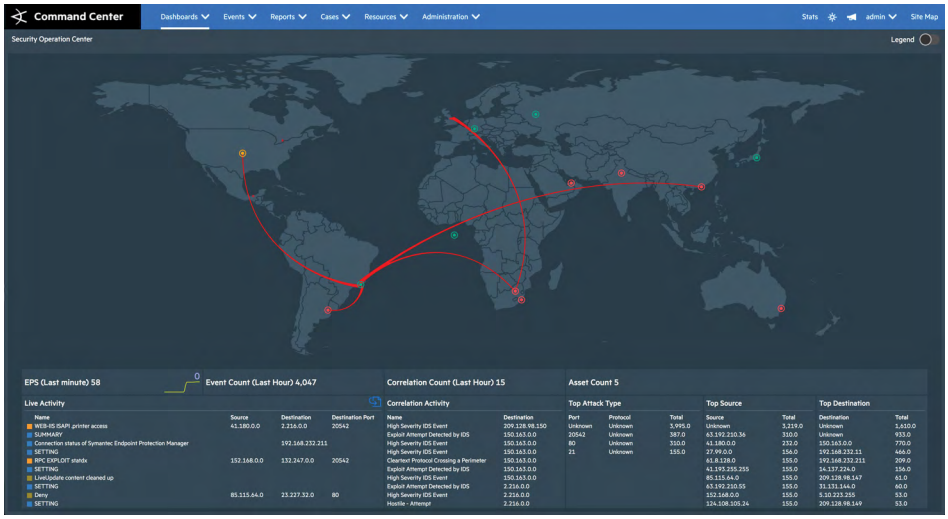
ArcSight Enterprise Security Manager (ESM)

When it comes to threat detection and response, every second counts. ArcSight ESM is a comprehensive SIEM platform that detects, analyzes, and prioritizes threats in real-time, and supports Security Operation Centers (SOCs) with workflow, response and compliance management. ESM's industry-leading threat correlation engine lays the foundation for effective security analytics in a SOC.



What's New over the Last 2 Years

- Global Event IDs make it easier than ever to **track unique events** across ArcSight.
- Performance and stability improvements, migration from Oracle JDK to **OpenJDK**, and an upgraded **MySQL** engine.
- Improved integration with **ServiceNow**
- New **default content** ready at installation.
- New dashboard maps events to the **MITRE ATT&CK** framework.
- **Improvements to UI**, including light/dark themes, new charts, right click drill-down features, and a **global SOC dashboard**.
- **Distributed correlation** mode deploys multiple instances of correlators and aggregators to **increase processing speed** and provide failover processing.

Did You Know?

- ArcSight ESM sits centrally within an organization to **collect, analyze and triage events** from across systems and security tools to detect cyber-security threats in **real time**, and to assist SecOps teams in responding quickly to evolving threats.
- Offers the industry's most powerful real time correlation to **drastically reduce threat detection and response times**.
- Can correlate up to **100k EPS** and collect and structure up to **1M EPS** from over **480 data sources**.
- Sets the foundation for **open, layered security analytics** (Correlation, UEBA, Threat Hunting, etc.).

Kuwait Finance House

"The ESM correlation engine is one of the best in the industry."

MR MAJEED BEHZADI
Executive Manager, Group Information Security Management and IT Infrastructure Design

Micro Focus

"MITRE is going to be used a lot more in the coming years. How we find solutions covering MITRE, making better use of MITRE, is the way to enable a Next-Gen SIEM."

EMRAH ALPA
Sr. Product Manager

IT Security Provider

"[ArcSight] is very flexible. They can customize it and fine-tune it any way they want."

MANAGER