More than a SOC tool, a SOC security portfolio

charles.clawson

06-19-2018 05:00 AM

One of the common first steps when selecting a particular software solution, whether in the security space or otherwise, is to do a “bake-off.” The goal of such an exercise is to bring together all the major competitors to attempt to detect feature parity and differentiators. In the crowded red ocean that is the SIEM space, this can be a difficult task. And with tools that are critical to Security Operations Centers (SOCs), it’s important that such a bake-off is done right.

When it comes to Micro Focus ArcSight, one of the biggest misconceptions I commonly see is that people think ArcSight is a single class tool with a singular purpose. While that may have been true back when it first entered the market and helped define SIEM, it’s evolved far beyond the limits of point solutions. One of the reasons Micro Focus was anxious to add ArcSight into its large software family was because of the potential it brought to its #StrongerTogether vision. As the name ADP (ArcSight Data Platform) suggests, ArcSight is truly emerging as a platform. Starting at the earliest stage machine data generation all the way to having an alert reach an analyst’s triage queue, all the different complimentary components of the ArcSight family play an important role. For those who may not be familiar with all of the ArcSight pieces, the following provides a brief introduction to the important roles the different components play.

ADP: SmartConnectors, Event Broker and ArcMC

Talking about “plumbing” is rarely an exciting topic. However, just as plumbing is a very important function of the homes and buildings that we often take for granted, the plumbing of event data collection and distribution within an organization has never been more important. If done incorrectly, security teams can spend the majority of their time onboarding and configuring data feeds, connectors and storage, while neglecting the very reason for collecting such data in the first place. Every hour spent dedicated to managing and monitoring the health of data feeds, is an hour that could be spent further maturing the security use cases that data is intended to solve.

By many accounts, ArcSight has leapfrogged the traditional SIEM competitors by including in its platform an open message bus technology to address this challenge. Pulling from leading open technologies such as Apache Kafka, Docker and Kubernetes, our research and development team was able to create a soup to nuts event collection system that not only ties in all the other ArcSight components, but also allows for

the enriched ArcSight data to be shared with other third-party data and analytic solutions. This is all easily managed using a modern interface within the ArcSight Management Center (ArcMC). ArcMC gives you a centralized view into all your deployed connectors, showing you graphically where data is being sent. Plus, it gives you a single location to apply data routing rules. Because of its inherent open and interoperable nature, our customers can take advantage of tight ADP integration with tools like ArcSight Investigate, Elastic, Hadoop, and Splunk.

ArcSight ESM

Leveraging ADP's powerful foundation of normalized, parsed and enriched data, ArcSight ESM is able to deliver industry leading real time correlation. This correlation takes advantage of the categorization and schema work done at the time of event collection. This empowers analysts to write and share content across vendor products without getting bogged down in the minutia of log event formats. Now with the advent of distributed correlation, ESM can handle more events than ever before, closing the visibility gap customers had to deal with in the past. Hand in hand, ESM and Event Broker give you massive scalability with their leading edge cluster and distributed technologies.

ArcSight Marketplace

Saving you and all of our customers hundreds of man-hours from having to build your own custom rules and alerts, Micro Focus provides no charge access to the ArcSight Activate threat framework and ArcSight Marketplace content for the most current security correlation rules, dashboards, reports, and use cases. Activate and ArcSight Content Brain combine to provide a one-stop library for hundreds of easy-to-install packaged use-cases, built to solve real business security challenges. As additional custom content (i.e., rules, trends, dashboards, and reports) is created to address different security use cases, this content can be easily packaged and deployed on other systems, shared with other business units, or contributed back to the ArcSight community.

SOC Workflows and Metrics

As the icing on the cake, ArcSight ESM natively includes a complete incident and case management workflow. This allows analysts to identify events of interest, create cases, track them through the stages of investigation, and escalate when needed. For those organizations that have an existing ticketing system like Service Now, ESM integrates easily with it and similar solutions.

In the end, the ArcSight portfolio gives SecOps organizations a scalable and centralized view into their multiple environments, while enabling them to create workflow efficiency for streamlined processes. Through improved detection, real-time correlation, and workflow automation, SOC teams can resolve incidents quickly and accurately. The technology advances offered by the ArcSight portfolio enable you to do more with less. Better security workflow powered by ArcSight enables your SOC to be more efficient with less staff, reducing your MTD (mean time to detection) and MTR (mean time to remediation).

Tags: ADP ArcSight SecOps siem SOC

Filter by Labels: Big Data Security Analytics | Threat Intelligence

0 KUDOS

ABOUT THE AUTHOR

charles.clawson

Key Links

- Security News and Events
- Other News and Events
- TAP Program
- Support
- Education
- Documentation