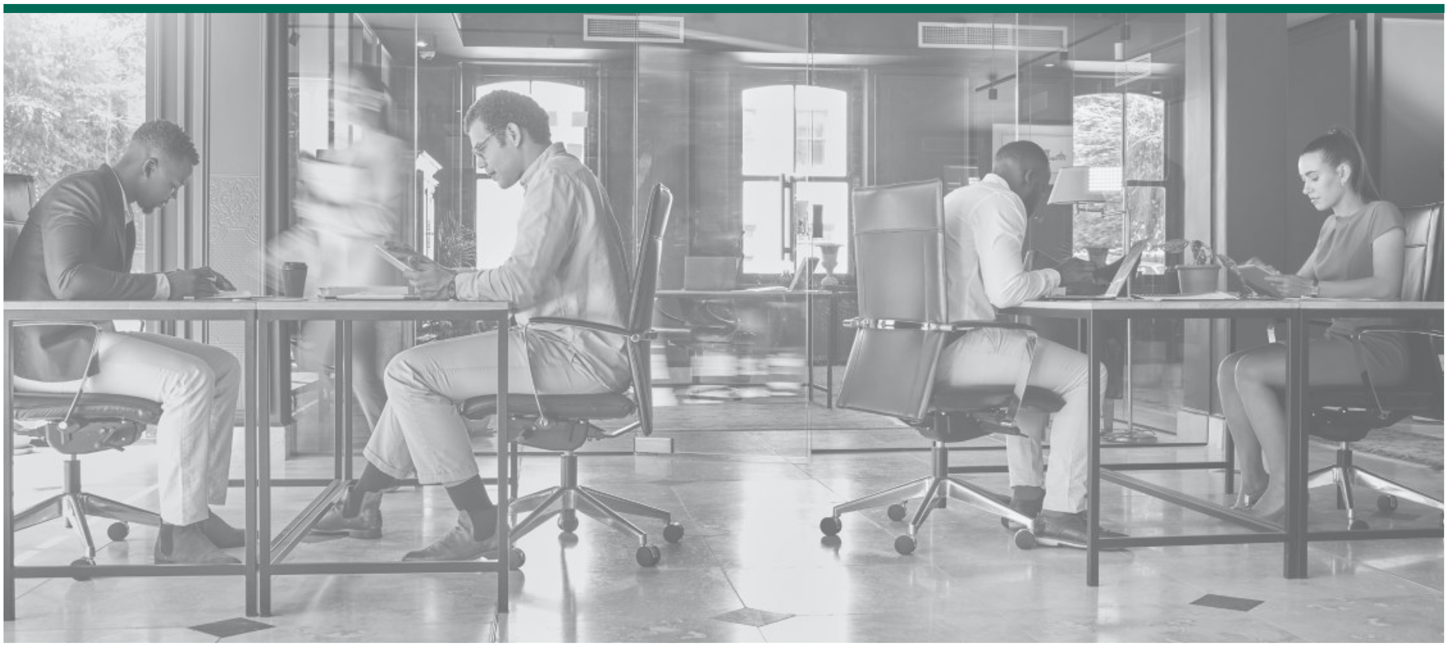
FORTRA

GUIDE

Enhancing Your Response Capabilities



Getting Started

Organizations that launch a response initiative without a properly defined strategy typically have one of two results:

- Rely on a single tool capable of detection and response
- Purchase a SOAR tool without the people or processes in place to take advantage of its full capabilities

Both of these outcomes usually result in poor return on investment. A better option is adopting a more comprehensive plan, such as our seven key pillars for effective response, that addresses people, process, and tools (see 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.

As you evolve your cybersecurity strategy, ensure you have a strong, comprehensive response plan built on a solid foundation. This guide, created for security professionals, explores the processes, challenges, and best practices of implementing automation into your response strategy.

7 Key Pillars for Effective Response

1. Detection Strength: 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 then can 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 also are necessary during forensics to complete the picture of an attack.

2. Broad Response Coverage: Discover ingress and egress points.

An organization's IT estate is dynamic, but the constants always will 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, network edge, and cloud service provider.

3. Risk Profile: Consider the value of an asset and type of attack.

A revenue-generating asset, such as an e-commerce 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 provided in an actionable way, including analytics content and configuration requirements. 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.

4. User Experience: Your solution should allow for configurable response workflows.

This solution 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 nor want everything automated as this can have adverse effects. The ideal scenario is to automate actions based on circumstances such as an 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.

> **“ 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*

5. Actions Taken: Recognize that effective response is often a blend of multiple actions.

Prioritization changes based on variables such as incident type, asset criticality, and desired outcomes. The blend should consist of:

- **Notification** — Inform appropriate responders of the security incident with sufficient detail to allow for decision-making.
- **Containment** — Limit access of the compromised entity, which may include 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. Steps may include revising a policy or change control, updating a misconfigured service, or applying patches to affected systems.

6. Use Cases: Every organization is at a different stage in their automation journey.

Your ability to incorporate human interaction for response actions allows adoption at a pace that is comfortable for you. Review the following scenarios that include both 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 either could be an early warning to a potential insider threat or be nothing. The anomalous activity triggers a playbook which sends a push notification to the IT admin and their supervisor on their mobile devices. They have the choice of disabling the user credentials on Active Directory or investigating further by opening a ServiceNow ticket.

- **Privilege Access Management Anomaly:** The privileged credentials of a senior executive are 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 privileged credentials are restricted, a push notification is sent to the security administrator, and a message is distributed via Slack to the security team to verify legitimacy of the activity.

- **Complex Indicators of Compromise:** A healthcare clinic's patient admitting system 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, multiple actions are 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: Carefully consider appropriate communications.

For your response strategy to be effective, communicating the action you are taking to stakeholders who need to be informed or provide additional forensic detail as part of the process is key. Users should be notified with collaboration tools such as Slack, Teams or email, or advanced ticketing systems like Jira and ServiceNow. Integrating your response strategy into these collaboration and ticketing platforms enables effective and efficient dissemination of critical information.

Once the seven pillars of effective response have been addressed, implementation and execution of your plan can begin. It is essential that the plan be carefully crafted, easily iterated, and improved as needed.

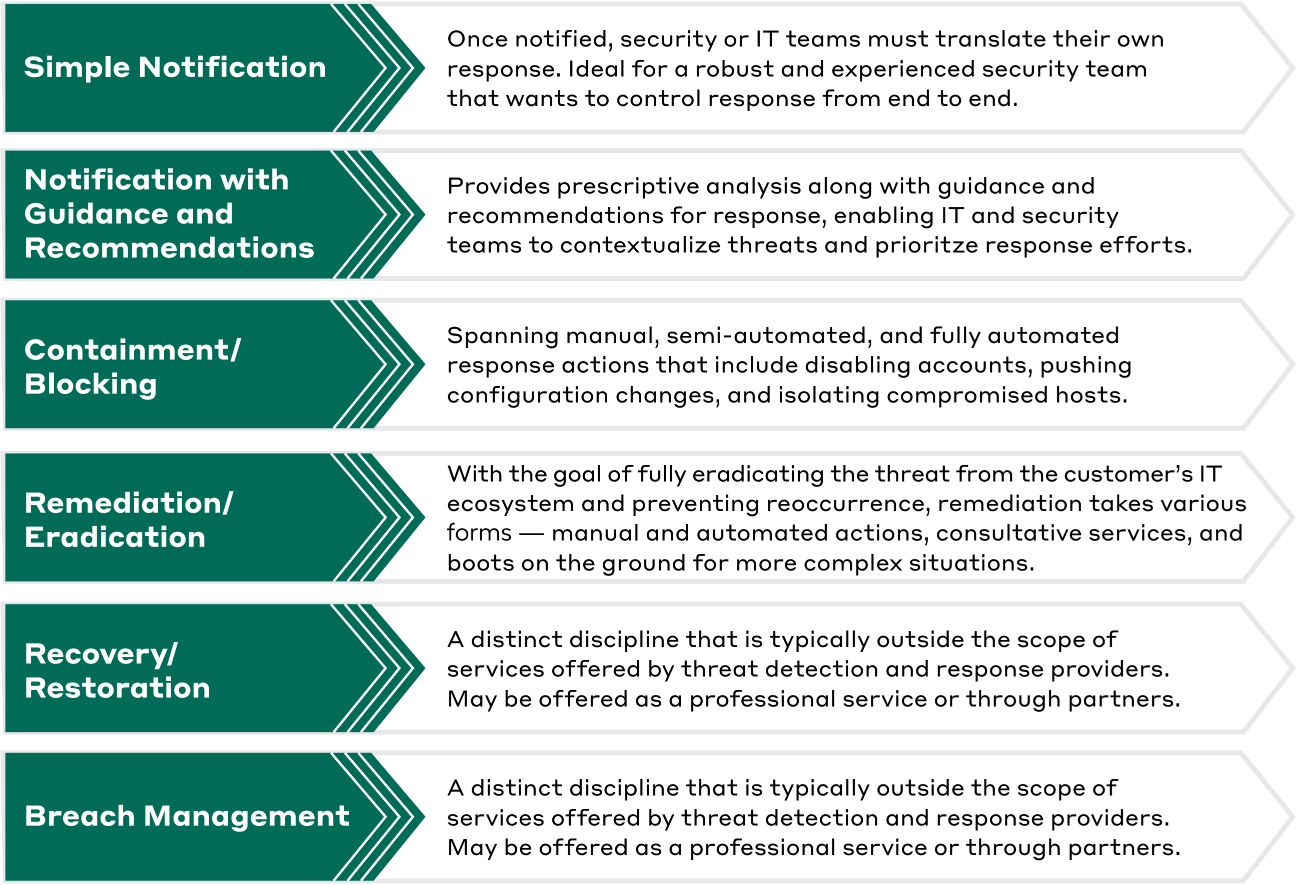
More sophisticated organizations should have the ability to design playbooks with the flexibility to create decision trees with multiple conditions and actions.

Challenges of Effective Response

People: There are more than 3 million unfilled security jobs** making it extremely challenging to find and keep skilled security professionals. Additionally, 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's common for mid-sized 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 each tool. There also are unintended misconfigurations that either are 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

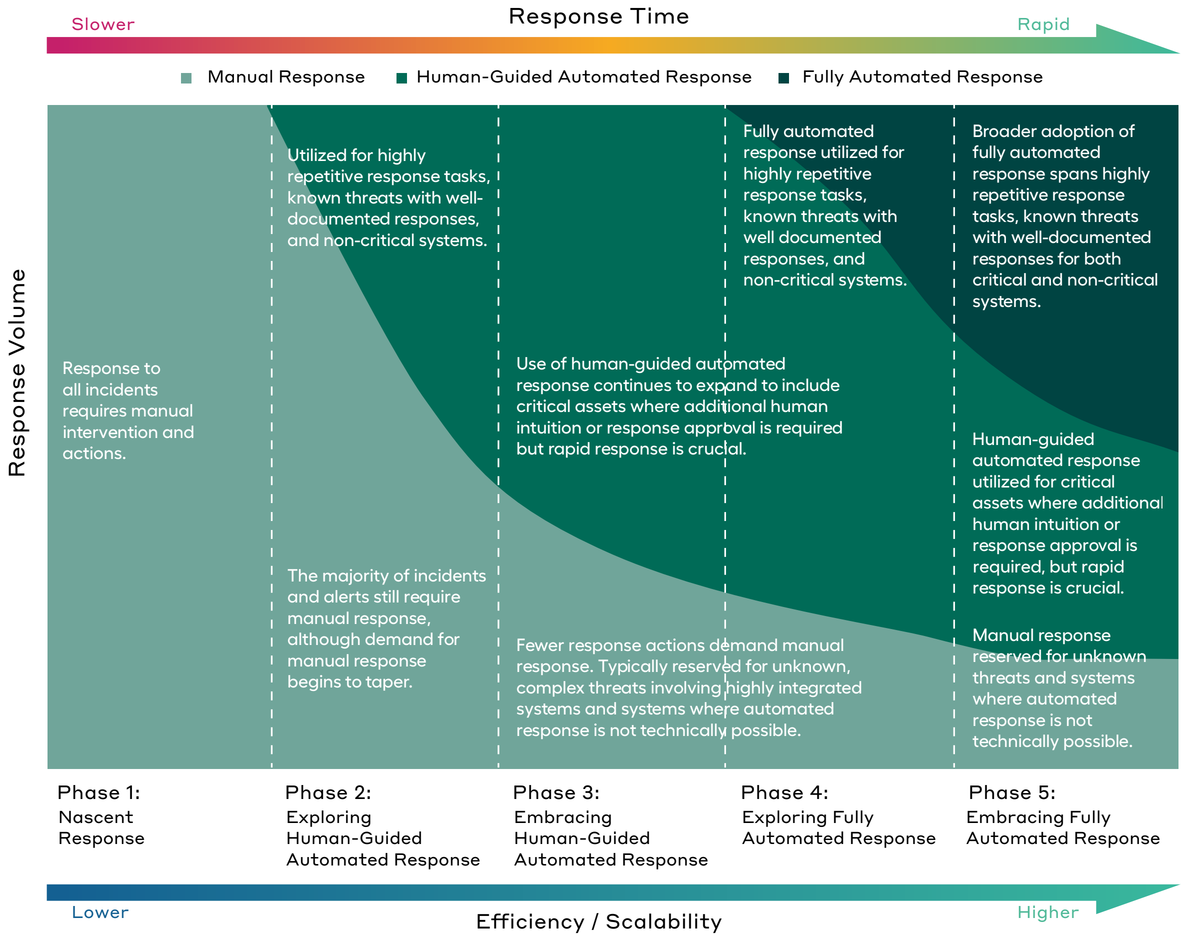
4 Best Practices for Critical Response

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 review by a person 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. Consider comprehensive automation for incidents or assets where speed is of the essence. If predetermined conditions are triggered, the workflow automatically will execute the policy adjustment on the security control and inform security personnel for further forensics and hardening.



Key Considerations

Implementing automation in your response plan will enhance your defense strategy as it serves as a backstop when prevention tools are evaded. Start slow and increase at a pace that is comfortable for you. Find a partner that can help you adopt and implement automation into your response strategy.

> **“ 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*

Security professionals agree there is no silver bullet in security as no investment will provide a 100% guarantee. Fortra's 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, our customers helped define our intelligent response capabilities and future innovations.

Our 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.

For more information, please visit **alertlogic.com**

**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.451reasearch.com/2020-mi-access-to-talent-driving-managed-service-opportunity.html*

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We’ve created a simpler, stronger, and more straightforward future for our customers. Our trusted experts and best-in-class portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We’re the positive changemakers and your relentless ally for cybersecurity that prevails. Learn more at fortra.com.