting is a critical aspect of the Threat Detection Trinity. ArcSight Investigate provides seamless integration with ArcSight Enterprise Security Manager (ESM), Hadoop and other existing analytics and security investments. ArcSight Investigate enables your security analysts (Leve 1 to Level 4) to build a single, structured data lake for data exploration—quickly and with ease. As part of the Threat Detection Trinity, ArcSight Investigate provides seamless integration with ArcSight Enterprise Security Manager (ESM), and ArcSight User Behavior Analytics (UBA).

Real-Time Correlation

SOCs need to turn findings into real-time correlation rules and alerts to make sure those indicators of compromise are not missed in the future. Attackers often start small, infiltrating and seeing how far they can get into the system without detection. Real-time correlation needs to detect that attack in the earliest stages and in real-time for security analysts to quickly and efficiently respond. Real-time correlation accounts for the fact that variables are constantly changing and can identify their specific relationship at every moment you need to react.

ArcSight ESM analyzes and correlates every event that occur across your organization to deliver accurate prioritization of security risks and compliance violations

Threat Detection Trinity: ArcSight Enterprise Security Manager (ESM) for Real-Time Correlation

Covering another crucial part of the Threat Detection Trinity, ArcSight ESM analyzes and correlates every event that occur across your organization to deliver accurate prioritization of security risks and compliance violations; these events include every login, logoff, file access, database query, etc.

Key ArcSight ESM attributes include:

- **Automatic Real-time Correlation**—ArcSight ESM sifts through millions of log records to accurately prioritize security risks and compliance violations then delivers distributed correlation.
- **Single Unified View**—Instead of trying to cobble multiple detection solutions, ArcSight ESM empowers your SOC with a unified view of who is on the network, what data they are accessing, what they are doing with the data, and how that impacts business risk.
- **Built-in Workflow Efficiency**—ArcSight ESM uses its built-in workflow engine to manage incidents and prevent damage once threats and risks are identified.
- **Augmented Speed and Integration**—ArcSight ESM delivers lightning fast speed with the ability of sifting through 100K events per second to enrich and prioritize events in real-time—even if the data is from another product.

ArcSight ESM helps SOCs gain knowledge of attack patterns while brining as much data—quickly and efficiently—into the SIEM. ArcSight ESM empowers security analysts with distributed correlation for greater collaboration and workflow efficiency. ArcSight ESM tracks 1000s of events per second using rule sensors to monitor event relationships and sends an alert when something suspicious occurs—all in real time. As part of the Threat Detection Grid, ArcSight ESM integrates easily with ArcSight Investigate and ArcSight User Behavior Analytics (UBA) to further tighten your detection grid.

Detection Analytics

Let's examine the challenges created by insider threats. Some insider threats are not purposely/intentionally malicious; for example, an employee falling victim to a phishing scam and accidentally downloading malware. However, how do you monitor behavior of employees and vendors who have access to your data? As example, an employee might log into his or her laptop late at night and is currently a different country. This gets flagged as an alert though nothing is wrong. You need intelligence behind the alerts to reduce the number of false positives which takes time and focus away from real threats.

ArcSight UBA empowers SOCs to detect breaches before significant damage occurs by finding the adversary faster and putting detection analytics into action.

Analytics and speed are critical components when organizations look for security insights

Detection analytics, which applies algorithms in area of even anomaly and entity relationship on specific data sources, can uncover unknown threats. Analytics and speed are critical components when organizations look for security insights.

The Threat Detection Trinity: ArcSight User Behavior Analytics (UBA)

ArcSight UBA empowers SOCs to detect breaches before significant damage occurs by finding the adversary faster and putting detection analytics into action. To specifically combat insider threats, Arc Sight UBA implements quick forensics investigation and analyzes user related data looking for threats in comparison to peers, historical activity, and/or violations of predefined expected behavior.

Key ArcSight UBA attributes include the abilities to:

- Increase visibility into attacks with real-time alerts on suspicious user and entity activities and behaviors
- Deliver immediate insight into security risks, streamlines investigations, and increases productivity
- Prioritize the most suspicious and abnormal activities across users and entities
- Detect cyberattacks and insider threats, even if legitimate credentials are being used
- Provide hundreds of supported use cases to target intelligence activities to various threat situations

Overall, ArcSight UBA puts high-quality detection directly into the hands of all security analysts. Time is to respond is critical for SOCs to minimize the risk and impacts of attacks. ArcSight UBA delivers that real-time insights through purpose-built security analytics. Solidifying the strength of the Threat Detection Trinity, ArcSight UBA seamlessly integrates with ArcSight ESM and ArcSight Investigate. .

Conclusion

Hunting, real-time correlation and detection analytics are all necessary tools and approaches for detecting known and unknown threats. However, when they work in accord together and seamlessly integrate as ArcSight Investigate, ArcSight ESM and ArcSight UBA do, they tighten the spaces/gaps in the detection grid and reduce the attack surface.

Fortunately, Micro Focus delivers all the three critical solutions to form the leading Threat Detection Trinity; and in doing so, promotes not only detecting known and unknown threats, but higher levels of collaboration between SOC analysts, hunters and other key stakeholders. Combating multi-vector attacks with the Threat Detection Trinity delivers augmented coverage of the detection grid, an evolution of layered security and is more comprehensive approach than a singular modularity. Micro Focus is committed to constantly innovating for our customers, partners and helping to move the entire industry forward.

Contact your Zones Account Manager at
800.408.9663, or visit zones.com, for more details.