Product Flyer
Security

Speed Up Security Operations with ArcSight SOAR

ArcSight SOAR is a leading Security Orchestration, Automation and Response Platform (SOAR) which combines orchestration of both technology and people, automation and incident management into a seamless experience. ArcSight SOAR helps security teams improve their efficiency in responding to cyberattacks in security operations.

ArcSight SOAR Solution at a Glance:

- **Robotic Process Automation for Cyber:**
  Eliminate repetitive activities to focus on what matters most.
- **Collaborative Defense:**
  Investigate and respond collaboratively, engage and involve everyone in the organization.
- **Central Command and Control for SecOps:**
  Single pane of glass for security operations.
- **Measure and Govern Security Operations:**
  Collect and measure all SecOps activities.

Automate Repetitive Activities

ArcSight SOAR provides an automation engine; one can think of it as a SOC robot. It is field programmable, so organizations can program the product to their liking; as if teaching a new employee how you handle different types of security incidents.

ArcSight SOAR automation engine supports visual programming and Python; one can define arbitrarily complex scenarios for the product to execute. ArcSight SOAR currently integrates with 120+ different infrastructure and security tools; so, it can interrogate these systems or take actions on them to understand an ongoing attack or take blocking action.

Many organizations may not feel comfortable with a product taking blocking actions on behalf of them and may be worried about potential wrongdoings. With ArcSight SOAR it is possible to define human approvals and/or checkpoints; the product can stop and asks confirmations to relevant staff members before taking critical actions.

Automation helps offloading time-consuming mechanical work, so the SOC staff can spend their time on what matters more and/or spend time on improving themselves.

Improve Analyst Efficiency

ArcSight SOAR provides a unified incident management service desk. All security incidents arrive at this service desk, and case management functionality is provided for all types of incident sources; SIEMs, other service desks, web forms, 3rd party applications, etc. can feed service desk.

The intuitive and simple service desk allows security investigations from a single pane of glass. Instead of switching between multiple different tools and logging in and out of them, product allows SOC staff to solely the service desk to invoke such tools, making the platform a unified investigations interface.

Instead of giving SOC analysts a lot of passwords, the product acts as an access control gateway. Controlling precisely who can do what and where allows delegation of sensitive security work to less experienced staff members without taking any disruption risks. ArcSight SOAR allows a lot of work to be delegated safely and securely.

Capturing and recording every command and its results, it builds an incident timeline; a history of every incident case recorded. The incident timeline not only allows accountability and auditability but also fosters collaboration;

Contact us at:
www.microfocus.com

Like what you read? Share it.

multiple analysts can work on the same incident together.

Measure and Monitor SecOps KPIs & Metrics

The product records all activities of the analysts and the product itself. Everything is not only logged but also forwarded to the SIEM platform of choice for segregation of duties. From all recorded events, ArcSight builds up a lot of metrics and continuously analyzes the security operations.

Product utilizes all collected data of the analysts and the product itself to build dashboards and reports for organizations to understand and govern their security operations better. Customizable dashboards provide 50 different dashlets that one can customize; so building custom dashboards is a breeze. By providing detailed reports on individual incident for analyst or team level ArcSight SOAR helps the SecOps teams understand historic events and better plan future directions. Product comes bundled with over 20 canned reports. Reporting also helps internal and 3rd party audit teams to be able to audit security operations.