LogicHub

SOLUTION BRIEF

Experience the LogicHub SOAR+ Difference

Challenges with traditional SOAR

Like most security operations teams, yours is probably buried by an overwhelming volume of alerts that requires learning and using dozens of specialized tools to address different threats, each with its own set of processes and tasks. And that buries your analysts in repetitive, low-value, time-consuming activities. Instead of taking a strategic approach to security, they end up reacting to individual threats without ever getting ahead of the problem.

SOAR (security orchestration, automation, and response) solutions entered the market to address these challenges. But traditional SOAR solutions are difficult to implement, and once they're up and running, SecOps teams don't know where to start automating or what playbooks to build. Often, the out-of-the box content doesn't map well to the organization's environment and requires extensive development time to customize. And even once the solution has been implemented, traditional SOARs aren't architected to handle the high volume of event and alert data to analyze, investigate, and triage threats. That means companies remain stuck with lengthy mean-times-to-detect.

Experience the LogicHub SOAR+ difference

LogicHub believes your SecOps team should be fully supported throughout the entire threat lifecycle. Our playbooks deliver automated detection and response, drastically reducing both MTTD and MTTR while freeing your analysts to focus on advanced, proactive and strategic security activities.

Reduce false positives by more than 95%

Lower incident response times by as much as 99%

Experience the LogicHub SOAR+ difference

Extensive integrations
Open API framework integrates with any platform or tool quickly. Any new, or required integration is added at no cost in under two weeks.

Easy to use and operate
Designed for usability with a simple playbook builder with automated suggestions for guided automation, ensuring rapid time-to-value and operational adoption.

Automation-driven case management
Fully enriched cases with suggested actions, task management, in-case commands, and hybrid automation with optional one-click execution deliver deep visibility and rapid response.

Powerful, automated analytics
Automatically analyzes millions of security events at machine speeds, letting you detect, triage and respond to critical security threats faster.

Accurate decision automation
Embedded machine learning in analysis, detection, and response playbooks enable them to learn like human analysts for more accurate decision making

Continuously updated content
Our security experts are constantly creating new detection and response playbooks, integrations, and dashboards to help you address critical use cases

Get the most out of your SOAR platform

Automation is critical to running effective security operations, but a traditional SOAR is only effective after a confirmed event has triggered a playbook. The LogicHub SOAR+ platform starts by automating the analysis and detection of advanced threats, drastically reducing both your detection and response times.

Capability	Traditional SOAR	LogicHub SOAR+
Open API integration framework	✓	✓
Automated incident response playbooks	✓	✓
Customizable dashboards	✓	✓
Automation-driven case management	Some	✓
Ability to execute hoc actions within individual cases	Some	✓
Extensive and easily customized out-of-the-box content	Some	✓
Automated incident response with one-click execution	Some	✓
Embedded machine learning for adaptive, automated decision making		✓
Automated analysis, investigation and triage of high-volume alert and event data		✓
Guided playbook builder with automatically recommended next steps		✓
Autonomous threat detection with automated risk scoring		✓

LogicHub SOAR+ has a flexible architecture that can run either in the cloud or on-premise—the choice is yours. Either way, you get security orchestration, automation, and response that is uniquely adapted to fit your requirements.

Learn more

To learn more about LogicHub SOAR+ visit: www.logichub.com/soar

LogicHub

a: 301 N Whisman Rd Mountain View, CA 94043
w: www.logichub.com
e: info@logichub.com
p: (650) 262-3756