Guide: Enhancing Your Response Capabilities

INTRODUCTION

No level of investment prevents or blocks 100% of attacks on your critical IT systems. The continuous monitoring, detection, and response to breaches and other security gaps — before damage occurs — is imperative to your organization's success. As hackers become savvier, attacks can increase in sophistication and more effectively evade existing prevention tools. Rising staff shortages have also forced a growing number of organizations to partner with cybersecurity providers, with proven technology and experts, to minimize damage and disruption to business operations.

This guide for security professionals explores the processes, challenges, and best practices of implementing automation into your response strategy.

Getting Started

Organization who begin a response initiative without a properly defined strategy will typically result in one of two things:

- Relying on a single tool capable of detection and response; or
- Purchasing a SOAR tool without the people or processes in place to take advantage of its powerful capabilities.

Both cases are typically poor returns on your investment.

A better option is adopting a more comprehensive plan to address people, process, and tools.

- See the seven pillars of a comprehensive automated response plan below.

It is essential to understand how to deploy an automated response solution BEFORE building a comprehensive strategy, as this will help define your requirements and goals. A combination of simple, self-service implementation, coupled with the right security partner, simplifies execution.

DRIVERS FOR OPTIMAL RESPONSE

As you evolve your cybersecurity strategy you need to ensure you have a strong, comprehensive response plan that is built on a solid foundation:

Seven Key Pillars for Effective Response

1 Detection Strength: ***Trust that the underpinning of an effective response strategy is broad detection.*** This requires a broad log ingestion ecosystem, allowing for the appropriate depth of data and breadth of sources to detect across the entire kill chain. Outcomes can then scale through analytics while implementing advanced technologies (e.g., machine learning and building extensions) through API-based connections. Visibility into pre- and post-breach environments, analyzing data, and producing insights across the IT estate are critical to enable response actions spanning network, endpoint, and cloud environments. Various data sources are also needed during forensics to complete the picture of an attack.

2 Broad Response Coverage: ***Discover the ingress and egress points.*** An organization's IT estate is dynamic, but the constants will always include endpoints (client and server), network (firewall, WAF), cloud (AWS, Azure, GCP), and identity (Active Directory, SSO). These are a sampling of sources for telemetry data which are key to detecting incidents. However, they also represent the targets where the response action will occur to minimize the damage of a detected breach. An effective response strategy should include a policy update applied at the endpoints, the network edge, and the cloud service provider.

3 Risk Profile: ***Consider the value of an asset and type of attack.*** A revenue generating asset, such as an ecommerce server, will have a different response than a non-critical asset, like a print server. To understand the type of attack against an asset, ensure you have access to the security content detail, including analytics content and configuration requirements. These insights should be provided in an actionable way. As your IT estate grows in size and complexity, the ability to classify assets with similar criteria to apply the response actions is imperative. Failure to do so will result in significant management challenges.

Strategy

A strong response strategy begins with detection. To cover your entire IT estate, you must have broad and deep detection capabilities or response capabilities will be limited. Ensure you have coverage everywhere you operate.

> "Responding effectively to security events means that responses are tailored to each threat, system and execution environment, as well as to compliance and regulatory requirements, customer obligations, and the organization's overall risk appetite."

Practical Requirements for Responding to Cyberthreats with MDR, 451 Research, S&P Global Market Intelligence, Pathfinder Report, 2021

4 User Experience: ***Examine a solution that allows configurable response workflows.*** They should invoke the optimal balance of process automation and human interaction to address your evolving security requirements. Resource-gapped organizations may not be able to respond to every incident. They may also not want everything automated as that can have adverse effects. The ideal scenario is to automate actions based on circumstances such as the organization's risk tolerance, skillset, and headcount. Some prefer a simplified experience with a sage to guide them in the playbook creation process. Consequently, more sophisticated users may prefer fully customized playbooks.

5 Actions Taken: ***Recognize that effective response is often a blend of multiple actions.*** Prioritization will change based on variables such as incident type, asset criticality, and desired outcomes of the business. The blend should consist of:

- **Notification** — Inform appropriate responders of the security incident with sufficient detail to enable decision-making
- **Containment** — Limit access of the compromised entity, which may mean limiting system services, restricting network access and egress, or reducing user roles and privileges
- **Elimination** — Disrupt the attack and block access to the vulnerable service

In most cases, there will be a notification prompting security teams to further investigate and execute the recommended remediation steps. This could be to update a policy or change control, update a misconfigured service, or apply patches to affected systems.

"[Alert Logic is] Easy to use, and I really like its dashboard because it shows a lot of useful and detailed information; the alerts are accurate and it allows me to be sure of any threat at any time. It is the best security tool and the best solution."

Jaci K.
Senior Software Engineer,
Alert Logic Customer
G2 Review

Did you Know

52% of organizations reported experiencing an increase in the number of information security incidents following the COVID-19 outbreak.*

57% of midsize and large enterprises believe their security staffing level is inadequate to handle the cybersecurity challenges they are facing today.*

50% of midsize and large enterprises believe they are likely to experience a data security breach over the coming year.*

46% of enterprises reported they have a security operations center (SOC) in place, and many of those only operate their SOC during business hours.*

6 Use Cases: ***Understand every organization is at a different stage in their automation journey***. As a result, the ability to incorporate human interaction for response actions allows adoption at a comfortable pace. Consider the following scenarios with human-guided and fully-automated response actions:

- **Indicators of Potential Insider Threat:** An IT administrator's credentials are being used to access and modify previously untouched systems. This could be an early warning to a potential insider threat or could be nothing. The anomalous activity triggers a playbook which sends a push notification to the IT admin and her supervisor on their mobile devices. They are given the choice of disabling the user credentials on Active Directory or investigating further by opening a ticket in ServiceNow.
- **Privilege Access Management Anomaly:** The privileged credentials of a senior executive are being used to manipulate company information from an unusual geography. The incident triggers a playbook to contain the potential threat and notify the security team. The privileges of the credentials are restricted, a push notification is sent to the security administrator, and a message is sent via Slack to notify the security team to verify legitimacy of the activity.
- **Complex Indicators of Compromise:** A patient admitting system at a healthcare clinic is demonstrating abnormal PowerShell activity consistent with known ransomware attack campaigns. The incident instantly triggers a playbook to isolate the compromised host and block communication from an external source at the edge to prevent spreading to other hosts.

In each scenario, there are multiple actions taken. The number of human decisions, conditions, and triggers in the playbook should be customizable to align with the organization's business requirements.

7 Communication: ***Consider appropriate communications carefully.*** In many cases, it is not simply acting that matters, but communicating that action to the stakeholders who need to remain informed or provide additional forensic detail as part of the process. Users should be able to get notified in the popular tools with which they are most comfortable working, such as Slack, Teams, email, or advanced ticketing systems like Jira and ServiceNow. Integrating into these existing collaboration and ticketing platforms enables effective and efficient dissemination of critical information.

Once each of these key pillars is addressed, the last critical piece is the capability to implement and execute that plan. It is essential that the plan be carefully crafted, and easily iterated and improved as needed.

Tips

- There should be a simplified workflow template that can easily be populated with values to achieve a response action on a security control. This is ideal for organizations new to automation.
- More sophisticated organizations should have the ability to design playbooks with the flexibility to create decision trees with multiple conditions and actions.
- When intuition is needed before executing an action, add human decision points.
- Highly repetitive tasks are great for full automation to help IT and security staff focus their resources.

CHALLENGES OF EFFECTIVE RESPONSE

People: There are over three million unfilled security jobs** making it extremely difficult to find and keep skilled security professionals. And it is not just people with security skills which are lacking. According to a report by 451 research, 86% of organizations have a skills gap when it comes to the cloud.***

Process: Introducing a new process or integrating with an existing process creates challenges. There are various tools in use; the assets need to be inventoried and categorized; and critical stakeholders need to be identified before the workflow is created. The workflow also needs to be proactively managed to improve efficiency and efficacy.

Technology: It is not uncommon for mid-sized organizations and smaller enterprises to have more than 20 security tools. Many have overlapping capabilities, and even with skilled security staff, there is a high probability of not getting full value from all the tools. There are also unintended misconfigurations that are either created or inherited across your IT estate.

Simple Notification	Once notified, security or IT teams must translate their own response. Ideal for a robust and experienced security team that wants to control response from end to end.
Notification with Guidance and Recommendations	Provides prescriptive analysis along with guidance and recommendations for response, enabling IT and security teams to contextualize threats and prioritze response efforts.
Containment/Blocking	Spanning manual, semi-automated and fully automated response actions that include disabling accounts, pushing configuration changes and isolating compromised hosts.
Remediation/Eradication	With the goal of fully eradicating the threat from the customer's IT ecosystem and preventing reoccurrence, remediation takes various forms — manual and automated actions, consultative services, and boots on the ground for more complex situations.
Recovery/Restoration	A distinct discipline that is typically outside the scope of services offered by threat detection and response providers. May be offered as a professional service or through partners.
Breach Management	A distinct discipline that is typically outside the scope of services offered by threat detection and response providers. May be offered as a professional service or through partners.

Figure 1: Overview — types of response from threat detection and response providers
Source: 451 Research

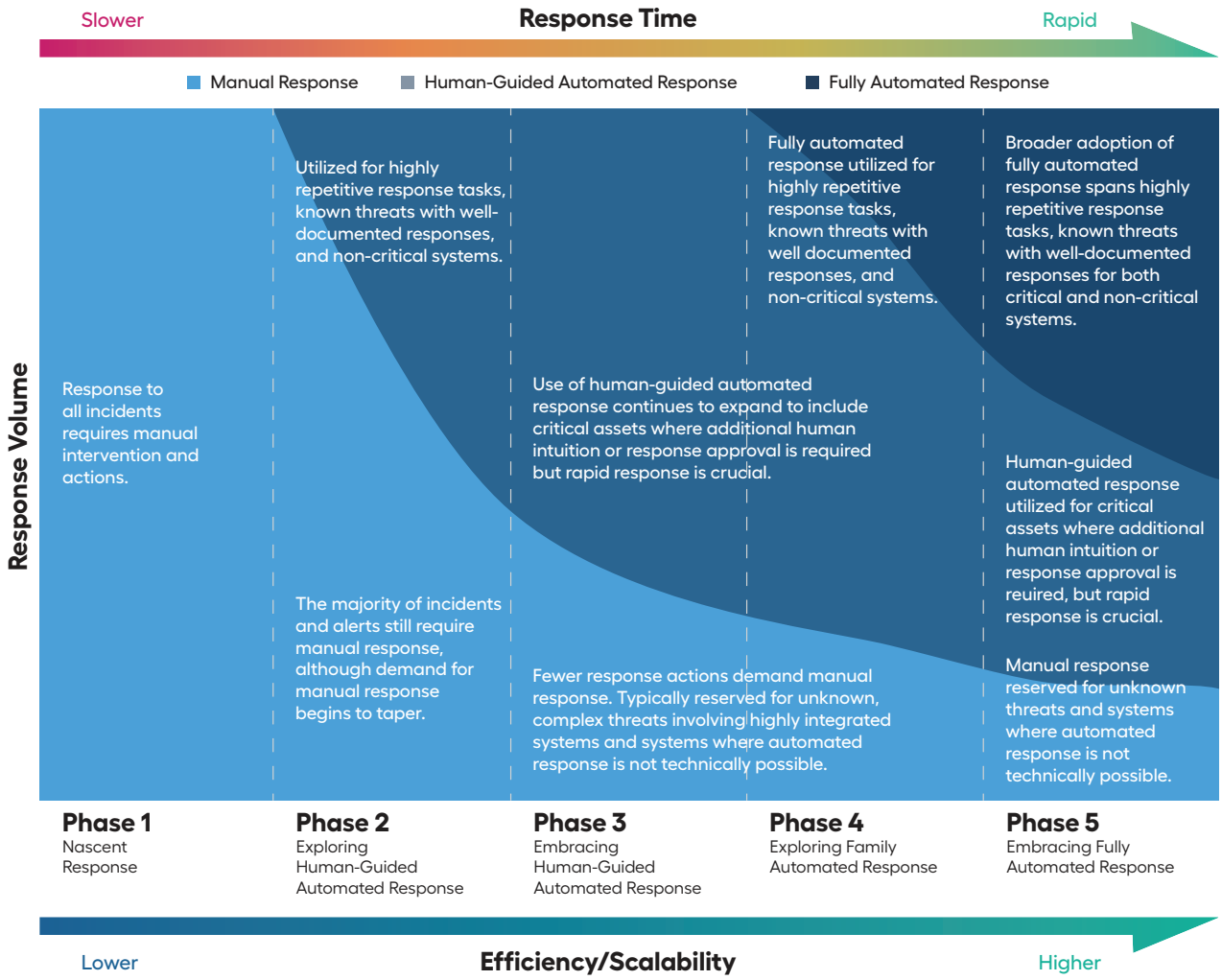

Figure 2: A strategic/phased approach to response

Source: 451 Research

Be Aware! Execution of the plan is as important as strategy and creation. The right partner should be able to help put into practice a self-service experience that enables simple adoption and quick time-to-value.

BEST PRACTICES FOR CRITICAL RESPONSE

1. ***Understand the criticality of your assets and categorize them.*** This is vital for scaling by applying policies to a category. Failure to do so may result in a management headache due to the number of assets spread across your environment.

2. ***Start with notifying appropriate personnel.*** This action carries the least risk of an unintended consequence because it requires human review prior to making a change to the security control. Patterns will emerge, enabling you to identify the types of incidents where you are confident the security control being adjusted will not yield an unintended consequence.

3. ***Add human-guided decision points where intuition is necessary before applying a policy update.*** Set-up the workflow where the security administrator only needs to click approve to execute the policy adjustment on the security control.

4. ***For incidents or assets where speed is of the essence, consider comprehensive automation.*** If predetermined conditions are triggered, the workflow will automatically execute the policy adjustment on the security control and inform security personnel for further forensics and hardening.

KEY CONSIDERATIONS

Implementing automation within your response plan will enhance your defense in depth strategy as it serves as a backstop when prevention tools are evaded. Start slow and increase at a comfortable pace. Also, find a partner that can help you adopt automation, as this is critical to increase your security posture.

> "Real-time alerts can proactively maintain current and accurate awareness. Having Alert Logic handle the detection and response allows our IT team flexibility to help in areas that need constant supervision."

Brett T.

IT Infrastructure Engineer, Alert Logic Customer

G2 Review

Ask Yourself

- Is your security staffing level adequate to handle the cybersecurity challenges you are facing today? In the coming years?
- What are the consequences of a breach on your operations?
- Can you staff a security operations center (SOC) 24/7?
- How do you address different types of incidents?
- Is improving your critical response capabilities a top strategic security objective this year?

RELY ON ALERT LOGIC

Security professionals agree there is no silver bullet in security as no investment will provide a 100% guarantee. Alert Logic MDR® with Alert Logic Intelligent Response™ ensures customers have a flexible, scalable, and integrated approach to protect their entire IT estate. By implementing and testing automated security response playbooks and use cases, Alert Logic customers helped define our new intelligent response capabilities and future innovations.

Alert Logic's cloud-native technology and white-glove team of security experts deliver peace of mind from threats by combining 24/7 SaaS security with visibility, detection, and intelligent response coverage wherever your systems reside. We achieve this through a platform that provides complete coverage of your attack surface and turns data into valuable information, which can be actioned using the right balance of automation and human interaction — vastly improving the security posture of your organization. We ensure you have the most effective response to resolve whatever threats may come.

Founded in 2002, Alert Logic is headquartered in Houston, Texas and has business operations, team members, and channel partners located worldwide. To learn more about how we can help improve the security posture of your organization, please explore Alert Logic's online resources.

UNRIVALED SECURITY FOR YOUR CLOUD JOURNEY.

** Practical Requirements for Responding to Cyberthreats with MDR, 451 Research, S&P Global Market Intelligence, Pathfinder Report, 2021*

*** Source: https://cybersecurityventures.com/cybersecurity-jobs-report-2019/*

**** Source: https://go.451research.com/2020-mi-access-to-talent-driving-managed-service-opportunity.html*