CyberActive℠

Upgrade your SOC with Security Analytics and Orchestration

Author:

Rajat Mohanty,
CEO, Paladion Networks

PALADION
HIGH SPEED CYBER DEFENSE

Overview

Security teams are always on the lookout to enhance the capabilities of their current Security Operations Center (SOC) to counter targeted attacks. Unlike common cyber attacks, targeted attacks are very different. Attackers explore sophisticated methods and spend a greater amount of time carrying out large impact breaches. So, the real question for an organization is: "Does your SOC detect and respond to targeted attacks?"

In order to mitigate targeted attacks, a SOC needs to have deeper detection and faster response times. Two new areas of cyber security; analytics and orchestration are incorporated to achieve this goal.

Below we describe how you can add these cyber security features to your existing SOC.

SECURITY ANALYTICS - FINDING MORE HAYSTACKS AND MORE NEEDLES

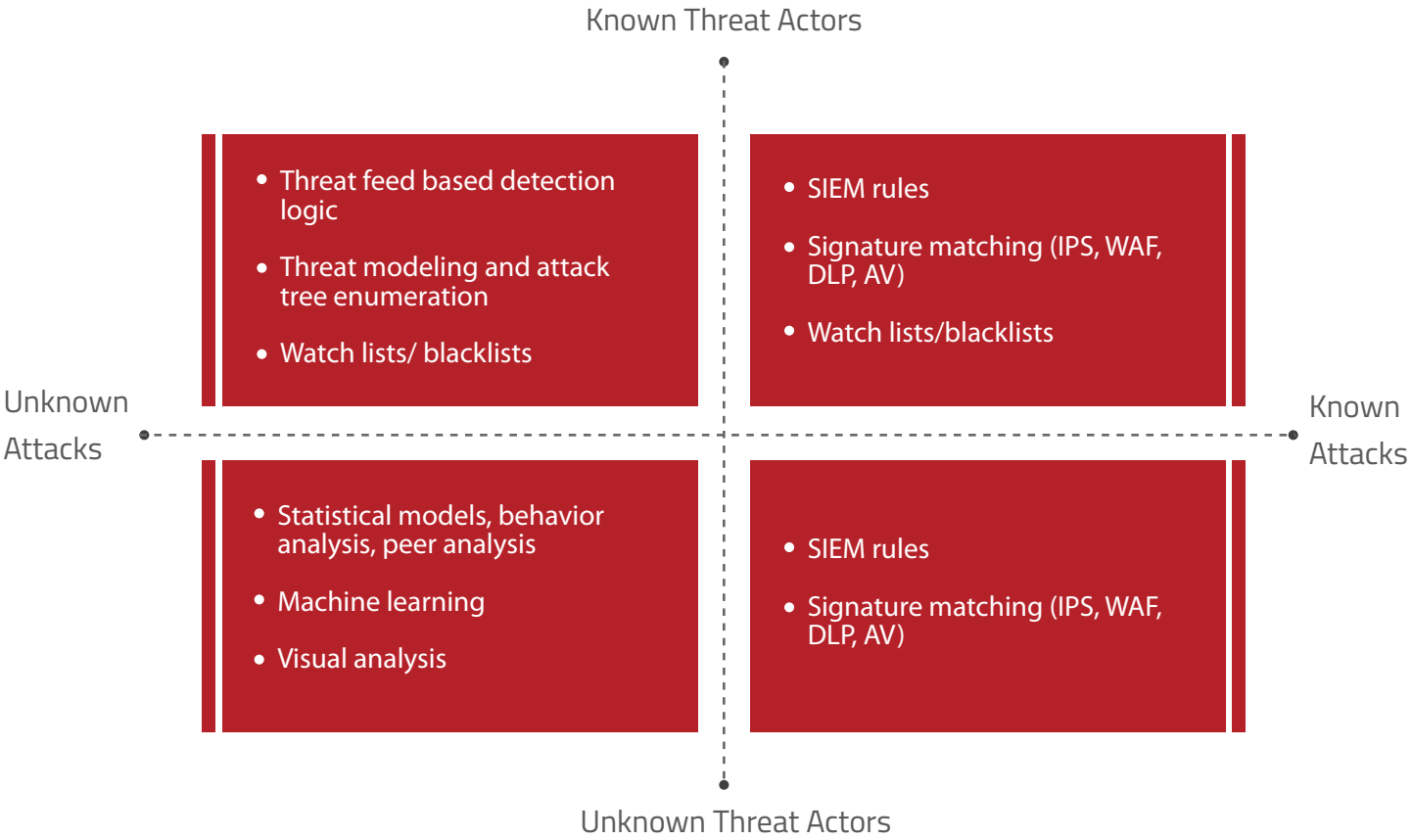


Figure 1

Using a conceptual framework to understand the role of security analytics, attacks can be grouped based on two dimensions, attackers, and attack methods, as shown in Figure 1.

When the attack methods are known, the security industry typically uses rules to detect them. These could be AV signatures or rules on IPS, WAF, SIEM, and others. The role of analytics comes up when the attack methods are not known a priori.

Given that an increasing number of targeted attacks have some form of unknown method, traditional rule-based systems are not sufficient in effectively eliminating threats. Instead, it needs additional analytics features, which are applied in two ways:

1. When the attack methods are unknown, analytics are primarily used to either detect anomalies in traffic, protocols, user access, and data usage or to detect a pattern that is similar to earlier breaches. This occurs in the following scenarios:

   - Analytics that do anomaly detection that focuses on outliers to a population's behavior or abnormality from past behavior or deviation to a baseline, etc.
   - Analytics that detect patterns are focussed on fraudulent behavior or connecting events to uncover linked attacks.

2. The security industry is also investing in tracking attackers and studying their attributes. This is termed as security or threat intelligence and uses a large amount of open source and underground data to obtain insights on attackers.

   - In this instance, security analytics is about collecting and applying threat intelligence to a variety of traffic such as packet captures, netflow, and proxy, emails, DNS and Identify, and access data. This is done through using watchlists and blacklists of IP/URLs/files, detecting Indicator of Compromise (IOCs), and enumerating attack trees.

Using analytics to detect "unknown attackers-unknown attacks" involves finding more and different haystacks for identifying attacks. Analytics will throw up suspicious alerts that will need further investigation or hunting to isolate the breach if any. On the other hand, analytics using threat intelligence (known attackers- known attacks) leads to a more direct detection of potential breaches.

How SOCs Can Upgrade to Security Analytics

USE CASES COME BEFORE TECHNOLOGY

The first step for upgrading a SOC is to identify the use cases for applying analytics, beyond the generic concept of unknown-unknowns and known-unknowns. Very often, the security analytics project starts with the deployment of an analytics platform and data collection that only leads to expensive data management and poor output. Therefore, it is essential to know where to apply statistical or machine learning methods, as well as what gaps such methods are covering.

The best way to understand this is to take the example of an unknown malware that is part of an advanced targeted attack. Rule-based systems including SIEM or signature based systems including IPS, anti-malware, and WAF are not efficient enough for detecting such attacks.

So much so, that the sandbox technology approach fails to detect malware. This is because malware software programs stop executing when a virtual environment is detected.

There are, however, traces of malware activity in different technologies across the entire IT landscape. One such source could be proxy logs since it can reveal data corresponding to beaconing of malware, most of which send out regular heartbeat information to its C&C server. In the case of advanced malware, the C&C servers may not be on the list of known malicious IP address. The heartbeat information, contained in proxy data, can be detected by applying the concept of entropy.

Entropy in data science terms refers to "uncertainty of data". When we look at proxy data in general, most of the data sizes corresponding to users communicating with URLs are randomly-based on the website and page being accessed. In this case, when we apply entropy on the byte size of the communication between user and URL, the entropy will be high, owing to a high "uncertainty of data".

This is because the user interaction data size is not a constant and varies with the interaction involved. On the other hand, if we apply the entropy function on data in which the heartbeat information being beaconed out by malware of the same size and similar frequency, the entropy will be zero. This is due to the fact that the byte size is the same for interaction with the C&C URL, enabling us to detect the "unknown" attack even though the attack signature or attacker is unknown.

This is an example of just one use case. Applying the complete analytical model in security needs to be driven through use cases and not technology deployment. (Details of use case-based approaches for security analytics and the platform components are available in a separate Paladion white paper "Use case approach for security analytics")

BUILDING THE ANALYTICS TECHNOLOGY PLATFORM

Once a set of use cases for analytics is defined, the next step is to utilize the analytics platform and connect the right data sources to it. Since the data size from security technologies and other passive sources, such as proxy, packet captures, netflows, user activity logs, etc. is high, the platform is usually a Big-Data platform.

A SOC can look at commercial platforms with built-in analytics that meet their use cases, in addition to the development of a customized platform. Typical components of such a platform could include a HDFS file system, Hive/Hbase for data storage, Spark for real-time processing, Scala/R/Python for statistical analysis, and D3 for visualization.

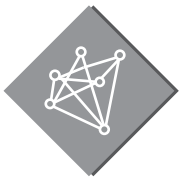
A short blog on the use of big data security analytics to detect unknown attacks can be found here: http://www.paladion.net/big-data-for-proactive-cyber-threat-prevention/.

APPLYING THREAT INTEL

Threat intelligence is the second pillar for the detection of unknown attacks. When the attack itself is unknown but the attacker characteristics are available, SOCs can integrate threat intelligence feeds from external sources to its analytics platform and model rules to detect unknown threats before it's too late.

Threat intelligence feeds contain values for typical Indicators of Compromise (IOCs) including IP address, URLs, geo-location, and device profiles. Threat intelligence sources have diversified over the years from niche commercial vendors to CERTs (Computer Emergency Response Team), ISACs (Information Sharing and Analysis Center), OSINT (Open Source Intelligence), global SOCs (Security Operation Center), private sharing within industry verticals, and the government.

Of course, threat intelligence isn't only external. In the case of a targeted attack campaign, an attacker could be inside the network carrying out multiple attacks against the organization. The need for tracking internal IP addresses and internal IOCs is an interesting perspective that Gartner analysts Oliver Rochford and Neil MacDonald propose in their research note "The Five Characteristics of an intelligence-driven SOC". Threat intelligence also requires a platform not only to capture the IOCs, but also to apply it in the context of internal event information.



Security Orchestration- Closing the Response Loop

While detecting more threats is just one aspect of enhancing a SOC, responding quickly to block an attacker's access is equally important. In the case of a targeted attack, an attacker's dwell time could vary from weeks to months. While their activities may prompt security solutions to detect alerts, poor response capabilities enable attackers to stay on the network for a lot longer until a large breach occurs.

Usually, the need for improving response capabilities does not get the attention it deserves. Advanced SOC, however, can enhance response capabilities by focussing on the following areas.

> "Not all alerts are created equal. They need to be seen in the context of each organization. Only then can SOC teams focus on critical alerts for investigating further and for remediating the threats."

REDUCING NOISE THROUGH AUTOMATED TRIAGE

It is common knowledge that a SOC can get flooded with alerts. As a result, SOC teams get overburdened and miss out on alerts that lead to security breaches. The first challenge in achieving a faster response time is to prioritize these alerts.

Not all alerts are created equal. They need to be seen in the context of each organization. Only then can a SOC team focus on critical alerts for investigating and remediating threats.

For example, a DLP alert is commonly triggered based on keywords configured by an organization or by fingerprinting certain type of documents. This leads to a high number of false positives. One way to triage this would be to look at the historical information on the desktop's outgoing data over a period of time correlated with a DLP alert and any alert from an anti-malware on the same desktop.

The context of the desktop user can also be correlated to understand, for example, if the user is a contractor or an employee in exit phase. This leads to improved rescoring or prioritization as compared to only the DLP alert being looked at in an SIEM console or DLP console.

As a generic approach, the triage process needs to take into account the following aspects:

Context Related Parameters

Every alert needs to be scored based on its asset, user, vulnerability, and network context. The asset context scoring is based on what the asset is, how critical it is to the business, and the value of data stored or processed by it. The user context scoring similarly is based on what level of privileges the user has on systems, how sensitive the user role is in the organization, and what the user status is (employee, contractor, separated, etc).

The vulnerability context scoring is based on the status of the vulnerability relevant to the threat alert. Finally, the network context scoring is based on the sensitivity of the network segment, how often the alert appears, and its likelihood to propagate to more critical assets.

History of the alert

Given that most targeted attacks will be a campaign and not just a one-off attempt, each alert should also be prioritized based on what was observed in the past. From historical data, alerts can be score-based on its occurrence in the past, its prevalence across assets, its deviation from normal volume, and its linkage to other alerts that potentially forms the cyber kill chain.

Threat Intel

One application of threat intelligence is to detect attacks using analytics as described earlier. The other usage of threat intelligence is to prioritize alerts. Alerts containing bad IPs, URLs, and known IOCs need immediate attention, so should be scored higher.

While these parameters are common across organizations, the way to combine, assign weight, and score them will be custom for each organization. An orchestration platform should have the capability to pull in data related to context, history, threat intelligence, and automate the scoring of alerts for faster triage.

Similar triaging can be done on IPS or WAF alerts by correlating the alert to the existence of the corresponding vulnerability, the value of the asset being attacked, and threat intelligence related to the attack source. While SIEMs have this capability they are limited by the lack of dynamic context integration.

Vulnerability information, for instance, is not static. It is constantly changing as new vulnerabilities are discovered in different online platforms every day. Similarly, asset components and services keep changing and corresponding vulnerabilities change accordingly. So, vulnerability information is a moving target.

SIEMs have tried to solve this by looking at vulnerability information as static and, as a result, have not been effective in correlating vulnerability data with the attack. In practice, this means that there should be a mechanism that enables the system (SIEM/supporting technology) to use available vulnerability information to predict if a specific vulnerability exists corresponding to the event that is being analyzed. This can lead to successful triaging based on vulnerability and asset data. A blog on dynamic context information can be found at: http://www.paladion.net/spatial-intelligence-soccer-and-security-monitoring/

Automating Investigation and Remediation

Once an alert comes up with a high triage score, it needs to be investigated by SOC analysts. Investigation primarily answers four questions -

- What are the attacker attributes (who is the attacker, what else can be known about their techniques, tools, and tactics)?
- What is the damage on the asset?
- Is it just one incident or part of a past campaign?
- If it is a campaign attack, what are the collateral damages and what other systems are impacted?

Rushing to mitigate an alert without answering these questions will only address the symptoms; it will not remove the root cause. Investigation can be very time consuming as it requires time and effort to collect data from various sources and additional tools to analyze the variety of high volume data.

It is typically easier to answer these questions if there is a platform to quickly pull in data from various sources in an automated manner and to provide a single window for data analysis. Also, some of these questions are easier to analyze visually through techniques such as tree maps, linked node graphs, scatter plots, and bubble charts. For faster investigation, organizations need to have a security orchestration platform that can automate these tasks.

SOCs must also build run books to respond to commonly known attacks, to ensure that investigation is thorough, and the response is not dependent upon the skills of the analyst alone. The run book can be automated through workflow tools or built into an orchestration platform that has workflow management. This makes it easier to manage known attacks as they occur and frees up the SOC team to work on advanced attacks.

Security Structure - A Final Word

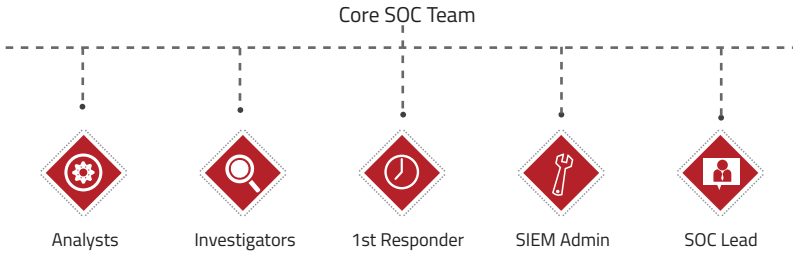
Applying security analytics and orchestration will necessitate a change in the roles and structures of SOC teams. Most SOCs have the traditional hierarchical organization structure with analyst (L1 response), senior analyst (L2 response) and SOC lead (L3 response). This structure worked well when attacks were more uniform.

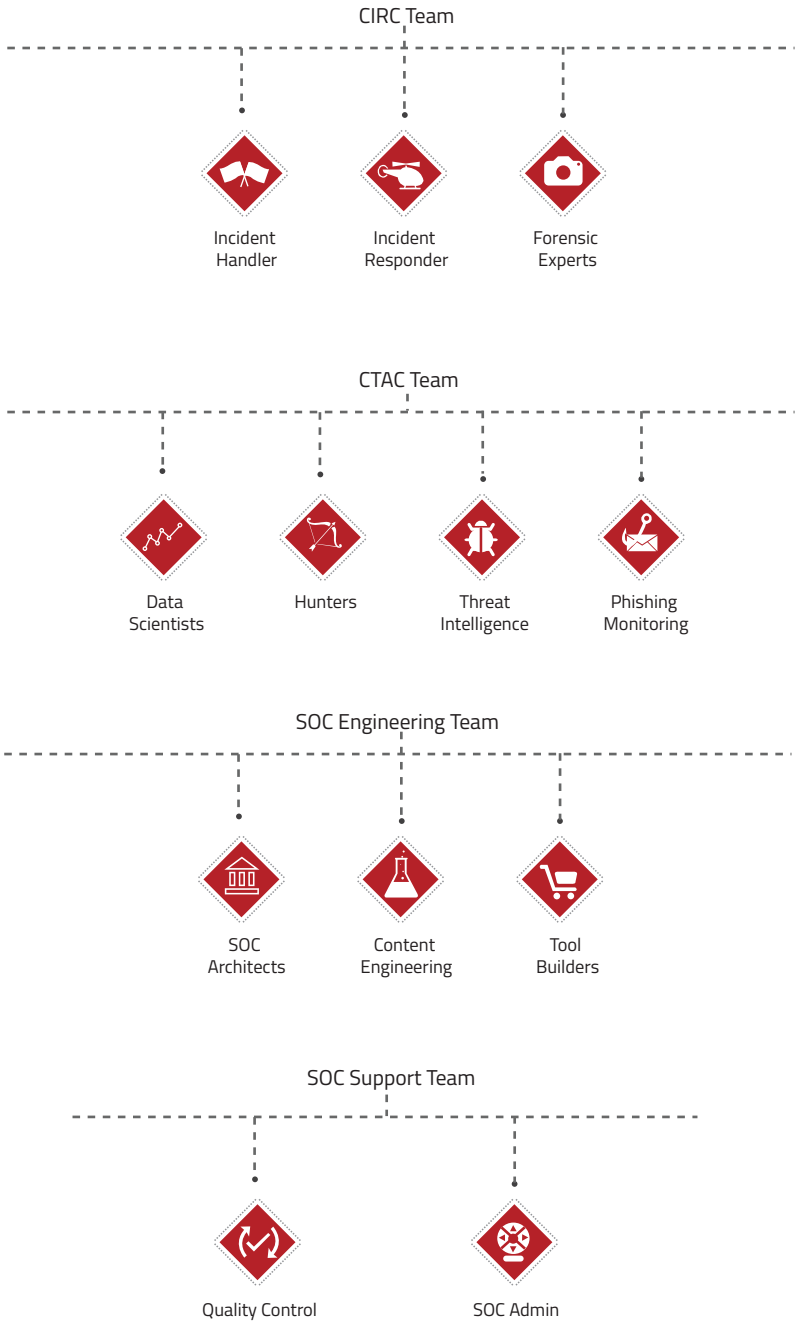
The current threat landscape has increased the number of roles in a SOC and broadened the skill requirements. There are attacks ranging from known to unknown; attacks at infrastructure/application/data layers and attacks that vary based on the technology being targeted.

Each of these attacks requires different types of detection and response mechanisms. In this context, expecting an analyst to manage all the variations based on seniority is not reasonable.

SOC roles need more specialization including analysts, hunters, threat intelligence experts, incident responders, data scientists, content authors, forensic experts, and technology specialists. There is a need for more integrated horizontal teams as opposed to a vertical hierarchy.

Based on these next generation SOC requirements, a proposed SOC structure is given in the diagram below. CIRC stands for Cyber Incident Response Center and CTAC is Cyber Threat Analytics Center.





Summary

Adding security analytics and orchestration capabilities helps improve a SOC's capability to counter targeted attacks. These capabilities need improved use cases, additional technology platforms and new sets of roles in a next generation SOC. Once implemented, they increase the depth of detection, improve response times, and help set up effective defenses against targeted attacks.

Paladion's CyberActive℠ Solution

Paladion's CyberActive℠ service provides customer specific security analytics implementation, based on your unique use cases. User specific implementations combined with our global threat monitoring network, analytics engine, and orchestration platform can significantly improve your capability to detect and respond to targeted attacks. Contact Paladion today to see firsthand how CyberActive℠ SOCs can help you swiftly detect and respond to, sophisticated targeted attacks in your environment.

Bibliography

Oliver Rochford and Neil MacDonald, The *five characteristics of an intelligence-driven Security Operations Center*, Gartner, Nov 2015

Oliver Rochford and Craig Lawson, *The five models of Security Operations Centers*, Gartner, Oct 2015

The National Cybersecurity Workforce Framework - NIST, National Initiative for Cybersecurity Education, 2013

Carson Zimmerman, *Ten Strategies of a world class CyberSecurity Operations Center*, The MITRE Corporation, Oct 2014

The cost of malware containment 2015, Ponemon Institute, Jan 2015

M-Trends 2015: A View From The Front Lines, Feb 2015

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by independent analyst firms and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668

Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net

PALADION