FIREMON

FIREMON TECHNICAL BRIEF

FireMon + Swimlane

Taking SOAR beyond SOC efficiency

Traditionally, security orchestration, automation, and response (SOAR) tools have been associated with security operations center (SOC) teams and how they accelerate the speed with which SOC teams validate incoming alerts and launch mitigation efforts. However, there is a larger, more comprehensive application of SOAR solutions when integrated with the FireMon platform – embedding this right at the point of designing and making future changes to the network.

A key expectation of SOAR solutions – apart from alert triage and incident response – is augmenting dynamic access control, ensuring that users are enabled and disabled accurately.

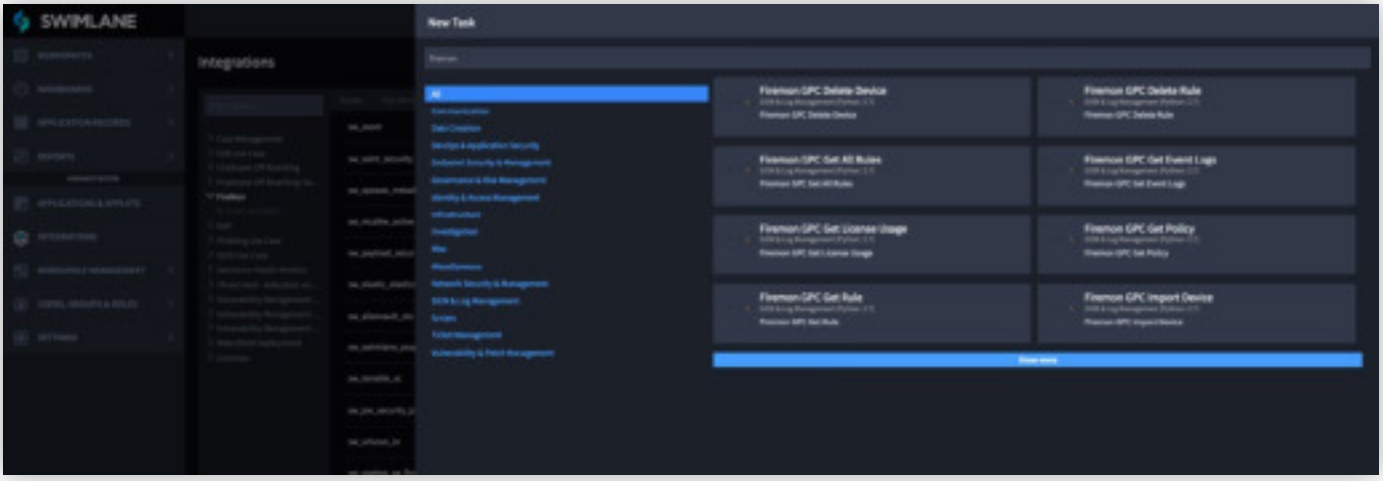
FireMon helps enterprises achieve forensic and real-time policy change management to mitigate risks. FireMon's platform offers infrastructure-agnostic, automation-powered security policy change management. By integrating with Swimlane, FireMon allows accelerated cross-platform network security policy management focused on access control with foundations in 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 the cloud, to execute change requests for restricting access to malicious IPs.

In addition, SecOps teams accelerate policy management changes up to 5x faster, reduce manual errors, and integrate with a variety of security tools.

How FireMon Adds Value

FireMon helps apply a formal cybersecurity response plan across your enterprise by integrating policy change implementations with your SOAR strategy. By integrating FireMon and Swimlane, you can speed up your SOC operations with:

- Security configurations generated in seconds, not days – saves SOC teams valuable time. FireMon enhances the threat hunting ability of SOAR platforms to make intelligent decisions in real-time to mitigate risks
- 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
- Seamless SOC workflow integration and with FireMon Security Manager monitoring and reporting tools



Features	Customer Benefits
Accelerated incident response	Native visibility features of FireMon integrated with vulnerability scanners to obtain real-time scan, correlating these with network topology and security configuration data from FireMon Security Manager.
Security can be integrated into network design to govern and control all the moves, adds, and changes to the network	Implement a security-driven network strategy
FireMon Automation added to SOAR's security orchestration capabilities	Faster remediation and simplified security operations
Extend FireMon's orchestration, automation, and analytics capabilities into your Swimlane deployment	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

How FireMon's Swimlane Integration is Unique

FireMon's integration with Swimlane helps strengthen the foundational elements of the SOAR solution so that it can deliver fully on its promises by leveraging contextual data, configuration and security policy orchestration, and precise visibility into the enterprise's security infrastructure. FireMon optimizes the Swimlane solution by making contextual data about all the devices across the security stack available automatically and in real-time. FireMon's extensive APIs allow effective and seamless integration with third-party security devices, delivering IP addresses, status of devices, and change information to the Swimlane platform. Swimlane can then use this data to block or unblock domains, check information on IP, host, network and domains, and enrich other security tools in the stack.

With FireMon + Swimlane, 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 manage security policies 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

To learn more about FireMon's integration with Swimlane, please visit www.firemon.com