Attack Intelligence: Why It Matters

WHITE PAPER

Core Security
+1 617.399-6980
info@coresecurity.com
www.coresecurity.com
A Proactive Strategy

Attacks against your organization are more prevalent than ever, with the resources required to execute these attacks available to anyone. In spite of numerous information security innovations, companies continue to struggle to protect their most critical assets. These could be patient medical records, credit card data, or an industrial control system, to name a few. What can you do to stop these attacks and how can you lower your risk? Simply running periodic vulnerability scans, monitoring security events, and tuning device configuration is not enough. In fact, the result is a mountain of data, requiring time and valuable resources to process.

The long-standing, reactive method of detecting and responding to incidents has steadily become less effective in recent years. To combat this, organizations are attempting to reduce the time it takes for them to detect an incident and effectively respond to it. Unfortunately, no matter how fast they respond, the process of acting only after an incident has occurred leaves organizations with an unnecessarily high-risk profile. A better approach is to anticipate an event before it happens in order to prevent the attack from ever occurring. This more proactive strategy focuses on identifying and eliminating potential attack paths to your critical business assets before they can be exploited.

With the Core Security Attack Intelligence Platform, your staff can better focus their energies on analyzing and remediating real threats and implementing new security controls, while requiring far fewer FTEs and person hours to manage these processes. In recent deployments, attack intelligence has demonstrated the ability to reduce tens of thousands of potential vulnerabilities from multiple scanners by more than 90% to produce an actionable set of likely vulnerabilities based on consolidated vulnerability data matched with known exploits.

Consolidate & Prioritize Vulnerabilities

Knowing which systems on your network are potentially vulnerable to attack isn’t enough. This could be thousands of vulnerabilities from different scanners, which can easily overwhelm an already resource-stretched information security team.

The Core Attack Intelligence Platform (Figure 1) offers an antidote for the data overload that’s common with traditional vulnerability management and assessment solutions. It creates a closed loop between vulnerability scanning, security testing, analysis and remediation.

To identify the most likely risks to an organization, the Core Attack Intelligence Platform performs the following three steps:

**Consolidates** – Modern security tools produce a flood of data and alerts resulting in data overload and resource limitations. Attack intelligence solves this challenge by collecting, managing and correlating raw network, web and client-side security assessment data across multiple locations and vendors and presenting it in a single dashboard. It also allows for continuous monitoring of enterprise risk by consolidating data across multiple threat vectors based on campaigns built to an organization’s operational risk profile.
Analyzes – Information does not equal intelligence. That’s why even organizations with pages of vulnerabilities fall victim to attacks; even those that are matched against known exploits. Intelligence is gained when context is applied to information – giving it meaning and operational significance. Attack intelligence correlates and derives intelligence from consolidated security data, system interdependencies, and previous attack methods.

Prioritizes – Traditional vulnerability management solutions often produce thousands of “high severity” vulnerabilities for the operations staff to fix. Attack intelligence adjusts prioritization based on the systems that are part of these paths and the assets they put at risk. This approach narrows the remediation process to the most critical vulnerabilities, freeing up both information security and IT operations resources.

Think Like An Attacker

While most organizations spend their time considering their defensive security posture, it’s critical that information security teams visualize their environment in the eyes of an attacker. This means understanding how an attacker views your defenses, and knowing the optimal attack paths to critical business assets. These assets could be anything that is important to the health of your business such as customer credit card data, an enterprise resource planning system, or patient data. Attackers usually have a goal in mind and it's up to you to understand how they will achieve it.

The Core Attack Intelligence Platform helps you Think Like An Attacker™ and narrow your focus on the most vulnerable points of your network and applications. Through a patented attack path engine, the platform correlates known exploits of vulnerabilities and actual attack patterns with security and network data to form potential attack paths to critical business assets.

Attack intelligence exposes the dynamic paths attackers might take to get to their high-value target. Unlike traditional vulnerability management, network management, or security analytics solutions, attack intelligence doesn’t leave anything to interpretation. This attack-based approach allows investigation of multi-staged attacks that pivot across systems, devices and applications, revealing how chains of exploitable vulnerabilities open paths to your organization’s mission-critical systems and data. These paths can be validated through advanced testing included as part of the attack intelligence platform. As a result, organizations with an attack intelligence solution in place know exactly how an attacker can reach their critical assets and what is needed to protect against these attacks.

An example: Traditional solutions will consider a vulnerable print server to be a non-critical asset – very low on the patch/remediation priority list. In this case, the attack intelligence solution instantly discovers it is on a path to other critical assets, and elevates the print server’s priority. The information security team is alerted for subsequent validation and remediation. Most traditional solutions would ignore the print server, even though a savvy attacker could easily use it as a pivot point to reach their goal.

In recent deployments, attack intelligence has demonstrated the ability to reduce tens of thousands of potential vulnerabilities by more than 90% to produce an actionable set of likely vulnerabilities based on consolidated security data already existing in your enterprise.
Extensible Attack Intelligence Platform

The Core Attack Intelligence Platform can leverage data from other security solutions including Network Security and Configuration Management, Vulnerability Management, and/or Security Information and Event Management (SIEM). The result of this extensibility is a greater return on investment from your existing security solutions.

Out-of-the-box integration with leading infrastructure vulnerability testing platforms means that the Core platform can be configured to start analyzing your organization in minutes. Integrated penetration testing and attack path generation allows your staff to see which combinations of vulnerabilities increase your risk and which attack paths might be used to exploit a known vulnerability.

Security Analytics

Burned time and again by low and slow moving “advanced” attacks, many organizations have already made the leap to security analytics solutions with real-time, full packet capture and event analysis. As powerful as these tools are, they only solve part of the problem. Organizations benefit little from the (considerable) investments in such platforms if they are repeatedly reacting to suspect incidents and chasing down potential offenses.

The combination of attack intelligence capabilities with security analytics solutions allows incident responders to quickly act on information gained while simulating and testing your entire network for other possible targets and attack paths. The Core Attack Intelligence Platform provides context for security analytics solutions by refining events and alerts related to high risk devices along attack paths. IT staff can help sort through alerts and log data from their security analytics solution and focus on what they know are the highest risks to their most mission critical systems.
The Core Attack Intelligence Platform, as shown in Figure 1, provides:

- Attack path planning and simulation leverages patented AI algorithms to show how an attacker can reach your most critical assets.
- Open API that provides the ability to integrate with other security solutions, focusing them on the most vulnerable points of your infrastructure.
- Automate vulnerability validation to continuously assess the security of your organization.
- Prioritized remediation efforts for vulnerable systems that are on attack paths leading to critical assets.

**Summary**

Today, many organizations rely heavily on a “detect and respond” strategy to secure their most critical business assets. While detection of incidents is becoming more real-time in practice, this approach still requires that information security teams react quickly to prevent significant breaches. The result is a slightly improved, yet still potentially high, risk profile. Attack intelligence consumes various security data such as vulnerability data, security events, and configuration data to provide a consolidated view of potential attack paths to your most important data. Applying this knowledge, you can take a proactive approach to information security and further mitigate the risk of an actual breach.

With the Core Attack Intelligence Platform, organizations can prevent attacks by consolidating multiple vulnerability scanner feeds, analyzing based on known exploits, and prioritizing the most critical vulnerabilities for remediation. Further, by simulating potential attack paths through your IT infrastructure, organizations can efficiently and effectively protect their critical assets.

This is what it means to *Think Like An Attacker.*