VECTRA®

IDS meets data science, machine learning and behavioral analysis

Dangers of the cybersecurity gap

The traditional approach of IT security has been based on two core ideas.

First, build an impenetrable wall of prevention that keeps any and all threats out of the network. Second, save the logs from all those prevention layers in case you need to analyze them as part of a post-mortem or forensic analysis.

As a result, there's a dangerous cybersecurity gap between the prevention and cleanup phases, during which an attacker has free reign to patiently spy, spread, and steal within the network.

By ignoring the active phases of cyber attacks that occur between prevention and cleanup, security teams have ceded the upper hand to attackers.

Intrusion detection and prevention systems (IDS/IPS) that are nominally dedicated to stopping modern threats are increasingly incapable of stopping them. Armed with custom attack tools, malware and social engineering techniques, cybercriminals easily outwit IDS/IPS.

The dependence of IDS/IPS on simple, fast-matching signatures is at the heart of the problem. The bad guys mount a new threat, the good guys respond with a patch or signature. The bad guys then slightly modify their attack to avoid the signature, and the cycle repeats, with security always a step behind.

Where do we go from here?

IDS was once its own security discipline, but over the years it was gradually subsumed by intrusion prevention. Today, IDS is simply an IPS deployed in listen-only mode.

IDS detection logic is based on quickly matching traffic to known indicators of a threat. But because IDS/IPS is tuned for performance, it is limited to a subset of detection techniques that can be performed quickly and with limited recall.

Unfortunately, the number and sophistication of new threats and intrusions continue to grow to the point where it's impossible to keep up. A new generation of IDS is needed to restore detections as the top priority.

Rather than clinging to a subset of IPS features, IDS must be reimagined as the intelligence that detects network threats, while IPS handles the enforcement of security policies. The new generation of IDS becomes the metaphorical brain while IPS remains the muscle behind enforcement.

To meet today's challenges, this new generation of IDS requires a new detection model that blends modern detection strategies and techniques, including the ability to identify threats even if no malware or exploit is used.

IDS visibility must extend inside the network perimeter to internal segments where intruders lurk. The new generation of IDS also requires sufficient time and resources to identify the progression of an attack.

What's in store for IDS?

Instead of deploying IDS at ingress and egress points, it must monitor all east-west traffic on internal network segments and north-south traffic along the Internet boundary.

This visibility into internal as well as Internet-bound network traffic is a requirement to detect cyber attack behaviors, such as internal reconnaissance, lateral movement, unauthorized data access and the staging of data for exfiltration.

To detect more sophisticated attacks that use encryption, signature evasion and perimeter avoidance, IDS must shed its reliance on traditional threat lists because they are often limited to searching for malicious payloads.

Modern attackers have caught on to this and are turning to new exploits, modifying tools, repackaging malware, and using new IP addresses and URLs to avoid detection.

That's why traditional IDS models must shift their focus to detecting underlying attack behaviors. By identifying attack behaviors, security teams can reliably detect network intrusions, even if the tools, malware or threats are unknown.

For example, detecting modern threats requires recognizing the unique behaviors of command-and-control traffic – one of the tell-tale signs of a malicious intruder – despite the application being used.

Similarly, IDS must be able to identify malware that is requesting instructions as well as malware that is updating the binary code – again, no matter what type of application is utilized.

The new detection model

The new detection model – automated threat managment – uniquely combines data science, machine learning and behavioral analysis. Together, they identify the underlying purpose of traffic, detect attack behaviors in real time regardless of application and if encrypted, and automate the management of detections by correlating threats to hosts.

Instead of analyzing event logs from other devices, automated threat management applies algorithmic models directly to network traffic to reveal underlying attack characteristics that wouldn't otherwise be visible.

To keep the automated threat management model current and dynamic, data scientists constantly analyze new attack samples from the research community and review data from customers who share metadata.

This helps uncover new and emerging attack behaviors and trends to develop new algorithms, and continually verifies supervised and unsupervised machine learning algorithms that benefit worldwide organizations.

Dealing with encryption

By focusing on the unique actions and behaviors of cybercriminals instead of malicious payloads, the automated threat management model can identify in-progress attacks without decrypting SSL/TLS traffic.

Automated threat management algorithms continually reveal the underlying purpose of traffic, even when the payload is not visible – a critical distinction because it allows security teams to protect without prying.

In addition, automated threat management models can detect and analyze miniscule fluctuations in protocols like HTTPS, HTTP and DNS, and reveal when additional layers of communication are hidden within them.

Vectra research shows that HTTPS is the most popular protocol for these hidden tunnels. And by detecting threats without decrypting traffic, it's possible to mitigate attacks without any performance penalty or privacy issues.

Taking the next step

Since attackers are as relentless as they are sophisticated, it's up to information security professionals to raise their game and recast the role of intrusion detection in their security infrastructure arsenal.

Automated threat management closes the dangerous cybersecurity gap in the wake of IDS by combining data science models, machine learning techniques and behavioral analysis.

By closing this gap, information security organizations can successfully disrupt the pattern of attack-and-response escalation between good guys and bad guys, and finally give the good guys the upper hand.

It's time for IDS to detect intrusions again

Download this white paper for a deeper dive into traditional and new approaches to intrusion detection, and how they measure up to today's advanced cyber attacks.

VECTRA®

Email info@vectranetworks.com **Phone** +1 408-326-2020 www.vectranetworks.com