FIREMON TECHNICAL BRIEF

The FireMon + Swimlane Integrated Solution

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.

Swimlane and FireMon's products have many strengths that this integration combines for an even stronger solution. Swimlane helps drive success by delivering key insights and ROI metrics to security managers and amplifies the efficiency of security operations.

Swimlane:

- Provide reporting capabilities through data aggregation across all security technologies and teams.
- Bring transparency into incident response processes, to reduce risk.
- Measure staff efficiency to identify bottlenecks.
- Allow managers and CISOs to analyze their technology stack to identify optimization opportunities.

FireMon empowers enterprises to achieve forensic and real-time policy change management to mitigate risks. By integrating the two, we can accelerate cross-platform network security policy management, early detections, and the mitigation of security risks. Our integrated solution will allow security personnel to utilize Swimlane's SOAR analytics along with FireMon's real-time visibility, across known and unknown networks, 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 the Integrated Solution Adds Value

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

- Security configurations generated in seconds, not days which saves SOC teams valuable time.
- Automation and orchestration reduces Mean Time To Resolution (MTTR) across alerts.
- Delivers global policy visibility and management of hybrid network security posture.
- Offer continuous security control across traditional and virtual platforms.

Features	Customer Briefs
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.

Why this Integration is Unique

Our joint integrated solution extends the foundational elements of both solutions by leveraging contextual data, configuration information, security policy orchestration and automation, and by adding precise visibility into the enterprise's security infrastructure. FireMon optimizes the Swimlane solution by providing contextual data about all the devices across the security stack available automatically and in real-time. FireMon's extensive orchestration 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. This data can also be used by Swimlane to orchestrate actions on other integrated products and devices within your security stack.

With FireMon + Swimlane Solution, 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

About Swimlane

Swimlane is the leading independent SOAR solution created by analysts for analysts. It delivers scalable security solutions to organizations struggling with alert fatigue & analyst burnout. www.swimlane.com

To learn more about FireMon & Swimlane, please visit www.firemon.com and https://swimlane.com