Preparing Through Prediction

Target Audience: CISO, VP of Corporate IT & Security, Director of Security Operations

The average cost of a security or data breach for corporations and enterprises is $3.62 Million according to the Ponemon 2017 Cost of Data Breach Study. This includes the impact to a corporation's internal personnel, processes, practices, and customer trust. The cost of a security or data breach along with the increasing number of evolving security threats and vulnerabilities is compounding daily and is a consistent worry for organizations from the security teams up to the board of directors. CISOs and their SOC teams work to safeguard their ever-changing environments, but bad actors are continually adapting—detecting unknown vulnerabilities in the latest technology, security devices, encryption methods, or network protocols. The prevailing method to combat security threats and vulnerabilities has been to implement a defense-in-depth strategy implementing preventative systems and devices to control access, enhance visibility on devices and network traffic, and minimize the exposure of the enterprise to security risk. The result has been a sprawl for the security infrastructure that continues to grow with expanding corporate networks, systems, and devices. Today CISOs and SOC organizations recognize that breach is inevitable. It is no longer a matter of if it will happen, but when it will occur and to protect against the long term impact of a breach – downtime, regulatory action, loss of reputation – you have to predict what may happen in the event of an attack and be prepared to make the fixes required to get back to business. and how quickly can they can respond to contain the damage.

LOGS, DATA, INFORMATION, AND THE SOC

As technology has evolved, security threats and vulnerabilities have also increased exponentially. Every day there are new threats being developed to exploit weaknesses in systems, devices, and software. Over the past five years, SOC organizations have implemented security information and event management (SIEM) technology to capture information coming into their enterprise network. This approach no longer works.

SIEM technology has allowed organizations to actively capture event information across their network and programmatically review the events. In the review of the events, the hope has been to detect vulnerabilities or threats that may have compromised the network to gain access or steal corporate data and information. The amount of data and logs from individual sources, such as firewalls, gateways, IPS, and IoT devices, is unmanageable for security teams. The data collected can provide several thousand events of information which multiplies daily and can overwhelm organizations with hundreds of individual personnel specifically designated to monitor, capture, mitigate, and remediate vulnerabilities and threats. SOC personnel are often tasked with manually reviewing these logs and attempting to identify anomalies or malicious attempts at network access. It is virtually impossible for a SOC engineer to manually review these logs and expect a high level of confidence in their security methods.

The utilization of a SIEM solution is imperative within a SOC environment to monitor the event data from the security infrastructure. While automation and event correlation provided by SIEM is extremely useful, is it also reactionary. The sophistication of today's attacker has forced security teams to move beyond responding to events and incidents and to hunt bad actors lurking on their networks. To do so CISO's recognize that they require data and information to predict future attacks. In typical attacks upon

networks there are signals and indicators from attackers that they are looking or probing networks to identify areas of weakness. This is standard. Attacks are not random. Attackers often scan a series of networks and identify one specific vulnerabilities or weaknesses to exploit. Once the weakness is identified, attackers will focus on the exploit and attempt to access any information that is available. At times it can be malicious. At times it can be exploratory. In all cases, this is a critical security threat to the enterprise.

For security threat analysts, the behavior of attackers is an endless weave of patterns, algorithms, and behavior. The ability to identify and act upon the uncovered information is the key for security teams. The quicker we identify an attacker, the faster we can contain his activity and remediate. Security teams are now combining the real-time data collected from their own networks with threat intelligence provided by outside sources to reliably predict threats to their organization. They are using predictive analytics to enable this feat. Predictive analytics is the new method to combat security threats, vulnerabilities, and exploits.

WHAT IS PREDICTIVE ANALYTICS?

Predictive analytics within cybersecurity is the ability to use data and information and anticipate likely actions a bad actor may take against the organization and uncover any ongoing attempts to breach the network. Predictive analytic models digest threat intelligence feeds from a variety of sources including social networks, the dark web and provide enhance the context of network data from the organization's SIEM. This information enables the SOC to identify anomalies in patterns of behavior by employees and systems that access information within the network.

Advanced analytics techniques are applied to the large volumes of monitoring data gathered from the infrastructure to achieve this level of monitoring. By ingesting detail of events such as date, time, length of activity, pattern of activity, size of data transferred, resulting behavior, and functions performed, predictive algorithms are developed and the machine learning is tuned. Most functions or behaviors within an organization are standard, regular, and performed to complete jobs and tasks daily. As such, the predictive algorithms uncover anomalies within this routine behavior.

The SOC uses predictive analytics to identify and respond to irregular behavior. For example, if every Monday at 11:00 GMT the network receives a scan of approximately 20 random IP addresses on a network from an unidentified source, this could indicate a singular event that needs to be monitored. The action would be to block the source. But if the scan happens each Monday from a different source, this could be an event that needs to be tracked and investigated further to see who is triggering the scan against the network. While the number of IP addresses scanned is relatively small, this is in fact a portion of a larger assault, designed specifically to go undetected. In this case, predictive analytics would identify this specific behavior of date, time, amount of IP address, and possibly ports scanned to raise an alert to a SOC that the event is happening and continuing. The pattern is then identified and becomes part of the monitoring matrix within the SOC. An investigation would occur each time this happens and attacks can be prevented with background, knowledge, and a previously defined method of remediation.

Predictive analytics is not only used for awareness of threats and attacks outside of the enterprise. It can also be used to detect insider threats and weakness. Insider threats are attributed to many of the attacks affecting corporations in today's world of cybersecurity.

Predictive analytic models enable a SOC to identify anomalies in patterns of behavior by employees and systems that access information within the network. Advanced analytics techniques can be applied to the large volumes of monitoring data gathered from the infrastructure to provide the accurate insight into potential anomalies. This includes employee edge devices, network appliances, servers and their respective inter-system communication. It will detail date, time, length of activity, pattern of activity, size of data transferred, resulting behavior, and functions performed. Predictive algorithms are developed as a result and the machine learning is tuned. Not all patterns and behaviors are malicious or unexpected. Most functions or behaviors within an organization are standard, regular, and performed to complete jobs and tasks daily. However, the underlying goal of predictive analytics is to identify anomalies.

MAPPING THREATS TO CRITICAL BUSINESS APPLICATIONS

Anomaly detection is a core objective of today's SOC. Each person and system within the SOC is tasked with finding the known and the unknown. Systems are required to detect known threats from across the cybersecurity landscape. Systems are also in place to identify the unknown for further investigation by personnel. Predictive analytics allows anomalies to be investigated and categorized as potential threats or regular behavior. This does not solely happen through machine learning and the system performing all actions. The SOC personnel must review, investigate, classify, and prioritize the anomaly. Predictive analytics is best used when SOC engineers have been taught how to utilize the implemented system, understand the output, and have a process and procedure to investigate its findings. Predictive analytics systems and implementations will be able to identify the severity 1 or severity 2 anomalies, but if there are several of each, these must be prioritized. The SOC systems can be programmed to identify the severity and importance of systems, devices, networks, or data locations. This can be based around usage patterns, availability needs, SLA requirements, or workplace recommendations. The detection of outliers and anomalies allow SOC personnel to be more productive and to keep their focus on the events and incidents that require investigation.

Predictive analytics allows organizations to implement an additional level of visibility and security inside their organization. As vulnerabilities are exploited, the threat can move within a network vertically and horizontally affecting locations, systems, and devices. Advanced analytics provides security organizations with an ability to support its infrastructure and business applications by detecting the threat and alerting security engineers of areas to quarantine from the threat. As millions of events are received within a SOC through logs and data, it is imperative for the SOC to have effective tools to combat threats and to protect the enterprise. With a proper implementation of advanced analytics, prioritization within the SOC can occur from incidents that are raised or anomalies that are detected. Through the addition of business intelligence systems, security engineers can reduce the amount of time spent on lower level alerts and incidents and focus on immediate occurrences and threats to investigate. Intelligent advanced analytics and prioritization in mature SOC organizations give threat analysts the ability receive prioritization of threats programmatically. The ability to reduce the work required by a security engineer to investigate, mitigate, and remediate a threat is critical to corporations. Added efficiency, increased awareness, accurate application diagnosis, and documented operational procedures create a mature SOC to effectively combat threats and protect the enterprise.

Machine learning is a technological benefit to mature SOC organizations. Analysts often struggle with the number of alerts and events received in corporations. Alert fatigue can demoralize and decrease the

productivity of a SOC. Security groups have terabytes of data and information that must be processed. Through the amounts of data and information that is gathered, there are thousands of events and incidents that are raised daily for security analysts to investigate. Advanced analytics can help analysts directly address the incidents that have a higher severity and threat assessment. It reduces the amount of noise and false positives within the SOC to improve the security posture. An implementation of advanced analytics can create an environment of intelligent awareness and increased operational workflow to investigate and mitigate threats quickly.

The combination of trained SOC personnel and predictive analytics allows a corporation to increase their confidence in their security posture. The SOC personnel can provide feedback and insight to help systems learn the patterns and behaviors that are inside and outside the enterprise. The personnel can help the system prioritize the events detected for increased efficiency within the SOC and within the corporation.

Predictive Analytics and The Enterprise

CISOs and the C-Suite have now identified that the approach to protection of cybersecurity attacks through prevention is not the only reasonable stance in today's cybersecurity world. The landscape has changed. Attacks will happen. Breaches will occur. The question is not "if" but "when". Company's now want to be aware as to when attacks and data breaches occur, contain and remediate the attack or breach, but they also want to ensure that if they happen it does not happen again. Company's also want to utilize the depth of information collected within the security organization to be aware of not only current events and incidents, but also use this information to predict what may happen in the future. The use of information, data, and logs from inside and outside the enterprise can provide valuable insight into the security posture of an organization. Through gathering data and machine learning, predictive analytics can be applied to organizations to identify potential attacks, threats, or irregular behavior. These anomalies in today's business can help organizations develop better internal process, procedures, and training for internal employees and staff and can also help organizations implement security measures to better protect themselves from exploits and vulnerabilities. Improved organizational efficiency Predictive analytics helps corporations increase the security for their organization, provide better tooling for SOCs, drive refinement of internal security policies and procedures, and protect the enterprise from insider threats and external vulnerabilities and attacks.