opentext™ | Cybersecurity

White Paper

Security Orchestration Automation and Response

ArcSight SOAR is a leading Security Orchestration, Automation and Response tool to empower security operations. ArcSight SOAR can do automation, orchestration of both technology and people, providing a comprehensive incident case management platform bundled with dashboards and reports.

Table of Contents

Introduction

ArcSight SOAR Is Built for the Masses

Most of the top SOAR tools are geared towards the most experienced SOC analysts or CSIRT members of the world. Unfortunately, such top talent is heading to extreme levels of scarcity. So, instead of building tools for top experts, we wish to build tools for masses; for both skilled and less skilled analysts. This change in target audience brings new challenges: making sure the system is safe (i.e., protects the infrastructure against analyst errors), allows operators decide what to do manually for just clicking a button, user-friendly, easy to learn, easy to operate and secure (i.e., can have very granular control over solutions).

ArcSight SOAR Is Flexible

Two organizations are never the same when it comes to SOAR expectations. This is why we do not only wish for features that we are currently adding in, but we also project the design of a platform where customers are free to innovate and literally build their own features. Super-powered automation engine, custom severity scales, custom SLAs and pre-processor pipelines are all facilities meant to take us towards that goal. Numerous times, prospective customers comment on ArcSight SOAR by OpenText as the most flexible among the platforms they review.

Arcsight SOAR Can Involve Everyone in Your Organization

Keeping the security running is too important. Security teams are spending enormous efforts on it. In many cases, investigating and responding to an incident involves communication and exchanging information with others. This is why from scratch, ArcSight SOAR is designed to involve potentially everyone into the plays. ArcSight SOAR can interact with other teams or members in the company through emails and 3rd party service desk tickets. All hands-on deck—if ever needed—will be a critical success factor for ArcSight SOAR.

ArcSight SOAR has many cleverly thought out features to back those drivers above. In this white paper, we will briefly focus on the key distinguishing aspects of ArcSight SOAR.

ArcSight SOAR has many cleverly thought out features to back those drivers above. In this white paper, we will briefly focus on the key distinguishing aspects of ArcSight SOAR.

Super-Powered Automation

Automation is an important ingredient of SOAR platforms and each platform claims to do automation; some are far more featureful than others. This section is dedicated to summarizing ArcSight SOAR's automation abilities. Please note that ArcSight SOAR secflow steps (called as playbooks) can be fully automated, fully manual or somewhere in between.

Automation Triggers
ArcSight SOAR can start a playbook upon triggered from a 3rd party product; like a SIEM alert, a REST API call from a custom application or receipt of a particular type of threat intelligence. It can also monitor an email address or a web page and trigger a play upon receiving an email or observing change in the page contents. ArcSight SOAR can also be integrated with a Service Desk application so whenever certain types of tickets are opened, ArcSight SOAR can take over and start a pre-configured play. Alternatively, a SOC analyst can manually create an incident record, triggering another play.

Maintenance jobs (e.g., restarting a service periodically, cleaning up disk space, etc.) or to fill / update lookup tables meant to be used in plays.

Notification Templates
At certain points in play, it might be needed to send out notifications: emails, SMS messages, Windows Popup notifications, etc. ArcSight SOAR allows you to store those notification templates separately, so you don't have to embed them into your plays and add more complication. This becomes particularly important if you like to use different templates based on one's language, geography or role. An ArcSight SOAR play can choose the right template and mail—merge them and send out like a breeze.

Multi-Match Plays
There can be plays defined for some specific conditions. When a new incident is created, it is matched with one or more plays which are globally defined in the platform. Unlike a typical firewall rule, which works with first-match, ArcSight SOAR purposefully uses the multi-match model. A new incident can be subject to multiple plays, doing different things on the same topic.

Our customers are coming up with new and interesting ideas regarding the usage of this facility constantly. For example, a banking customer uses this feature to evaluate the severity of new incidents. The first play in the list checks if the subject user of the new incident has any open incidents already. If (s)he has more than three incident cases opened in the last hour, the severity is escalated to critical.

Incident Triggers and Event Handlers
ArcSight SOAR provides a group of incident triggers and allows certain event handlers to be defined against them. Certain playbooks can be triggered upon incident creation—investigation scope change (e.g., observing a new IP, user, URL or domain name), SLA miss and incident closure.

Unlike a typical firewall rule, which works with first-match, ArcSight SOAR purposefully uses the multi-match model. A new incident can be subject to multiple plays, doing different things on the same topic.

Such triggers open up possibilities for a lot of different cases of usage and our customers are coming up with new ones all the time. A sample usage for this might be incident creating and closing triggers to run automations to open and close tickets on a 3rd party service desk, because there might be a case for entire IT organization wanting to get SLA adherence reports from a 3rd party service desk. It can also be used investigation scope changes to trigger automated investigations; so, as soon as an analyst encounters a new IP, ArcSight SOAR triggers an automation to lookup that IP or whenever an analyst hits a new username, info on that user is retrieved from multiple internal data sources. As such, triggers provide a different way to automate repetitive mechanical activities.

ArcSight SOAR supports role-based access control, a bulletproof auditing subsystem and integrates with a credential vaulting (e.g., certified CyberArk integration), same as others, but it has far more to address to the mission-critical security needs.

Iron-Clad Security

SOAR platforms are used to command & control a multitude of different cyber security and infrastructure systems and which require privileged access to these systems. Many see this as putting all your eggs in one basket, as all credentials are handed over to a single tool.

This is exactly why ArcSight SOAR takes security very seriously and has a superior security model compared to the rest of the industry. ArcSight SOAR supports role-based access control, a bulletproof auditing subsystem and integrates with a credential vaulting (e.g., certified CyberArk integration), same as others, but it has far more to address to the mission-critical security needs.

Capability-Based Access Control

ArcSight SOAR talks to 3rd party software and devices through plugins. Plugins allow ArcSight SOAR to either be able to retrieve data, take actions or both on a particular target. Whereas most of the industry focuses on device type-based access control (e.g., analyst A can invoke Active Directory functions and analyst B cannot), ArcSight SOAR provides more granular access control through what is called ‘capabilities’. Capabilities are all the different functions a particular plugin exposes; for example, Active Directory plugin exposes some 15 different functions like user details, members of a named AD group, lock a user, etc. So, the ArcSight SOAR platform administrator cannot only allow analyst A to access Active Directory functionality but can also be very specific that he can only invoke ‘user details’ function, but not others. Where the device-based access control model is no different than giving analysts the admin passwords to the systems, the capability-based access control model allows ArcSight SOAR to act as an access control gateway, significantly limiting risks and increasing security.

Investigation Scope

When an incident case is created, ArcSight SOAR starts to store both the history of activities and all the relevant IPs, users, URLs, domains, e-mail addresses, program names, hashes, etc., as artifacts. Those artifacts are stored in a structured manner in what is called an investigation scope. By definition, the investigation scope is the sum of all relevant cthat might require further review.

The scope is not just a guidance tool for analysts but more importantly, a security feature. In the subsection above, we explained capability-based access control; a way to control what functions of a particular software or device an analyst can invoke. Capability-based access control, for example, allows a particular analyst to retrieve files agentless from a PC.

Most probably, you wouldn't want your analysts to be retrieving files from an arbitrary PC, out of the blue. This is why ArcSight SOAR, by default, restricts analysts from exercising their privileges outside the incident scoped items. Which, in practice, means unless there is an incident that involves a particular computer, no analyst will be allowed to retrieve files from that computer even if he has the privilege of retrieving files from PCs. Same goes for blocking: one cannot block a particular IP, unless that IP is in the investigation scope.

Unless ArcSight SOAR administrator chooses to override it, investigation scope adds another level of security. Capability based access control defines what analysts can do, investigation scope defines on which artifacts they can exercise their power.

Unless ArcSight SOAR administrator chooses to override it, investigation scope adds another level of security. Capability based access control defines what analysts can do, investigation scope defines on which artifacts they can exercise their power.

Restrict Non-SOC Access

Many of the SOAR platforms allow getting IT and user feedback, by sending links via email and asking the users to click, join the platform and then provide feedback on the browser interface. We believe that this is a very dangerous approach. Take a moment and reflect on the significance of the data stored in the SOAR platform and imagine whether anyone would appreciate such exposure. More people touching the SOAR interfaces increase the attack surface significantly and potential data loss.

Instead of such browser-based feedbacks, ArcSight SOAR chooses to interact with users through messaging applications. The current version supports emails, as ArcSight SOAR can send out messages asking for written feedback. This is not only simpler when someone is out of the office (which would probably require a VPN connection first), but also more secure as they don't have direct access to the platform anymore. Moreover, such user feedback can not only contain a response (e.g., YES or NO) but can also include comments or further explanation that improves the case history.

Exclusion Lists

Many organizations want to provide exclusions around what SOC people can do. Exclusion of a particular extremely sensitive network seems to be a solution, so that under no circumstances SOC team is able to reach out to them and collect data or maybe take actions, because that network's availability is mission critical at all times.

For all the different types of investigation scope items discussed above (IPs, usernames, emails, URLs, domains, etc.), it is possible to define exclusion lists. Neither ArcSight SOAR automation, nor analyst activities through the browser interface can disregard such exclusions. So, whatever the containing of exclusion list is, it is always ensured untouchable on the ArcSight SOAR platform.

Super Flexible

Every single organization is different and so are their SOAR needs. ArcSight SOAR is super flexible in many different aspects to accommodate such differences.

Severity Levels and SLAs
Some SOCs work with a 4-level severity scheme, some with a 5-level one; ArcSight SOAR provides completely configurable severity levels and the ArcSight SOAR administrator can define whatever will be used. Accordingly, for every different severity level response and resolution SLAs can be defined.

ArcSight SOAR is super flexible in many different aspects to accommodate such differences.

Classifications
ArcSight SOAR comes equipped with a group of incident classifications; malware, phishing, lost laptop, among others. ArcSight SOAR administrator chooses to either use these classifiers or define their own and run the platform with their own choice of classifications.

Incident Dispatch and Staff Shifts
ArcSight SOAR's incident dispatch algorithm can be completely re-written from scratch; in fact, it is yet another play defining what shall happen when a new incident is created. ArcSight SOAR administrator can define a completely custom incident dispatch algorithm based on incident fields and parameters. With the help of scheduled plays, it is possible to define how handovers and shifts are to be operated. There are no limits in defining dispatch and shifts.

Triggers and Event Handlers
Triggers are discussed in the Automation section of this document. The trigger facility provides great flexibility in defining what shall happen in ArcSight SOAR when a specific scenario happens. There are a million different potential use cases to use triggers and associated event handlers in ArcSight SOAR and the automation section already discussed a few practical ones.

Alert Preprocessing and Incident Consolidation
Every single alert received by ArcSight SOAR goes through the alert pre-processing pipeline. ArcSight SOAR administrator can define a lot of different actions and changes to an incoming signal while being processed on this pipeline—changing severities, filtering out unwanted alerts, classifying the incoming alert and even consolidate multiple alerts into one incident.

ArcSight SOAR supports rule-based incident consolidation that works with time windows; arbitrary and multiple consolidation rules can be deployed and run by the ArcSight SOAR platform administrator, significantly reducing the number of incident cases presented to the analysts.

Involve IT End Users

Most SOAR platforms are built exclusively for SOC teams; rarely some allow reaching out to others in the organization to take their feedback. Unfortunately this doesn't reflect the real world.

In the real world, SOC teams reach out to employees of the organization to ask or confirm about particular activities that are deemed suspicious and sometimes even reach out to someone's manager to ask if (s)he's aware of the subordinate's activities.

ArcSight SOAR allows such interactions between the SOC team and the rest of the IT users through electronic communications. At any point during an investigation, ArcSight SOAR can reach out to people with emails and ask an arbitrary question. Based on the email response, ArcSight SOAR can alter the course of action in the play and carry on accordingly.

Reaching out to non-SOC people through ArcSight SOAR has also added the benefit of recording such feedback into the incident timeline and preserving such emails. So that it provides non-repudiation into whatever feedback these people are providing.

Another interaction between ArcSight SOAR and other members of the organization happens when a particular action is to be taken on security or infrastructure technologies. ArcSight SOAR allows defining device owners and marking any particular device as requiring approvals. Whenever ArcSight SOAR engine is to reach out to a particular device for further action, if the device is marked for approval requirements, ArcSight SOAR sends an email to the respective device owner and asks for device owner's consent.

ArcSight SOAR allows defining device owners and marking any particular device as requiring approvals. Whenever ArcSight SOAR engine is to reach out to a particular device for further action, if the device is marked for approval requirements, ArcSight SOAR sends an email to the respective device owner and asks for device owner's consent.

Conclusion

In the Introduction section, we tried to describe the fundamental and unique design goals behind ArcSight SOAR:

- Be a platform for all types of SOC Teams / CSIRTs despite their maturity level
- Be flexible to accommodate expectations of different organizations
- Engage the entire organization, not just the SOC team in enhancing security

Most organizations appreciate those three goals mentioned above, as they formulate the needs of the larger portion of the cyber security industry.

In sections, B thru F, we tried to describe what and how is different in ArcSight SOAR, in order to address the above:

- Discussed how automation is superior in Section B,
- Why and how iron-clad security model is designed as it is in Section C,
- The flexibility brought to the table and how the sky is the limit in Section E,
- And how to involve people beyond your SOC team in Section F.

To learn more and see these features and functions in action, please visit: **www.microfocus.com/en-us/cyberres/secops/arcsight-defend**

To learn more and see these features and functions in action, please visit: **www.microfocus.com/en-us/products/arcsight-soar/overview**

Connect with Us

www.CyberRes.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.