SOAR BUYER'S GUIDE

SECURITY ORCHESTRATION AUTOMATION AND RESPONSE

DOMAINTOOLS®

SOAR:
A BUYER'S GUIDE

TABLE OF CONTENTS

INTRODUCTION

Research conducted by ESG found that 58% of organizations have a threat intelligence program, however with a reliance on manual processes and incompatible tools, organizations struggle to realize the value of threat intelligence. To meet these challenges, some security teams are aiming to effectively operationalize threat intelligence through the fundamentals of people, processes, and technology. When aligning people, process, and technology, you get the ideal cross section for SOAR (Security Orchestration, Automation, and Response) platforms.

WHAT IS SOAR (SECURITY ORCHESTRATION AUTOMATION AND RESPONSE)

Before diving into SOAR, it is important to understand the precursor to implementing a SOAR solution, and that is proper logging. SIEM solutions combine SIM (Security Information Management) and SEM (Security Event Management) functions into one security management system. SIEM solutions collect and aggregate log data that is generated within a technology infrastructure, including applications, network traffic, endpoint events, etc. From the aggregated data, SOCs (Security Operations Centers) and CSIRTs (Cyber Security Incident Response Teams) can then detect events and incidents for further analysis.

ORCHESTRATION

Refers to the machine-based coordination of distinct yet interdependent security solutions. Through the collection and centralization of event data, all the information necessary to assess and respond to incidents is available and easily accessible in one location. Furthermore, in the case of a security incident, information is presented in context, and actions can be invoked even in third-party systems.

AUTOMATION

Is the machine-based execution of security processes with minimal human interaction. Monitoring the entire attack surface can often require having a large IT security function – a commodity that not many organizations can afford.

RESPONSE

Is the combination of human and machine security processes, procedures, and actions that need to be performed when a security event occurs.

SOAR AND SIEM
are complementary platforms that when leveraged properly, enable SOCs and CSIRTs in detecting and responding to events which can lead to being able to measure and reduce MTTD (Mean Time To Detect) and MTTR (Mean Time To Respond).

IS SOAR THE RIGHT SOLUTION FOR YOU?

Not all security solutions are created equal and it is important that all the enterprise-specific, internal factors are taken into consideration when opting for one over another.

THE THREE FACTORS THAT SHOULD INFLUENCE YOUR CHOICE ARE:

1

PLATFORM'S CORE CAPABILITIES

These should broadly cover:

- Orchestration
- Automation Engine
- Alert Management
- Case Management
- Playbook/Workflow Management
- Incident Management
- Automation Editor
- App Framework
- Metrics and Reporting

2

PLATFORM'S ATTRIBUTES

COLLABORATIVE platforms benefit from feature completeness, app integration coverage, and the capability to address a wider and evolving range of scenarios. If collaboration happens across the community, users can benefit from a range of playbooks/workflows and app integrations, but also of non-technical resources such as tech notes, blogs, and other documentation.

COGNITIVE SOAR platforms should be able to leverage the knowledge from humans, codify it and learn from previous decisions to inform playbooks/workflows.

3

BUSINESS CONSIDERATIONS

Aside from the obvious product specifications, a SOAR vendor's reputation and overall professionalism and support should also be considered in the decision process.

WHAT CAN SOAR HELP YOU ACHIEVE?

BETTER QUALITY INTELLIGENCE

With a deep knowledge of the threat's TTPs (Tactics, Techniques, and Procedures), SOAR can consolidate all the data from different sources such as firewalls, IDS (Intrusion Detection System), SIEM, UEBA (User Entity Behavior Analysis), TIP (Threat Intelligence Platform), etc. SOAR solutions provide analysis and context, and can automatically take actions based on a customer's, and sometimes vendor's, set of rules. This can result in faster MTTD and MTTR.

IMPROVED OPERATIONAL EFFICIENCY

SOAR automates daily mundane tasks conducted by security personnel. Using artificial intelligence and machine learning, SOAR minimizes the need for "context switching." In turn, this efficiency increases productivity without needing additional personnel - and it typically results in freeing up some tier 1 security analysts to do higher value tier 2 analytical work.

FASTER INCIDENT RESPONSE

SOAR allows organizations to reduce MTTD and MTTR. This can be done by remediating quality alerts in a fraction of the time compared to traditional means where it can take days or months. It also helps automate playbooks, workflows, and incident response procedures, which can include blocking IP addresses, suspending user accounts, and quarantining infected endpoints.

CHOOSING THE RIGHT SOLUTION FOR YOU

splunk> phantom

IBM Security

With DomainTools Iris Investigate API, the powerful Iris dataset is available not only for ad-hoc research on specific incidents in SOAR platforms, but also for automated actions in playbooks/workflows. Organizations will be able to easily fetch a complete Iris profile for a domain including:

- IP address and hostname details for the name servers, mail servers, and web server powering the domain
- SSL certificate details and tracking codes for the website hosted on the domain
- Email addresses extracted from DNS SOA record
- DomainTools Risk Score, with components (malware, phishing, spam, and proximity to known badness) and evidence

AN EVALUATION CHECKLIST

ONE COMPREHENSIVE PLATFORM

An effective SOAR solution needs to provide a broad set of functionalities, integrated in a single platform. These include the automation of responses based on a set of rules, with minimal reliance on human intervention (e.g. gathering some additional information, opening tickets, sending out automated status alerts and updates). It should be able to invoke tasks across other, independent, security systems (e.g. SIEM), and it should manage each case in a centralized fashion, providing analysts with a single interface to execute incident response arrays. It should also have a built-in or integrated third-party reporting and analytics tool.

DOES THE SOAR SOLUTION:

□ Enable technologies to work together

□ Insert humans into the decision process

□ Give access to the playbooks/workflows code

□ Feature built-in testing and debugging tools, and runtime logging

□ Have a good model for organizing playbooks/workflows

□ Allow for bulk editing of playbooks/workflows

□ Support the ability to gather contextual data from trusted third party sources

SCALABILITY

The automation engine of a SOAR solution should scale both vertically and horizontally. As users automate more use cases over time, the automation should, for instance, increase RAM resources to increase performance, and increase server instances to improve performance. Furthermore, as the threat landscape evolves, the system should support new functions without the need for major re-engineering.

□ Is the platform scalable, open, and extensible

□ What are the interface restrictions

□ Does it feature an open integration framework

EFFICIENT ALERT AND CASE MANAGEMENT

Having the right information at the right time is key to efficient threat management. A SOAR solution should queue inbound requests according to their priority level, thus simplifying the triage process.

Cases, being fewer in number, should be driven through a lifecycle that accommodates the greater complexity of the event, and should be aggregated for easy access. The case management interface should contain all the technical relevant data, such as the alerts source data, and also allow for non-technical comments, memos, and emails.

CAN THE SOAR PLATFORM:

□ Aggregate alerts and cases

□ Provide alert details, action results and activity logs

□ Organize alerts based on status, severity and sensitivity

□ Manage privacy, compliance and fraud cases

□ Provide case data organization

□ Provide activity auditing

□ Provide mapping to existing processes

□ Link cases to alerts

□ Allow for adding data, memos and notes to a case

A PLATFORM FOR THE USER

One of the purposes of a SOAR solution is to ease the pressure on IT security teams. To do so, its interface should be customizable and flexible, allowing each user to create tasks and reporting that suit their needs. Whether an analyst needs to automate mundane tasks and reduce the time spent on false positives, or a CISO needs accurate metrics to compare and report on the performance of the cybersecurity function, a SOAR solution should accommodate their needs and allow them to direct their attention to those they consider to be higher value tasks.

DOES THE SOAR PLATFORM:

□ Feature RBAC (Role Based Access Controls) and tailored dashboards

□ Record and report security performance metrics

□ Allow for IR (Incident Response) processing and SOC metrics to be generated

□ Come with pre-set playbooks/workflows or can you create your own

□ Give you access to expert advice

CONFIGURATION AND ONBOARDING

An onboarding period can be useful to allow for the appropriate configuration of system settings, connect all the data sources, and test playbooks/workflows. To accelerate the automation process, SOAR platforms can enable users to access a portfolio of automated playbooks.

□ Is there a set of pre-set playbooks/workflows

□ Does it offer an onboarding/testing period

HOW DOMAINTOOLS CAN HELP

DomainTools enables organizations to take indicators from their network, including domains and IPs, and connect them with active domains on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure.

PHISHEYE

Discovers newly-registered domain names with the ability to identify existing and new domains that spoof legitimate brand, product, organization, or other terms, for defensive or investigative actions.

IRIS

Combines enterprise-grade domain intelligence and proactive risk scoring with industry-leading passive DNS data to guide threat investigations and uncover connected infrastructure.

SC MEDIA ★★★★★

DOMAIN RISK SCORE

DomainTools Risk Score predicts how likely a domain is to be malicious, often before it is weaponized. This can close the window of vulnerability between the time a malicious domain is registered, and when it is observed and reported causing harm. The Domain Risk Score algorithms analyze a domain's association to knownbad infrastructure, as well as intrinsic properties of the domain that closely resemble those of known phishing, malware, and spam domains.

APIs

The DomainTools APIs bring a critical subset of capabilities to third-party products and custom integrations, enabling rapid in-context profiling of domain-based threats and effective pivots that help build comprehensive lists of malicious infrastructure.

DOMAINTOOLS®

To test the power of DomainTools or get pricing information:

WWW.DOMAINTOOLS.COM • SALES@DOMAINTOOLS.COM • 206.838.9020