opentext™ | Cybersecurity

Flyer

ArcSight SODP and Splunk

Successful SecOps implements integrated security architectures that share data across solutions. ArcSight SODP offers scalable and interoperable solutions that can increase the ROI of existing tools.

Benefits

Enhancing Splunk with ArcSight SODP enables you to:

- Cut license utilization costs by up to 90 percent
- Parse data into a common standard schema instead of 20+ proprietary schemas
- Normalize and categorize events to simplify queries and reporting regardless of data source
- Reduce hardware storage costs
- Gain an immediate SODP return on investment

Optimize Your Splunk Investment with ArcSight SODP

ArcSight Secure Open Data Platform (SODP) by OpenText vs Splunk seems to be a common debate in security circles. Vocal proponents in both camps often take a hard stance on why their favorite is best in class. The approach of each solution is very different, but both have compelling merits that are impossible to ignore. ArcSight SODP offers an open architecture approach that easily scales, normalizes, and aggregates data from multiple sources in real time, and then delivers that enriched data to multiple destinations for easy analysis. Splunk gives you quick deployment and onboarding of new data sources, combined with powerful search capabilities and advanced built-in analytics. When stacked up against each other, both offer many similar capabilities and benefits, but depending on who you talk to, one solution will inevitably outshine the other in multiple categories. So, how do you choose?

The best answer is you may not have to choose in order to benefit from the best of what each has to offer. ArcSight SODP and Splunk can play nicely together in a way that lets you combine what you love most about each solution, while enhancing your analysis capabilities and significantly reducing your overall licensing costs.

Understanding Differences in Approach

To understand how ArcSight SODP and Splunk work together, you first have to understand the differences in their approach. The first difference is in what they do at the time of data ingestion. Splunk simply collects event data in its raw form, indexes it, but does not parse or normalize the data until search time or when the data is rendered. This is referred to as “schema on read.” The benefit of this approach is that it makes it very easy to add new data sources and start collecting machine data of all types. It simply accepts what you give it, no questions asked. It does have some downsides. Without parsing, aggregating, and filtering the data at the time of ingest, it can significantly increase your Splunk license utilization, as well as escalate data processing overhead in your downstream workflows.

ArcSight SODP on the other hand, uses SmartConnectors to normalize, categorize, enrich, and aggregate data at ingestion. Since this “schema on write” approach enriches data in a structured format that is consistent across all data sources, it enables the data to be easily shared with any big data or analytics tool. Additionally, proper aggregation of events—grouping common events while preserving common fields with minimal data loss—can result in huge data store reductions. The end result is that downstream applications no longer have the burden of collecting and parsing the data. And analytic tools—including Splunk—can quickly make use of the data, while reducing the amount of data that needs to be consumed, indexed, and processed.

Additionally, ArcSight SODP uses the industry standard Common Event Format (CEF) to normalize all machine data into a common schema. With more than 480 SmartConnectors, as well as the Flex Connector framework

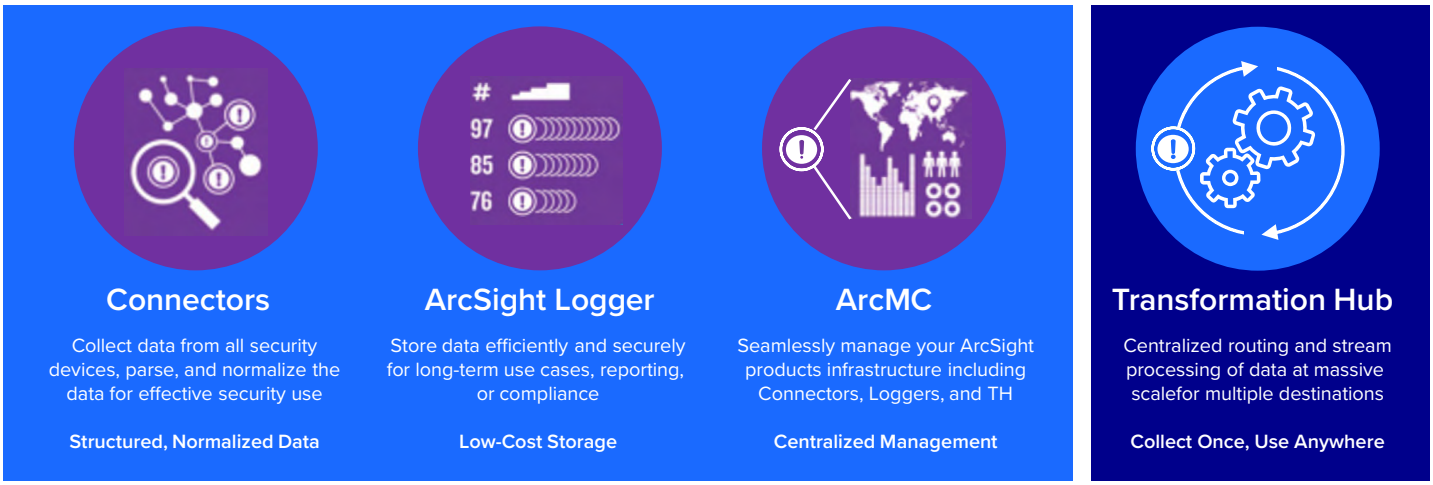

Figure 1. ArcSight Security Open Data Platform Portfolio

for custom data feeds, virtually any type of data can be collected and distributed in CEF. Normalizing data in a common schema speeds up correlation, enables easy consumption by any target destination, and gives analysts a common taxonomy that makes event messages vendor-agnostic. This greatly simplifies and enhances the way analysts work since they only need to learn a single schema and can use nearly identical search queries across diverse platforms.

Splunk uses a normalization methodology called the Common Information Model (CIM) as its search-time schema or schema-on-the-fly. Keep in mind that it is not actually a single schema. Splunk employs 23 different schemas that you choose from depending on what the data source is. This pseudo normalization complicates the use of the data, making it difficult to effectively correlate data, and requires customers to create custom reports and dashboards specific to the sources they're pulling data from.

How to Enhance Splunk with ArcSight Security Open Data Platform (SODP)

So how can Splunk benefit from ArcSight SODP CEF formatted data? SmartConnectors offered in the ArcSight SODP serve multiple functions. First of these is the ability to simply onboard any data source once and then share it with multiple destinations simultaneously. Using the ArcMC management server, all of these connectors can be easily maintained and deployed through a single interface, including the ability to send the data to any new destination with a few simple clicks. With the added help of ArcSight SODP for Splunk app, Splunk can accept and understand all these normalized events.

Additionally, by deploying the app and ArcSight SODP SmartConnectors between your data sources and your Splunk environment, you enable Splunk to start receiving aggregated data instead of non-aggregated data. In some cases, this aggregation can enable you to reduce the flow of information into Splunk by as much as 90 percent*, while still delivering all the essential information you need for analysis. The following basic scenario can help clarify how it works:

- If a system reports 100 failed login attempts by user Bob, the normal non-aggregated data stream into Splunk receives 100 separate failed raw login events for user Bob.
- If a system reports 100 failed login attempts by user Bob, the ArcSight SODP SmartConnector generates one single event that indicates user Bob had 100 failed login attempts and sends this single event to Splunk.

As an added benefit, the SmartConnector actually enriches the event data in multiple ways before sending it to Splunk. Since the SmartConnector knows it's an authentication event, it categorizes it as such for future reporting. It also looks up the IP address of the source and destination IP and resolves those to host names. Finally, it might see that Bob is part of the accounting group, and adds that helpful context as well before sending it on to Splunk.

Not only can the aggregation that ArcSight SODP provides significantly reduce unnecessary data utilization of your Splunk license, but it can lower data storage requirements as well. You also get simplified and more consistent querying and reporting in Splunk through the data normalization provided by ArcSight SODP. Since the

*Validated with internal benchmark testing; however, aggregation thresholds will determine the reduction.

The SOC must fundamentally restructure itself to ingest and process the tsunami of data required for threat detection.

ArcSight SODP SmartConnectors normalize your data into the single CEF standard schema instead of 23 different schemas, you can create a unified set of dashboards and reports that will work for all your data sources.

You can also enjoy all of these same Splunk enhancing benefits through ArcSight SODP's Transformation Hub module. The Transformation Hub is a massively scalable message bus and stream processing cluster that brings together data from multiple sources to multiple destinations in a way that reduces network complexity and computing requirements. Transformation Hub provides centrally managed routing and filtering on CEF fields, delivering the right data to the right application. It also offers SmartConnector normalization and enrichment for syslog data as streaming processors, allowing customers to easily handle data storms and increased data flows. Designed to handle hundreds of clients at hundreds of megabytes per second, Transformation Hub's cluster can be easily expanded to meet the data ingestion and delivery needs of the largest SOC, while reducing complexity and improving manageability.

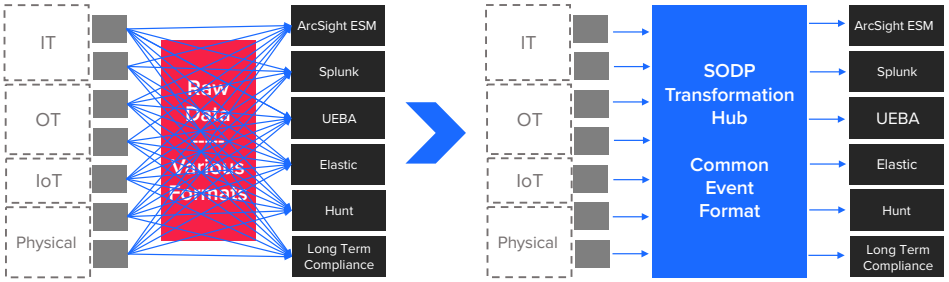

Figure 2. Before ArcSight SODP and after ArcSight SODP architecture

Get More from Splunk with ArcSight SODP

It's the open architecture approach that OpenText takes with ArcSight SODP that enables it to deliver the cost-saving aggregation and report-enhancing normalization benefits. ArcSight SODP removes the complexity and chaos that often accompanies big data security, making it easy for your SOC to share and leverage enriched security data with your Splunk environment, data lakes, analytics tools, and other best-of-breed security solutions. For more information on how you can leverage ArcSight SODP to get more out of your investment into Splunk and your other security solutions, contact your OpenText sales representative.

Learn more at
www.microfocus.com/sodp

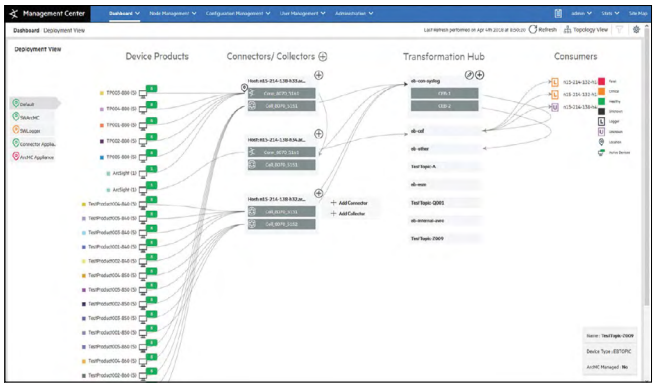

Figure 3.
SODP centralized management console—end-to-end monitoring

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.

761-000075-003 | O | 10/23 |