8 Must-Haves for Detecting Advanced Attacks

There is no possibility of complete protection because cybercriminals are resourceful and relentless. Their tactics are continually being refined not only to increase effectiveness but also to remain undetected for as long as possible. But even though perimeter defenses will be breached, organizations can aggressively hit back at cybercriminals with machine learning-based security analytics. Below are the must-have tactics organizations can use to quickly detect attacks on the inside and severely limit the damage they can do.

#1: Use Machine Learning

With the massive number of potential threats being flagged by security monitoring systems, it's no wonder that analysts are suffering from alert overload. Forget about trying to connect the dots and discovering multi-stage attacks. Just deciding which of the events need investigation is a daunting challenge. For example, of the 166 million security events at the 2012 London Olympics, only 783 required investigation! When working with data at such massive scale, machine learning is the only way to effectively offload the work of accurately identifying the security events that need human attention.

#2: Do it Automatically

Profiling across time and detecting advanced attacks should happen continuously and automatically. It's not something that security professionals (who are in extreme short supply) should have to manually initiate. Given that cyber attacks are constantly evolving, it's important to automatically identify changing attack patterns without the need for labeled training samples. That means unsupervised algorithms, which can learn without the need for human intervention, must be integral to any machine learning-based defense against cybercriminals.

#3: Leverage Big Data

Big data democratizes capabilities previously reserved for organizations with huge security budgets. Low cost distributed computing enables advanced machine learning analytics, data correlation, and rapid search across massive volumes of data from disparate sources. Low cost storage means relevant security data can be retained for far longer time periods than what's possible with traditional security monitoring solutions. This enables analysts to perform historical impact assessments and threat hunting further in the past, important given that the median time to discover advanced attacks is currently 205 days.

#4: Integrate with Existing Infrastructure

You've likely spent heavily on security and IT, so any solution for combating advanced attacks should leverage these investments. Logs should be ingestible natively from the source (e.g., DNS logs) or from a SIEM. The solution should be able to stand on its own but not everyone

is open to yet another management console. So APIs that make it easy to incorporate your security analytics solution's output into the console of your choice (e.g., your SIEM console) is a must.

#5: Fuse Relevant Security Data

Organizations have vast troves of packet, flow, log, file, alert, and threat feed data that can yield intelligence for thwarting cybercriminals. How? Correlate data so it is attributed to a user, or a host, or an application. Then distill it into summaries that provide rich context (e.g., authentication and device usage histories, port-protocol relationships, etc.). Security analytics that use varied security data sources provide better visibility than do analytics using a single data source. And with correlation and distillation, security professionals are better positioned to ferret out hidden adversaries.

#6: Profile Across Time

Multi-stage attacks stay under the radar by performing actions that individually do not rise to the level of a security alert. To detect these attacks where the markers do not rise above the noise requires looking across time, generally over extended periods, and stringing together seemingly unrelated actions.

#7: Maintain Layered Forensics

Even with automatic machine learning-based systems, security professionals' intervention is required. They will need to perform spot checks to ensure that the defense systems are working properly and also to make the final determination on whether an event is real. Forensics provide security analysts with the context as to why something was flagged. But forensics should include not just packet data but also machine logs, packet header analysis, the time history of actions, outputs from machine learning algorithms, and more. Hence the term layered forensics.

#8: Ensure Rapid Search

"Have my defenses been breached?" is a question that security analysts must be able to quickly answer. This is enabled by rapidly testing many hypotheses, which requires search, coupled with forensics to provide the context, across the raw data and any computed data. But given the magnitude of data inundating organizations, and the silos within which it typically resides, search is often a tedious exercise in time wasting, and grinds to a halt. So any search must happen across massive amounts of data, executing rapidly without degrading the performance of the existing security infrastructure.

About Niara

Niara's security analytics platform delivers contextually relevant security analytics by fusing network and security data to discover compromised users and malicious insiders, perform advanced threat hunting and conduct incident investigations. Headquartered in Sunnyvale, Calif., the company is backed by NEA, Index Ventures, and Venrock. For more information, visit www.niara.com.