Huntsman's "Defense-grade security platform" Challenges the U.S. SIEM Market with Its "Automated Threat Resolution"

Abstract

Huntsman Security, founded in Australia ten years ago, entered the U.S. security information and event management (SIEM) market in 2015. Its mature security platform counts defense, intelligence, and national infrastructure deployments as customers, and several of its solutions address organizational information and operational silos and disparate security intelligence tools and communications to its ultimate goals of achieve more accurate and faster incident response.

Huntsman Enters U.S. with New SIEM Tools

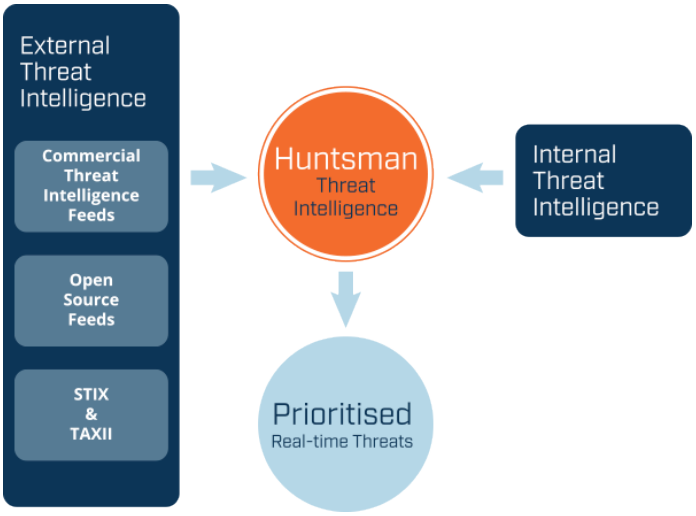
Huntsman's entry into the North American market coincided with one of its two latest product updates in the first half of 2015. The first is the Huntsman Unified Console, which delivers consolidated access and a cohesive, consistent view into an organization's security functions, including legacy security software and services and various internal departments. The console integrates multiple security views and information sources into one dashboard for security teams.

The company's other new release of 2015 is the Hunstman Analyst Portal, which tackles the common backlog of enterprise threats by automatically investigating alerts to provide corroborating evidence of the real threats and prioitizing them while simultaneously sorting out the false alerts and deprioritizing them, lets analysts focus their time on the key issues.

The functionality of these products is designed to automate many of the routine tasks of threat management to free up security teams to resolve actual threats. The technology also triangulates security information from multiple sources to deliver only verified credible information. Huntsman's security software also contains its own embedded incident management system so customers do not have to have additional solutions to manage security and supports integration with other systems so customers with existing systems do not have to change their processes.

Envisioning Unified Security

As malware and system attacks proliferate, so too do security incident and event management products. Organizations of every size are awash in threat information culled from a huge variety of events, and they are often stymied in trying to pinpoint and take action against real threats. Security solutions are often limited in their ability to interpret the threat information that is gathered, and many organizations cannot address all the collected data with the in-house resources on hand. There are often significant delays between the threat incursion, the identification of the threat, and the business's response to it. Too many manual processes are an obstacle to actionable threat response, wasting valuable time and increasing resolution



costs. Siloed IT and security departments exacerbate the security challenges; these old structures cannot meet the real-time demands of threat detection and action.

Huntsman uses its patented Behavioral Anomaly Detection, which is based on machine learning, to identify the real threats for security teams. The tool uses information collected from various data sources and corroborates the alert(s) by scanning the suspect endpoint and instantly evaluating the registry, memory, file systems, OS, and other aspects, thus producing only hi-fidelity actionable items. It also uses the endpoint agent interrogation to present information through continuous monitoring and reporting dashboards that are aligned with governance, risk, and compliance initiatives.

For security analysts, false positives obscuring the real issues are one of their largest impediments. Huntsman designed its Analyst Portal to remove false positives using the data from its endpoint scans. The scan correlates the alerting system and the end system for a continuous and complete process, and in doing so, emulates the actions of an advanced analyst to validate all incoming alerts, becoming a force multiplier for overburdened and/or underskilled teams. The Analyst Portal scans a wide range of systems extracting and indexing indicators of compromise (IOCs) such as data malware, collection/exfiltration, lateral movement, and command and control methodologies. When a malware artifact is captured, it is catalogued and channeled into a safe storage space for later analysis.

The Analyst Portal eliminates false positives and negatives and compiles and prioritizes case files for the threats that do matter. It also adds details in the case file and creates a summary report that can be tailored depending upon appropriate details to be shared—something particularly important for security clearance situations. Additionally, Huntsman's entire system uses role-based access control. The end result is faster and more accurate security decisions, shorter threat queues, and a far shorter time at risk—seconds, rather than hours or longer. This reduces the dwell time for attackers as well as numerous costs associated with breach response and forensics.

EMA Perspective

Huntsman Security's entry into the U.S. security field is an intriguing addition to the current anomaly detection, threat detection, and incident response markets. As a mature company, Huntsman can draw on its experience to direct its innovation around its advanced anomaly identification engine. Because it already has a solid customer base in Australia and the UK using TTS tools in mission-critical deployments, including many in defense and government as well as policing and border protection, it can show U.S. prospects real, demonstrated, long-term value and performance that competing start-up companies cannot. Those real-time, in-stream processing tools supported by the machine learning-based behavioral anomaly detection promise to cut through the noise often associated with threat monitoring. Continuous monitoring and reporting, plus GRC dashboards, round out the offering, providing data feedback for operatiors through senior management.

Automation and efficiency—two of Huntsman's technological driving forces—are relevant and necessary for solving current IT security challenges. Huntsman's aim of working across business and technology silos also gets at a systemic issue in most operations environments that attackers can easily take advantage of; complex threats are surprising, and a fragmented business likely cannot defend their systems effectively because none of the groups have sufficient visibility to make the proper identification of the attack. Huntsman collects security information from all available data and acknowledges that external and internal attackers can be equally dangerous. Their goal is delivering a resilient, complete threat detection and action platform, and its task now is to show North American businesses how experience from the Land Down Under combined with cutting-edge technology can produce the best actionable intelligence.