Signal Sciences + Cortex XSOAR

Optimize application security with automated incident response and threat intelligence feeds

Benefits

- Robust incident response workflows ensure timely and relevant Layer 7 threat analysis.
- Integrations with threat intelligence providers enrich real time blocking decisions.
- Visualization of application security events enables correlation across other security operations alerts.

Compatibility

- Cortex XSOAR
- Signal Sciences Next-Gen WAF and RASP

Overview

According to the 2019 Verizon Data Breach Incident Response Report, web application attacks are the number one source of data breaches and have doubled since last year. While the volume of Layer 7-based attacks has increased, so has the diversity of attack patterns looking to exploit vulnerabilities in web apps and APIs.

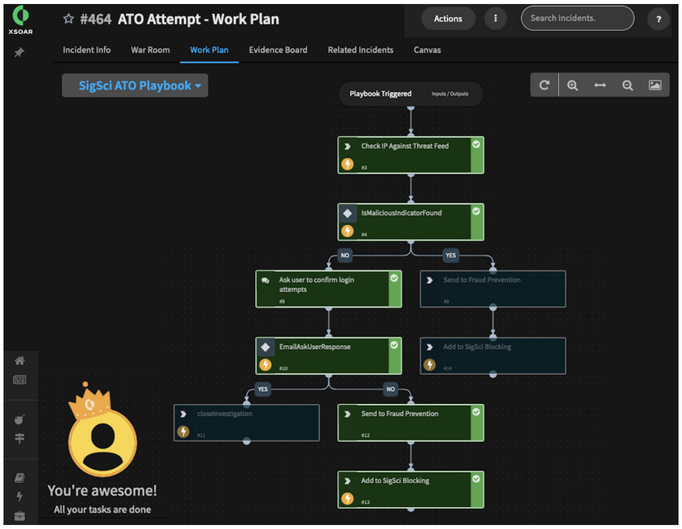
DevOps and application security teams are scrambling to assess the risks associated with these threats and prioritize remediation efforts. Together with Cortex XSOAR, Signal Sciences provides active protection across a wide breadth of web attacks and delivers actionable insights to incident response teams.

Signal Sciences and Cortex XSOAR Integration Features:

- Automate incident response workflow based on granular event classification and context.
- Ingest threat intelligence from other sources to enhance automated detection and blocking decisions.
- Leverage hundreds of Cortex XSOAR third-party product integrations to coordinate response across security functions based on insights from Signal Sciences.

Use Cases

Use Case 1: Putting relevant alerts in the hands of the right teams



Challenge: Given the variety of attack types and anomalies that bad actors execute against web applications, there is no one size fits all approach to implementing an incident response process. Manual triage is resource-intensive and often results in costly delays that exacerbate the damage caused by an attack.

Solution: Cortex XSOAR's event classification framework allows teams to design custom workflows that ensure that security events from Signal Sciences are sent to the right teams in real-time. For example, an event detailing a Layer 7 DDoS attack may be sent to a site reliability team, while a massive account takeover event could be routed to a fraud/loss prevention team. Furthermore, XSOAR playbooks can run a series of automated tasks in response to each event type.

Benefit: By leveraging the Signal Sciences integration with XSOAR, security teams can dramatically improve the effectiveness and timeliness of their response to application security incidents.

Use Case 2: Improve protection efficacy by leveraging external data feeds

Challenge: Cyber security teams in most organizations collect threat intelligence data gathered internally and through third party feeds. While this data is typically used to protect networks and endpoints from malware or other exploits, it's harder for WAFs to utilize this data due to the rigid REGEX-based rule sets that are used for detection.

Solution: Because Signal Sciences does not use static rules for detection, the fact that a request comes from a suspicious IP doesn't alone determine that the request is blocked. Signal Sciences can ingest lists from an IP reputation service that are used to more quickly and accurately determine the risk associated with a web request. Using the integration on Cortex XSOAR, IP lists can be automatically imported from external threat intelligence feeds or other sources to enhance blocking decisions in real time.

Benefit: Companies that have invested in threat intelligence data can now extend those benefits to their application security posture. Providing this additional context to Signal Sciences threat analysis engine will result in more secure applications and faster performance.

About
Signal Sciences

Signal Sciences is the fastest growing web application security company in the world. With its award-winning Next-Gen WAF and RASP solution, Signal Sciences protects more than 40,000 applications and over two trillion production requests per month. Signal Sciences patented architecture provides organizations working in a modern development environment with comprehensive and scalable threat protection and security visibility. The company works with some of the world's most recognizable companies, like Under Armour, Aflac, and Duo Security, across industries, including five of the top ecommerce companies, five of the largest software companies, in addition to many others in the financial services, retail, healthcare, media and entertainment, and government sectors. Signal Sciences is also the recipient of 451 Firestarter award, InfoWorld's Technology of the Year and Computing's DevOps Excellence Award for Best DevOps Security Tool.

About
Cortex XSOAR

Cortex XSOAR, a Palo Alto Networks company, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks, and manage incidents across their security product stack to improve response time and analyst productivity.

For more information, visit https://www.paloaltonetworks.com/cortex/xsoar