There are two critical roadblocks to an effective security, orchestration, automation, and response (SOAR) strategy. 1. Organizations tend to focus on automation without really defining security workflows, and 2. Adding context to security threats for threat validation and effective remediation/mitigation. We need to see this against the backdrop of a rapidly expanding attack surface and the associated costs. The 2019 Cost of a Data Breach Study by the Ponemon Institute found the average cost of a data breach increased from $3.86 million to $3.92 million in the last year. Add to this a significant shortage of skilled security talent to fill jobs. Some estimates put the number of unfilled security roles at 3.5 million by 2021. In a survey conducted by ESG in 2019, 53% of organizations reported they were facing a cybersecurity skills shortage.

In such a scenario, there is a strong need to enhance the performance of SOAR technologies in order to fully realize their potentials in threat hunting, detection, and response. FireMon integrates with a number of SOAR platforms like Swimlane, Splunk Phantom, Palo Alto’s Demisto, and Rapid7 to deliver a highly integrated workflow to accelerate any moves, adds, and changes (MAC). With FireMon, organizations can achieve forensic/contextual and real-time policy change management to mitigate risks, something that is not possible with standalone SOAR platforms.

The integration of FireMon increases the value of SOAR into a truly dynamically enforced solution. As threats are discovered, FireMon can automate global firewall containment policies across the infrastructure, spanning the network and security devices from multiple vendors. The SLA lead time for both temporary and continuous threat containment is shortened significantly.

**Strong Integration, Multiple Use Cases**

Using a rich set of APIs, FireMon offers a set of customizable playbooks for SOAR integration to provide multiple services to the enterprise including:

- Faster provision of user accounts by applying global policies to endpoints
- Speeding up and streamlining audit and compliance reporting by tracking and logging all steps taken to contain and mitigate threats
- Automation of host and perimeter alarms by blacklisting the risk-prone URLs, IPs, and domains

While some security teams report mitigating threats from identified malicious IPs can take hours or days, with FireMon integrated into your SOAR platform, you can block these threats immediately. FireMon can address the needs of multiple security decision makers (SOC, SecOps, NetOps) and use cases (proactive threat
With FireMon, identified risks can be immediately remediated while ensuring that there are no unnecessary policy changes and avoiding misconfigurations. FireMon’s policy automation solution speeds up response and allows your security team to unleash the full potential of your SOAR investments to:

- Automate and optimize workflows to reduce manual errors
- Make policy changes in real-time, ensuring that your networks are always protected
- Integrate with a variety of security tools to optimize your organization’s security posture
- Speed up policy management changes by 5x

Learn more about how automation can change your network and supercharge your threat and vulnerability management by visiting www.firemon.com.