Flyer
Security

The New ArcSight Enterprise Security Manager Is Here! Introducing ESM 7.0

Does your SIEM need rejuvenating? ESM 7.0 is bigger and badder than ever.

ArcSight Enterprise Security Manager is central to the modern intelligent Security Operations Center (SOC). As a leading Security Information and Event Management (SIEM) platform, it sits centrally within an organization to collect and triage events from across systems & security tools, detecting cyber-security threats in real time while helping SecOps teams and analysts respond quickly to evolving threats. Paired with the new ADP Event Broker and the power of distributed correlation, it is able to scale to meet the most demanding security requirements.

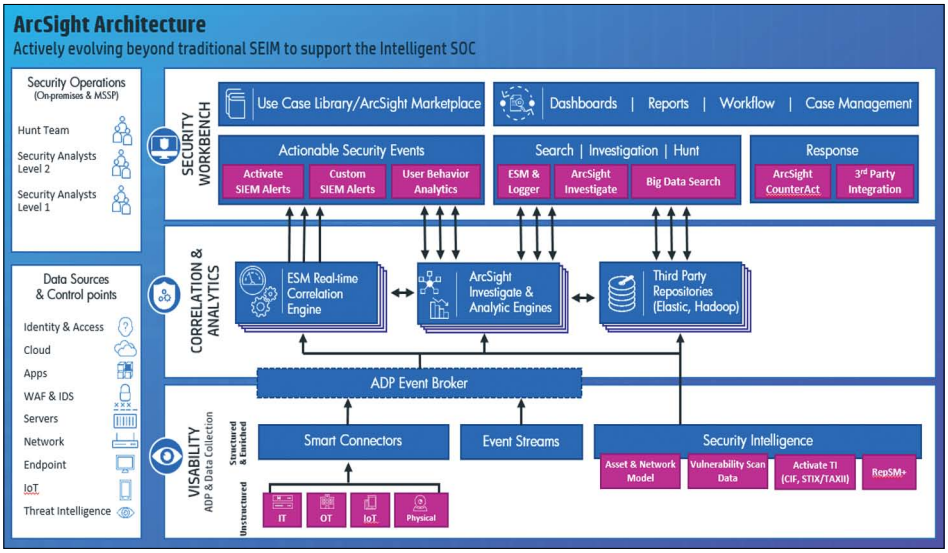

Figure 1. ArcSight Architecture

New ArcSight Capabilities

Distributed Correlation

What happens when you combine the most powerful SIEM correlation engine with distributed node/cluster technology? ESM 7.0! By decoupling the components used in the advanced correlation processes, customers can now add additional nodes to the ESM cluster, scaling ESM like never before, analyzing up to 100,000 events per second.

New UI Options

Adding to the popular light and dark themes, ESM 7.0 brings with it more user interface & visual improvements. Check out the new charts, global SOC dashboard and right-click drill down features within Console.

Event Broker Event Collection

Many organizations continue to struggle with the volume and velocity of events generated by their internal systems. As part of the ArcSight Data Platform (ADP) Micro Focus® has adopted

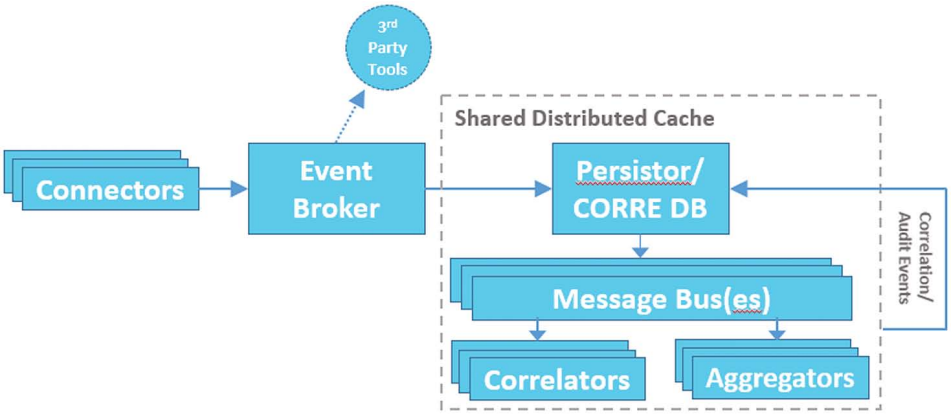

Figure 2. ESM Distributed Correlation Architecture

the leading edge, open message bus technology, based on Apache Kafka. ArcSight ESM can now subscribe directly to Event Broker topics to ingest normalized events off the bus.

Activate Framework

ESMs best practice content framework Activate continues to gain traction by allowing customers to build and share correlation rule sets and logic in their SIEM. Activate now includes hundreds of use case solutions and packages, and the list of support vendor products included with Activate continues to grow.

Cyber Threat Intelligence (CTI)

A new addition to the Activate Threat Intelligence package now includes support for common threat sharing standards like STIXX and CIF. Customers can now gain more value to their SIEM by adding threat intelligence to the SIEM correlation content.

Be sure to check out the new ArcSight Content brain at: https://arcsightcontentbrain.com

New Audit Events

For mature SOCS and managed security providers, metrics are everything. ESM now includes new audit events for tracking SLAs, case changes & rule modifications.

The ArcSight suite continues to lead in their comprehensive real-time threat detection, analysis, workflow, and compliance management platform. Visit the ArcSight page to see what we've been working on or call your representative to schedule a demo or participate in a virtual workshop.

Contact us at:
www.microfocus.com

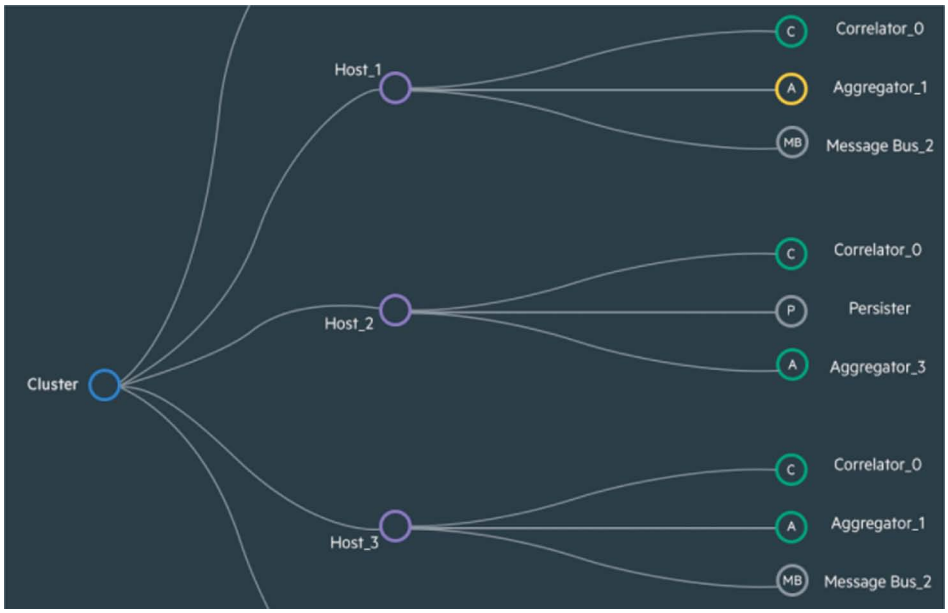

Figure 3. Cluster view as seen from ArcSight Command Center

Learn More At

www.microfocus.com/arcsightesm