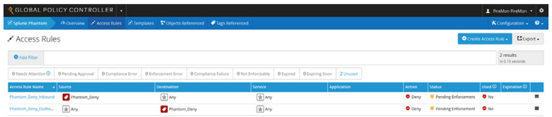
REV UP YOUR THREAT DETECTION AND REMEDIATION WITH FIREMON AND SOAR SOLUTIONS

Security Operations Centers (SOCs) are under growing pressure to achieve more with less, detect and counter threats with sub-second response times, and yet be very consistent in their approach to enterprise security. FireMon's security policy automation solution, integrated with best-of-breed security, orchestration, automation and response (SOAR) tools, allows you to combat security incidents at lightning speed.

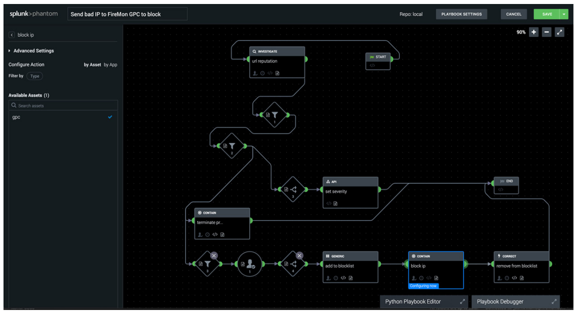


Access Rules

2 results in 0.15 seconds

0 Needs Attention | 0 Pending Approval | 0 Compliance Error | 0 Enforcement Error | 0 Compliance Failure | 0 Not Enforceable | 0 Expired | 0 Expiring Soon | 2 Unused

Access Rule Name	Source	Destination	Service	Application	Action	Status	Used	Expiration
Phantom_Deny_Inbound	Phantom_Deny	Any	Any		Deny	Pending Enforcement	No	
Phantom_Deny_Outbo...	Any	Phantom_Deny	Any		Deny	Pending Enforcement	No	



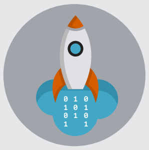
THE CHALLENGE

SOC Optimization and Threat Management

SOAR platforms offer enterprises an arsenal of tools to achieve multiple goals – streamlining SecOps and incident response workflows by identifying malicious domains, automating malware analysis, orchestrating security processes across multiple tools, and assigning priority and response to incidents. Many organizations that have deployed SOAR platforms are trying to prioritize and manage exactly where automation and orchestration should be applied. However, SOCs work with multiple security tools, so it is important to see how SOAR solutions can be integrated with others in order to ensure that enterprise security response efforts are optimized.

One area of integration that helps organizations realize the potential of their SOAR investments is network security policy management (NSPM) platforms with SOAR to achieve forensic and real-time policy change management to mitigate risks, which is not possible with standalone SOAR platforms. FireMon's NSPM platform offers infrastructure-agnostic, best-in-class, automation-powered security policy change management. By integrating with industry-leading SOAR platforms such as Splunk (Phantom), Palo Alto Networks (Demisto), and Rapid 7 (Komand), FireMon offers accelerated cross-platform network security policy management focused on early detection and mitigation of security risks. This integration will allow security personnel to triangulate SOAR analytics with FireMon's real-time visibility across known and unknown networks, including cloud, to execute change requests for restricting access to malicious IPs. In addition, SecOps teams speed up policy management changes up to five times faster, reduce manual errors, and integrate with a variety of security tools.

FIREMON



HOW FIREMON ACCELERATES SOAR

77% of organizations do not have a formal cybersecurity incident response plan*. If you want to apply a formal cybersecurity response plan across your enterprise, it is important that policy change implementations are integrated with your SOAR strategy. FireMon adds value to your SOAR investments with:

- Security configurations generated in seconds, not days – saves SOC teams valuable time
- Global policy visibility and management of hybrid network security posture
- Automatic cleanup of device rules that are no longer required
- Continuous security control across traditional and virtual platforms
- Support for new architectures such as microsegmentation and Zero Trust
- Seamless SOC workflow integration and with FireMon Security Manager monitoring and reporting tools

* Ponemon Institute. "The Third Annual Study on the Cyber Resilient Organization." March 2018.

THE SOLUTION

Take SOAR to the next level with FireMon

FireMon offers out-of-the-box integration with SOAR tools to deliver accelerated incident response. This is achieved by combining automation, machine learning and natural language processing in a simple, workflow-centric interface to deliver context to data.

Most incident response (IR) teams spend a lot of time collating increasingly complex data, normalizing data from disparate sources, and analyzing it – resulting in very long lead times before remediation can happen. FireMon's orchestration, automation, and analytics capabilities transform complex and disparate data into actionable insights in real-time, accelerating threat detection and analysis without requiring a query language or customization, saving valuable time and costs. FireMon's rich set of APIs allows organizations to build their own integrations and automation while our Security Intelligence Query Language (SIQL) enables in-depth and conclusive assessment of security infrastructure.

Five must-ask questions for best-of-breed NSPM + SOAR integrations

Irrespective of the type of SOAR solution that your organization has deployed, any SOAR and NSPM integration must satisfy the following five questions:

1. Does your NSPM vendor provide out-of-the-box integration with SOAR solutions as well as custom integrations to future-proof any additions to your SOAR deployments?
2. How does your NSPM vendor support SOC workflow and collaboration? Can they support always-on visibility and real-time reporting to ensure that nothing is lost in transit?
3. Does the platform deliver intelligent alerts – offer evidence-based, grouped alerts so that the SOC teams can quickly make informed decisions on remediation?
4. Using the data delivered, can your SOC team identify the context on indicators of compromise (IoCs) and the tactics, techniques, and procedures (TTPs) of threat actors?
5. Does the NSPM platform perform the necessary sanity checks before a policy change is implemented – at the strategic, tactical, and operational levels?

WITH FIREMON, YOUR SECOPS TEAM CAN:

☑ Achieve real-time vulnerability discovery and analysis, saving time and optimizing the efforts of security personnel

☑ Perform contextual analysis and correlation of internal and external data, both historical and in real-time

☑ Gain 100% infrastructure visibility and situational awareness across physical, virtual and cloud networks

☑ Automatically perform device-level policy changes, minimizing policy change latency

☑ Ensure that blocking IPs from SOAR tools does not trigger outages or performance degradation of applications

WHO IS FIREMON?

FireMon delivers continuous security for hybrid enterprises through a powerful fusion of vulnerability management, compliance and orchestration. Since creating the first-ever network security policy management solution, FireMon has continued to deliver real-time visibility and control over complex network security infrastructures, policies, and risk postures for more than 1,700 customers around the world. For more information, visit **www.firemon.com.**

FIREMON