CyberRes

White Paper

A Business Case for ArcSight SOAR

Cybersecurity is a complex problem. We need automation and all sorts of automated assistance to scale our limited expertise and connect the dots among our independently operating security tools.

ArcSight SOAR is a security operations platform that combines every security tool under one unified umbrella, helps them work in tandem and assists your people achieve far more to defend your organization better.

Cyber Security Today

Cyber attacks are increasingly #1 source of risk for all enterprises; every organization tries to ensure all attacks are defeated and the crown jewels are protected. Insider and external attackers are successfully stealing data, tampering with databases, forcing and stopping the execution of critical services. These attackers might be individual, organized crime syndicates, competing corporations and even nation states.

Enterprises in all sectors are spending a lot to secure their data, computing environment and services from such attacks. However this is a increasingly becoming a super tough challenge for several reasons:

- **Attacks are super fast now.** Attackers use malicious software to attack which explains why we see attacks getting in, doing some harm and getting out in 15-20 minutes today.
- **Organizations are getting hundreds of cyber alerts a day.** Several hundreds of attack alerts a day are typical, if not more, and investigating and responding to all of this high is impossible.
- **Existing security tools are not working together.** This lack of cooperation results in poor overall protection
- **There are never enough cyber experts in the team.** In order to operate regardless of the security technologies we have, we always need more people

Due to this reasons, cyber security is increasingly being observed as an *unconquerable* problem. Attackers are having the upper hand and the situation is only getting worse. ArcSight SOAR is here to change that.

Cyber security is increasingly being observed as an *unconquerable* problem. Attackers are having the upper hand and the situation is only getting worse. ArcSight SOAR is here to change that.

What Is ArcSight Soar?

ArcSight SOAR is a Security Orchestration, Automation and Response (SOAR) platform. It allows anything repetitive in the day to day security operations to be automated and provides a single unified pane of glass for all security team members to work on cyber security incidents.

By providing a unified operations environment ArcSight SOAR allows security teams to be more agile, be more tim efficient and defend their organizations far better than before. Because of the way ArcSight SOAR is architected, it will keep working even if you start changing existing security tools or adding new ones.

What ArcSight Soar Brings to the Table

ArcSight SOAR brings a lot of value to security teams. Below you will find some of the most important four ones.

Automating Alert Triage and Consolidation
ArcSight SOAR can automatically prioritize which alerts are more important than others; sorting all alerts in priority order. This helps organizations to always start with the most important alert and carry on over to less important ones.

ArcSight SOAR can also analyze the alerts based on the organization's rules, consolidate multiple independent alerts into a smaller number of consolidated cyber incidents to investigate. This decreases the total volume of work for the security operators significantly.

"Our manual alert triage is now mostly automated, requiring 90% less human resources, we'll be reaching 95% soon. Also, in a typical day, ArcSight SOAR consolidates 1.000 alerts into 250 cyber incidents; a 95% reduction on cyber incident cases to investigate decreases our efforts dramatically."

Telco CISO

Eliminating False Alerts
Security tools are not foolproof; we often receive false alerts. ArcSight SOAR can automatically eliminate such false alerts by automatically collecting additional data from systems and/or reaching out to employees and asking questions. By collecting more data, consolidation and understanding the root cause, ArcSight SOAR can reveal whether the alert is genuine or false.

"Since we started ArcSight SOAR, we put a special emphasis to eliminating false alerts. Today, in a typical month, ArcSight SOAR eliminates some 60-70% of all false positives. In this way ArcSight SOAR is saves us 1.6 full time employee effort per month."

Bank CISO

By collecting more data, consolidation and understanding the root cause, ArcSight SOAR can reveal whether an alert is genuine or false.

Automating Alert Investigation and Response

If the investigation and response to a particular type of attack alert can be presented as instructions to a newly joining security staff member, it is possible to automate most (if not all) of those steps in ArcSight SOAR. ArcSight SOAR automation can help security teams offload whatever is repetitive, allowing them to focus on things that require the human intellect.

ArcSight SOAR can automatically collect all data and evidence an operator needs, even before the operator starts working on the case.

"We automated the investigation and response processes of most of the monthly top-10 frequent alerts. Most are fully automated where some are still involving a security operator to confirm sensitive actions like taking a computer off the network. During the course of a full year, ArcSight SOAR automation saved us 9.5 full-time employee effort."

CIO of Government Agency

Increasing Productivity

During an investigation, the security operator uses multiple different tools. ArcSight SOAR unifies all these different tools by providing a unified command & control interface.

This interface allows operators to do far more in less time. This greatly increases the productivity of the security operator.

ArcSight SOAR can automatically collect all data and evidence an operator needs, even before the operator starts working on the case, saving a lot of precious time and focuses the operator on resolution but not gathering data.

"We have very few security operators. ArcSight SOAR's unified command and control interface allows them to investigate more cases per day. We ramped up from 8–10 investigation cases a day to 100-120 a day; a 12x increase in operator productivity."

Bank CISO

Summary

Cybersecurity is a complex problem and attackers are far ahead of us. We need automation and all sorts of automated assistance to scale our limited expertise and connect the dots among our independently operating security tools.

ArcSight SOAR is a security operations platform that combines every security tool under one unified umbrella, helps them work in tandem and assists your people achieve far more to defend your organization better.

ArcSight SOAR provides a lot of additional benefits, such as driving down training costs for security operators, decreasing the ramp-up time to enable a new hire in sensitive day to day security operations and reduce the risk of security operator mistakes and misbehavior.

The platform has successful references in banks, telcos and government agencies in several different countries.

ArcSight SOAR is a security operations platform that combines every security tool under one unified umbrella, helps them work in tandem and assists your people achieve far more to defend your organization better.

Contact us at **CyberRes.com**

Like what you read? Share it.

CyberRes

A Micro Focus Line of Business