LogicHub

4 Common Objections to Security Automation…

…and how LogicHub will help you overcome them

Why Your Team Needs Security Automation

When it comes to protecting your organization from malicious threats, fast response times are critical. But security analysts waste as much as 75% of their time investigating false positives and are further slowed down by repetitive manual processes, making automation a critical need for security operations.

Automation can reduce false positives, increase threat detection accuracy, improve operating efficiency, and rapidly execute incident response actions. Simply by eliminating the majority of false positives, you can reduce alert fatigue and staff burnout while significantly improving your organization's mean time to detect and respond (MTTD and MTTR) to real threats.

And on top of the efficiency gains, security automation is a critical component of risk reduction.

Nobody plans on being breached, but the odds that it can happen to you are uncomfortably high. And industry research shows that automation can deliver quantifiable, significant risk management returns.

But many organizations are reluctant to fully embrace automated incident response for a variety of reasons, including:

- Security automation will be too complex and expensive to deploy
- Security alerts are too inaccurate to trigger the right response
- Ensuring that the right action is executed every time is too difficult to control
- Executing the wrong action may do more damage than the initial threat

LogicHub addresses these concerns in numerous ways, giving you flexible options for deploying security automation without the concerns typically associated with an enterprise SOAR platform.

$6.03 million -the average cost of a data breach for organizations without fully deployed security automation

$3.58 million -the average savings from a breach for organizations with fully deployed security automation—a 60% reduction

2020 Data Breach Inivetigations Report-Verizon

Security alerts are too inaccurate to trigger the right response

If you can't trust the alert, why would you trust the response? The majority of security alerts are false positives, so by nature there's a high probability that any automated response is the wrong thing to do.

LogicHub solves this problem in two ways. Automated alert triage reduces false positives by more than 95%, allowing you to focus on the threats that really matter. And one-click automation queues up the correct response, letting you investigate the alert before authorizing any action. When a case is generated, it delivers all relevant context allowing you to quickly verify if a threat is real so that you can take action.

This allows you to use a phased approach to automation, letting you assess detection and triage accuracy before authorizing any response, until you've reached a comfort level to toggle a fully automated response.

How LogicHub solves this problem:

- **Automated alert triage reduces false positives by 95%**
- **One-click automation allows for verification before execution**

Ensuring that the right action is executed every time is too difficult to control

Security automation has traditionally operated in a very binary way, lacking the intelligence to accurately assess when and if an automated response is appropriate to a specific situation. This all-or-nothing approach assumes that every aspect of a specific threat and the target is the same in all situations. But threat severity is often dependent on a variety of factors, requiring a more intelligent approach to deciding what action is appropriate when for each instance.

LogicHub uses machine learning to deliver intelligent decision automation that emulates human expertise, accurately assessing the actual risk for each individual threat. This allows you to base your level of automated response on multiple factors like threat severity, intended target, potential impact, and type of action. That allows you to fully automate containment actions for severe threats with greater damage potential, while giving you the opportunity to rapidly investigate lower risk threats before authorizing a potentially intrusive action.

How LogicHub solves this problem:

- **Intelligent decision automation uses machine learning to accurately assess each threat, delivering accurate risk ratings to guide response actions**
- **Automated response can automatically adapt to different threat vectors, specific event context and organizational factors**

Executing the wrong action may do more damage than the original threat

How LogicHub solves this problem:

- Ad hoc CLI let you choose your response directly within the case
- Recommended actions within any case let you intelligently select and execute any automation based on industry best practices

One of the biggest barriers to automation is the fear that without an expert set of eyes managing the process, a response will be automatically executed that causes more damage than the threat. This could result in a potentially catastrophic business disruptions like a mission critical production server being taken offline or a user account being disabled at the wrong time.

LogicHub gives you complete control over how automation is deployed in your environment. In addition to one-click approval, analysts can also quickly choose and execute any action from an intelligent CLI built into every case. That allows them to test and assess different actions in response to specific threats to pinpoint the correct response. And hundreds of out-of-the-box detection rules are mapped to the MITRE ATT&CK framework, including recommended response actions that can be executed based on your comfort level.

Security Automation will be too complex and expensive to deploy

Perhaps the primary reason organization are slow to adopt security automation is the complexity and cost of getting an enterprise SOAR platform deployed. And that's assuming that you know where to begin automating. And when out-of-the-box content isn't mapped exactly to your environment and requirements, or the actions that you need haven't been developed yet, you're either on the hook for complicated software development or costly professional services.

LogicHub offers inexpensive and flexible solutions for removing deployment complexity and controlling operating costs. From fully managed SOAR deployments starting at $500/month, to a strong development focus on ease-of-use, we deliver the solutions you need to make security automation a reality.

How LogicHub solves this problem:

- We'll deploy security automation for you, with minimal overhead
- You'll benefit from an extensive library of out-of-the-box content adapted to you
- You can easily request new actions directly within the platform, delivered in under 3 days
- Switching between one-click authorization and full automation is a simple toggle
- If you prefer to build your own playbooks, an automation-driven builder can suggest recommended actions for fast and simple configuration

1. How much of your team's time will be required to implement and configure your playbooks?
2. How will you be able to test and verify actions to align them correctly for each specific threat?
3. How easily can you add new actions that are not included out-of-the-box
4. How will your SOAR help you ensure response actions will be triggered by accurate security alerts?
5. How easy is it to test different response actions within the SOAR platform based on different event variables?
6. How much time will it take to tune vendor-provided content to match your environment?
7. Do you have the time and skillset to fully define and plan your playbooks?
8. What capabilities does the SOAR platform offer to help you keep false positives to a minimum?
9. How well equipped will your SOAR be to automate deep threat detection and enrichment?
10. Does your SOAR provider offer managed solutions that will allow you to benefit from SOAR without adding the overhead?

10 Questions to Answer When Choosing Your Security Automation Solution