IMPACT REPORT

Seceon offers security for those too busy to sit in front of a pane of glass

SEPTEMBER 15 2016
BY ERIC OGREN (/ANALYST-TEAM/ANALYST/ERIC+OGREN)

Single security information and event management (SIEM) alerts are seldom sufficient to detect or describe threats in the network. A point security product that is smart enough to recognize a threat is smart enough to execute a block/allow decision before generating a log entry. By the same token, log entries typically do not describe a threat if the logging product does not identify it.

Seceon's applied behavior analytics (ABA) product adds a multitude of clarifying data sources to the SIEM log file repository, including network packets, application data, directory logs and threat feeds, to present security operations with a comprehensive view of a threats, along with remediation recommendations.

The 451 Take

We forecast the ABA market will reach $1.3bn by 2021, with Seceon firmly in the hastily emerging user/network behavior analytics segment, which we see growing at a 40% CAGR. This market growth is spurred by the fact that attacks abuse the company's business logic once they have penetrated the network. Attacks can only steal sensitive

data if they have permission to access servers, or are allowed to escalate privileges. Defenses that look to match individual pattern attacks are augmented by ABA with its context of time and analytic models to detect unusual changes in user, device and network behavior. The classic 'vulnerability, exploit, patch' vision no longer holds once an attack is in the network.

Context

Seceon has taken the pragmatic approach of reducing the amount of data a security team has to deal with. It does this by understanding every asset that is on the network, then applying machine learning to detect outlier activity, and finally referencing threat intelligence to prioritize and accelerate IT responses. One enterprise we talked to uses Seceon to reduce the noise from SIEM and next-generation firewall alerts. The company has managed to avoid hiring additional security staff to respond to alerts, and that has a lot of value in a difficult hiring environment for security practitioners.

Three things happen when an attack evades cyber defenses: users eventually call help desks with performance and availability issues, customers trace sensitive data loss back to the company, or security never knows if it's been breached. ABA growth is also due to efficiencies in incident response by reducing a multitude of events, compromise indicators and communications into a single actionable report for security teams. ABA's job is to fill in the gaps between preventive security product silos to detect threats that security teams don't know about, and to give IT a fighting chance to ward off the threat before catastrophic damage occurs.

Seceon is founded with the machine-learning-based Open Threat Management (OTM) platform. The vendor has the only Docker container architecture for ABA that we have encountered with an ability to run ABA as a service within Amazon Web Services. Seceon is still relatively small, at approximately 50 employees, but its focus on producing fewer and more comprehensive alerts for IT should help it execute against larger competitors.

Seceon got its start in 2014, and began generating revenue for OTM in early 2016. The company features high-performance networking experience in its leadership team, with

many members having worked together at Juniper Networks and BTI Systems. Seceon is headquartered in Westford, Massachusetts.

Technology

The OTM platform takes in a wide variety of data. It concurrently processes algorithms to spot unique questionable behavior, and chews on threat, asset and behavior information, before prioritizing the alert for IT. Most ABA vendors in the network process SIEM and directory data for user behavior, network packet information for communications insight, and application logs when they are available.

In our opinion, an ABA vendor cannot open its doors without those capabilities. However, Seceon has other characteristics that we find noteworthy:

- The first week of machine learning is spent identifying and characterizing network assets. Rather than rely on admin consoles of asset management products, Seceon compiles its list from network activity. The network doesn't lie, and this give IT a baseline of what is actually on the network, as opposed to what was thought to be on the network.

- The product accepts streams from the network, directory logs, SIEM and syslog, and raw application logs. The container architecture allows Seceon OTM to run real-time processes in parallel to process data, collect threat intelligence, correlate indicators and policy violations, and drive reporting. We like the Docker approach because it promises flexibility in shifting architectural elements between the cloud and on-premises datacenters.

- Seceon adds threat feed analysis as it prepares its incident response package. By mapping threat intelligence against assets and detected anomalies, OTM further prioritizes alerts, and adds clarity to suggested remediation actions.

- The 'learn it now' feature should be a staple in ABA products. There are many occurrences where a detected anomalous behavior reflects a shift in business

requirements, and is not a threat. Security teams need an easy mechanism to tell machine-learning algorithms that unusual behavior is authorized, and to then push that feedback into machine-learning algorithms to improve the signal-to-noise ratio for security operations.

Competition

The ABA market is evolving. Most proof-of-concept efforts are noncompetitive, and can easily come with an investment of professional services. It is essential that decision-makers narrow down the required use cases and evaluation criteria to keep POCs focused and productive.

Most SIEM vendors either have ABA products and/or partnerships with the leading applied behavior analytic vendors. Splunk UBA is based on acquired Caspida technology, Alert Logic scooped up Click Security, Rapid7 has moved aggressively to integrate Log Entries with high-performance search features, and LogRhythm is finding significant traction with Network Monitor to bring deep network packet inspection into its analytics engines.

Our research with enterprise executives continues to pop up with extreme-scale, corporate-wide ABA initiatives that have performance requirements that traditional database approaches are challenged to meet. We continue to see interest in Splunk and Cloudera, with its Hadoop-based technology to process network, user and application data. Leading ABA vendors such as E8 Security, Niara and Securonix, leverage Cloudera structures to reach beyond security log data to endpoint configurations and performance measurement. However, we feel these vendors aspire more to large, complex threat-detection problems than Seceon might be trending toward.

Elsewhere, vendors are taking slightly different approaches than Seceon. PatternEx applies artificial intelligence to clone an experienced security practitioner. FourV's API approach allows enterprises to shrink security data by up to 20% in managing risk. Meanwhile, Bay Dynamics provides for a high level of risk management customization for large organizations, and Exabeam and Gurucul are effectively working with their installed bases for upcoming launches. Finally, Microsoft ATA leverages interfaces with domain controllers, active directory and Windows to ensure the integrity of Kerberos tickets and user behavior.

SWOT Analysis

Strengths

Seceon's Docker container-based platform gives the company flexibility to add features to the platform and shift ABA workloads to Seceon cloud-based datacenters.

Weaknesses

The company is too new to have strong relationships with the major SIEM vendors. Competitors' push to Hadoop data stores with open source search may pin Seceon into a corner, where strong SIEM vendor relationships would help alleviate some sales hurdles.

Opportunities

Seceon is AWS-friendly, presenting an opportunity to capture new accounts with lower acquisition costs than commonly found in subscription services.

Threats

We have identified roughly 50 vendors competing in the user/network behavior analytics segment of ABA. Seceon will need to carefully differentiate its product to avoid getting lost in the noise.

Eric Ogren (/analyst-team/analyst/Eric+Ogren)

Senior Analyst

M&A ACTIVITY BY SECTOR

Security / Security management / Other (1) (https://makb.the451group.com/results?basic_selected_sectors=757)

Security / Premises network security / Other (6) (https://makb.the451group.com/results?basic_selected_sectors=733)

M&A ACTIVITY BY ACQUIRER

Alert Logic Inc. (3) (https://makb.the451group.com/results?basic_acquirers=Alert+Logic Inc.)

Amazon.com Inc. (46) (https://makb.the451group.com/results?basic_acquirers=Amazon.com+Inc.)

Amazon Web Services Inc. [aka AWS] [Amazon.com Inc.] (4) (https://makb.the451group.com/results?basic_acquirers=Amazon+Web Services Inc. [aka AWS] [Amazon.com Inc.])

Click Security Inc. (1) (https://makb.the451group.com/results?basic_acquirers=Click+Security Inc.)

Cloudera (5) (https://makb.the451group.com/results?basic_acquirers=Cloudera)

Docker Inc. [fka DotCloud] (8) (https://makb.the451group.com/results?basic_acquirers=Docker+Inc. [fka DotCloud])

Juniper Networks Inc. (20) (https://makb.the451group.com/results?basic_acquirers=Juniper+Networks Inc.)

Microsoft Corporation (157) (https://makb.the451group.com/results?basic_acquirers=Microsoft+Corporation)

Rapid7 LLC (3) (https://makb.the451group.com/results?basic_acquirers=Rapid7+LLC)

Figures shown indicate number of transactions

COMPANY MENTIONS (PRIMARY)
Seceon (/search?company=Seceon)

COMPANY MENTIONS (OTHER)
Alert Logic , Amazon , Amazon Web Services , Bay Dynamics , BTI Systems , Caspida , Click Security , Cloudera , Docker , E8 Security , Exabeam , gurucul.com , Juniper , LogRhythm , Microsoft , Niara , PatternEx , Rapid7 , Securonix , Splunk (/search?company=Splunk)

CHANNELS
Information Security , Networking (/dashboard?view=channel&channel=4)

SECTORS
All / Security / Security management / Other (/search?sector=757)
All / Security / Premises network security / Other (/search?sector=733)