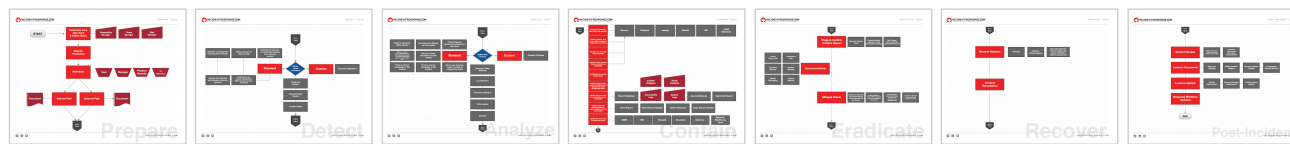


## Automate Response

Congratulations on selecting [IncidentResponse.com](http://IncidentResponse.com) to retrieve your custom incident response playbook guide. This guide has been created especially for you for use in within your security response team. We hope you find it valuable and ask that you share it with the rest of your organization so you can collectively be successful in managing incidents and reducing risk throughout the business.

### Your playbook overview - “Elevation of Privilege”



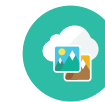
### Incident Response: A Top Priority in Security Management Programs

In the April 2014, U.S. Government Accountability Office reported (GAO-14-354) it's noted that “major federal agencies did not consistently demonstrate that they are effectively responding to cyber incidents (a security breach of a computerized system and information).” The GAO projects that these agencies did not completely document actions taken in response to detected incidents. While the agencies identified the scope of an incident, they frequently did not demonstrate that they had determined the impact of an incident, nor did they consistently demonstrate how they had handled other key activities, such as whether preventive actions to prevent the reoccurrence of an incident were taken. The GAO notes, “without complete policies, plans, and procedures, along with appropriate oversight of response activities, agencies face reduced assurance that they can effectively respond to cyber incidents.”<sup>3</sup>

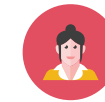
### Did you know?



In **2014**, incidents **increased by 78% since 2013.**<sup>1</sup>



**1,023,108,627** records were breached in **2014.**<sup>1</sup>



**54%** of the breaches consisted of **Identity Theft.**<sup>1</sup>



**\$3.5 million** is the **average cost of a breach** for a company.<sup>2</sup>



Companies experience an average of **10 unauthorized access incidents per month.**<sup>2</sup>



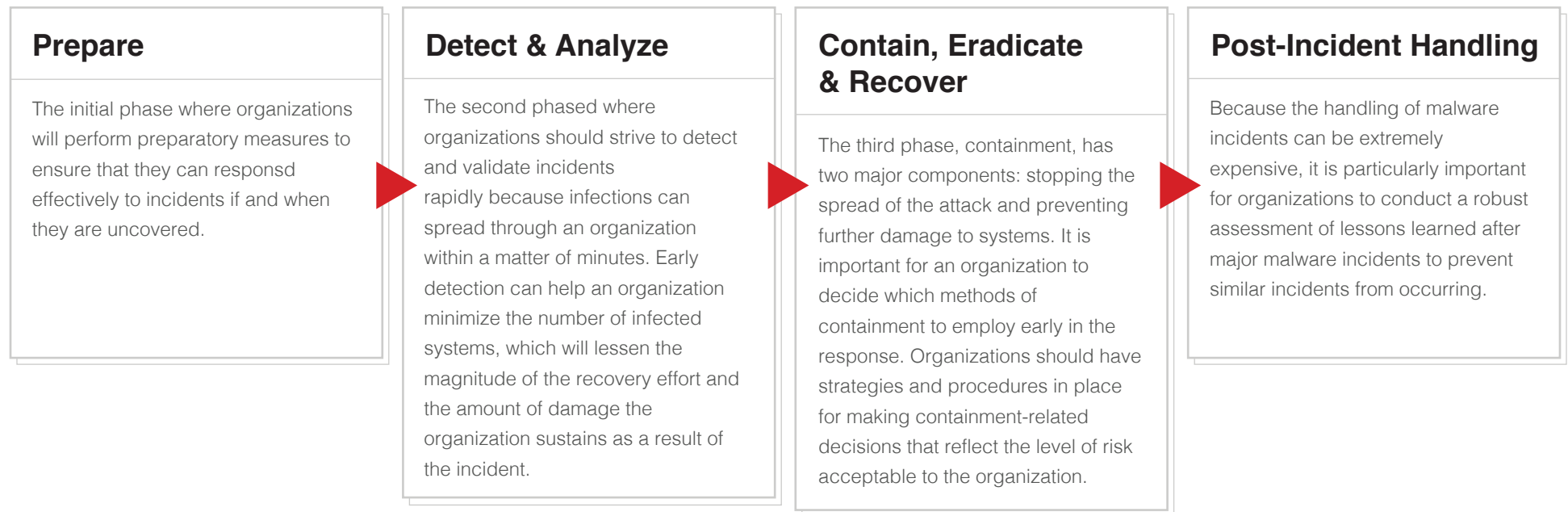
**Malicious insiders and criminal attacks** are the top causes for breaches.<sup>2</sup>

1. **Source:** Gemalto - Breach Level Index

2. **Source:** Ponemon 2014 Cost of a Data Breach

3. **Source:** GAO-14-354, p.2

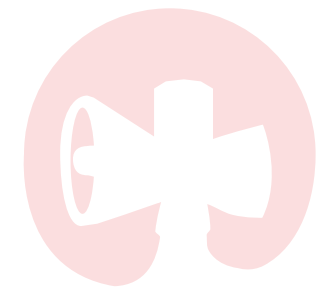
**What is an incident response playbook?** According to NIST Special Publication 800-61, an incident response process contains four main phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. Descriptions for each are included below:

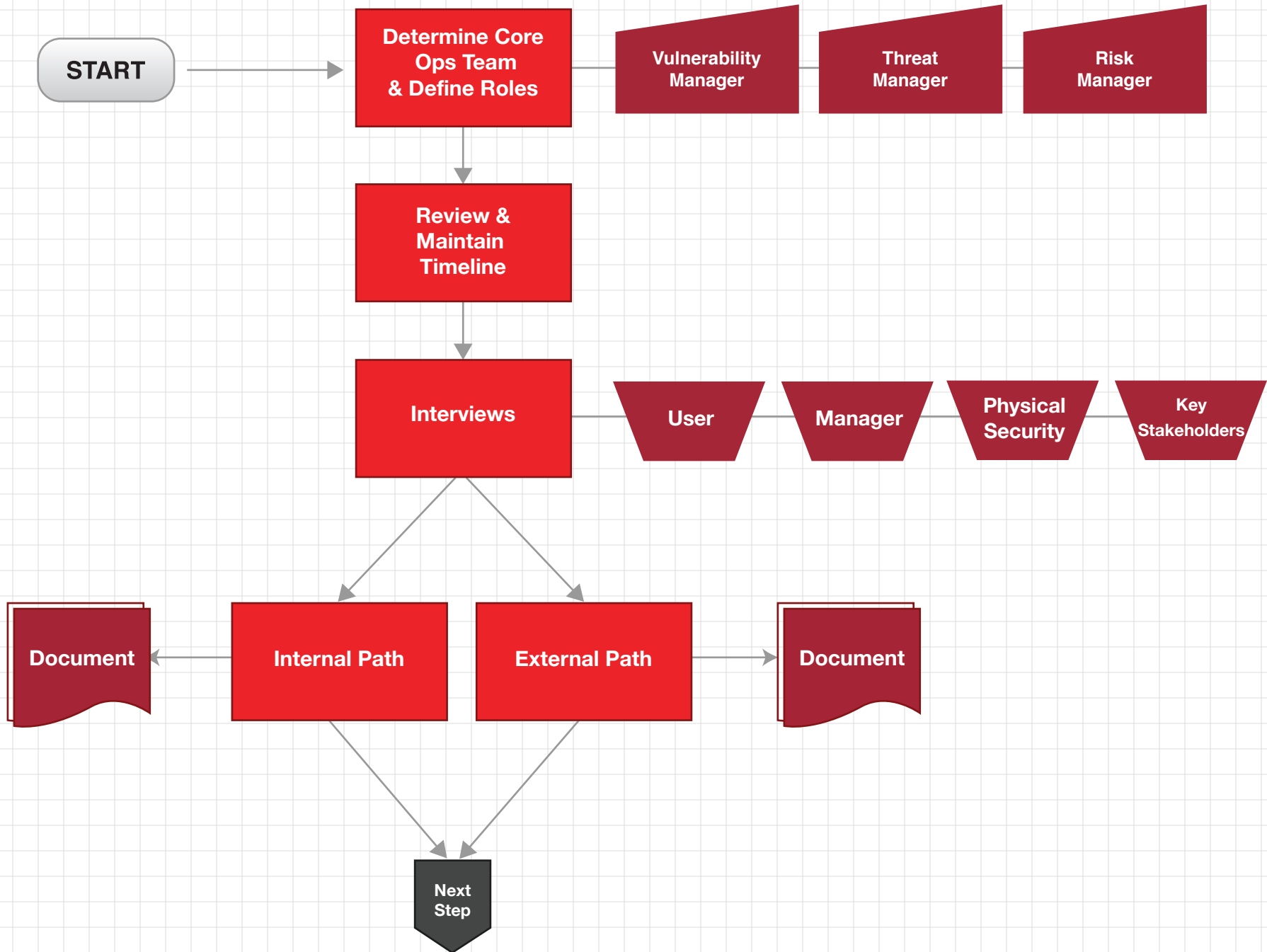


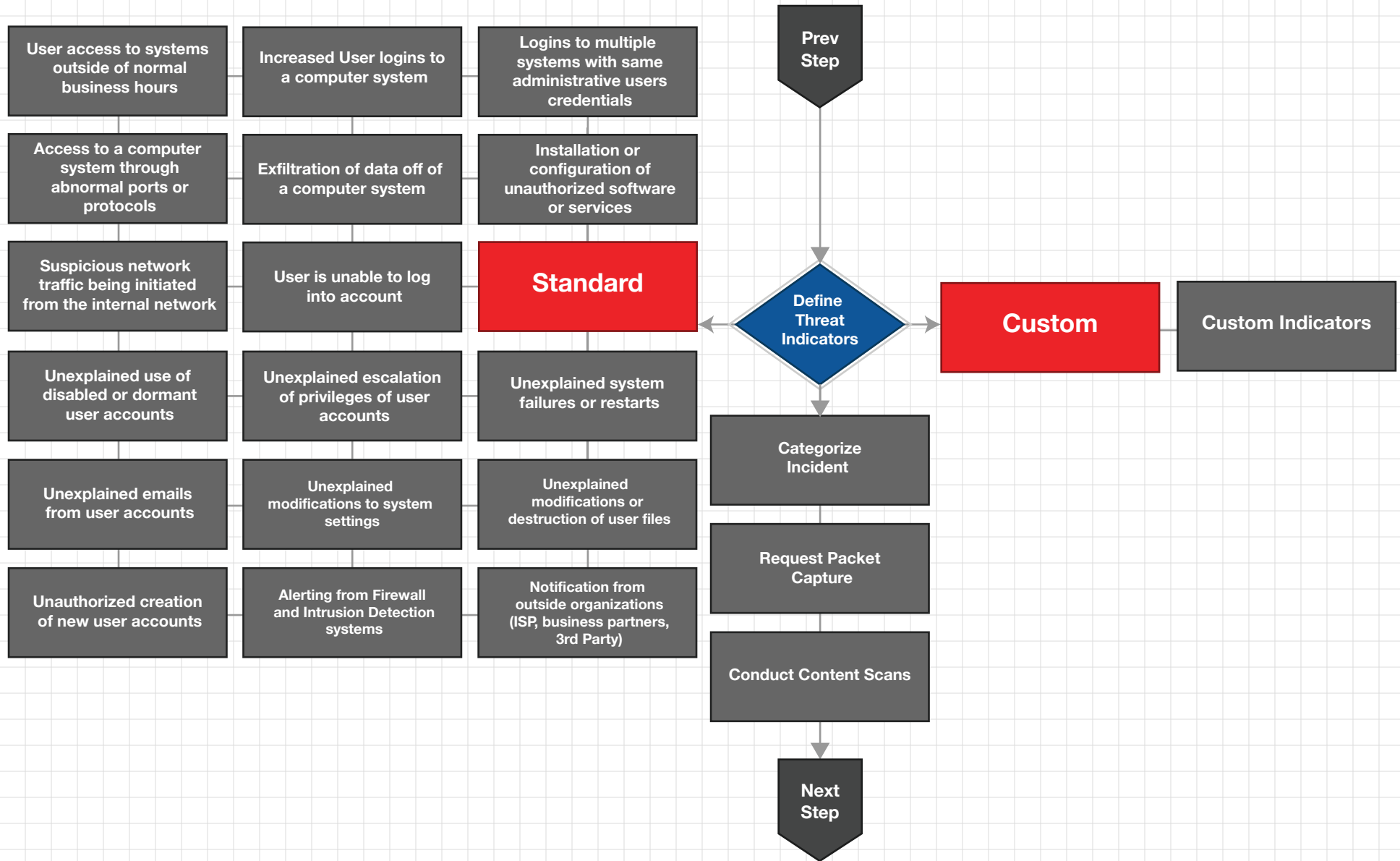
## User Access

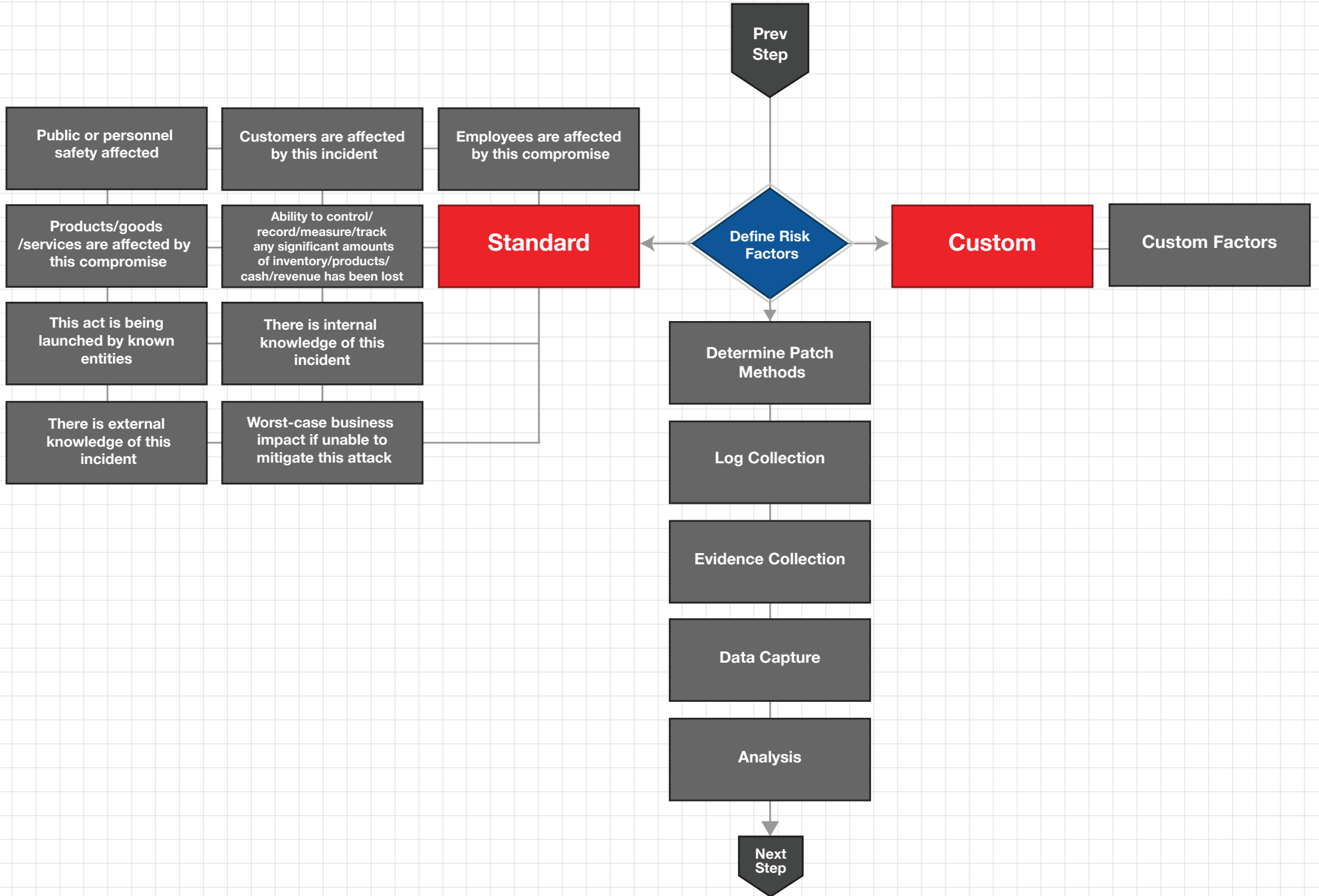
You've selected the "**Elevation Of Privilege**" playbook. On the pages that follow, you will find your incident response playbook details broken down by the NIST incident handling categories.

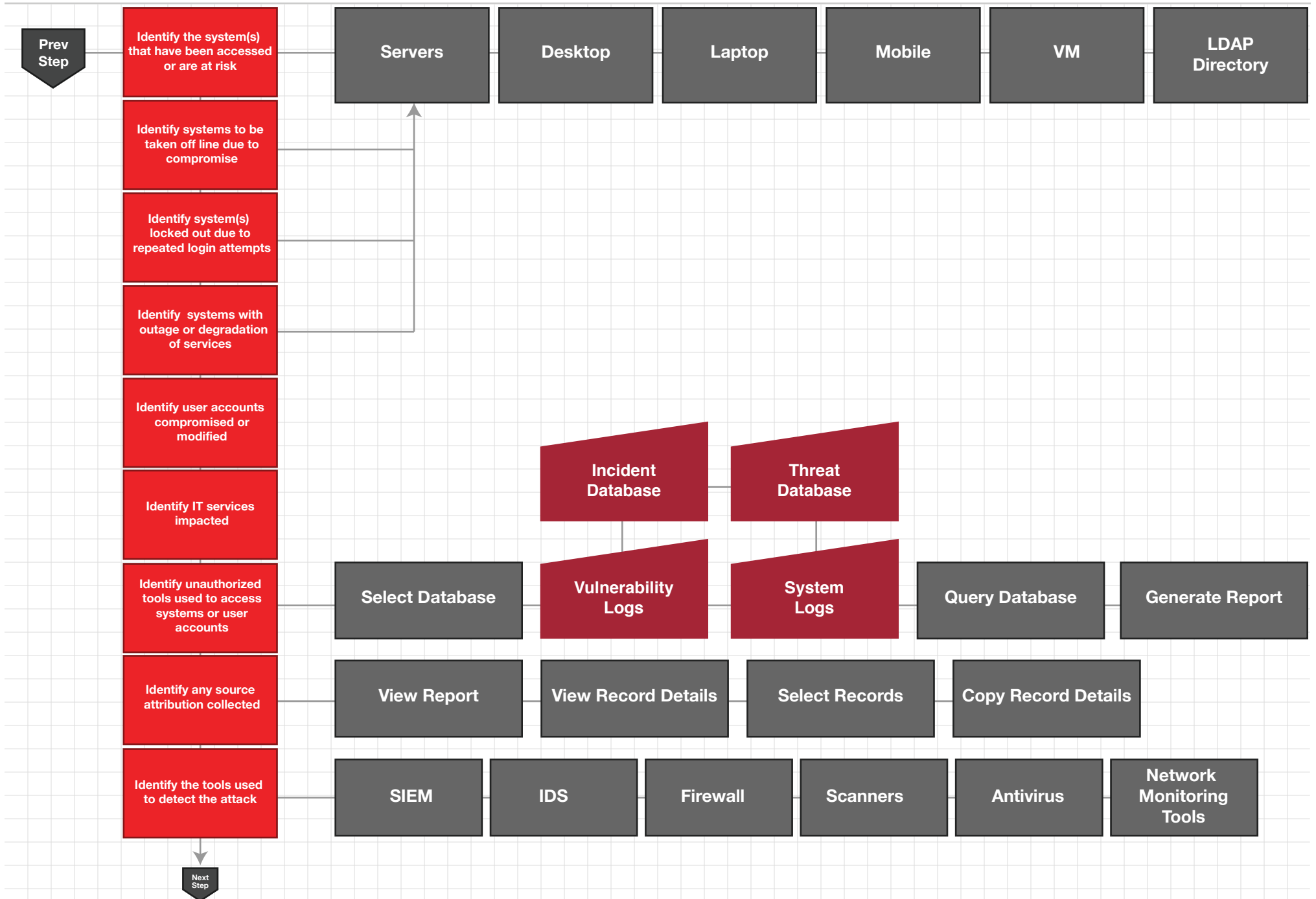
To view your playbook online, visit <https://incidentresponse.com/playbooks/elevation-of-privilege>

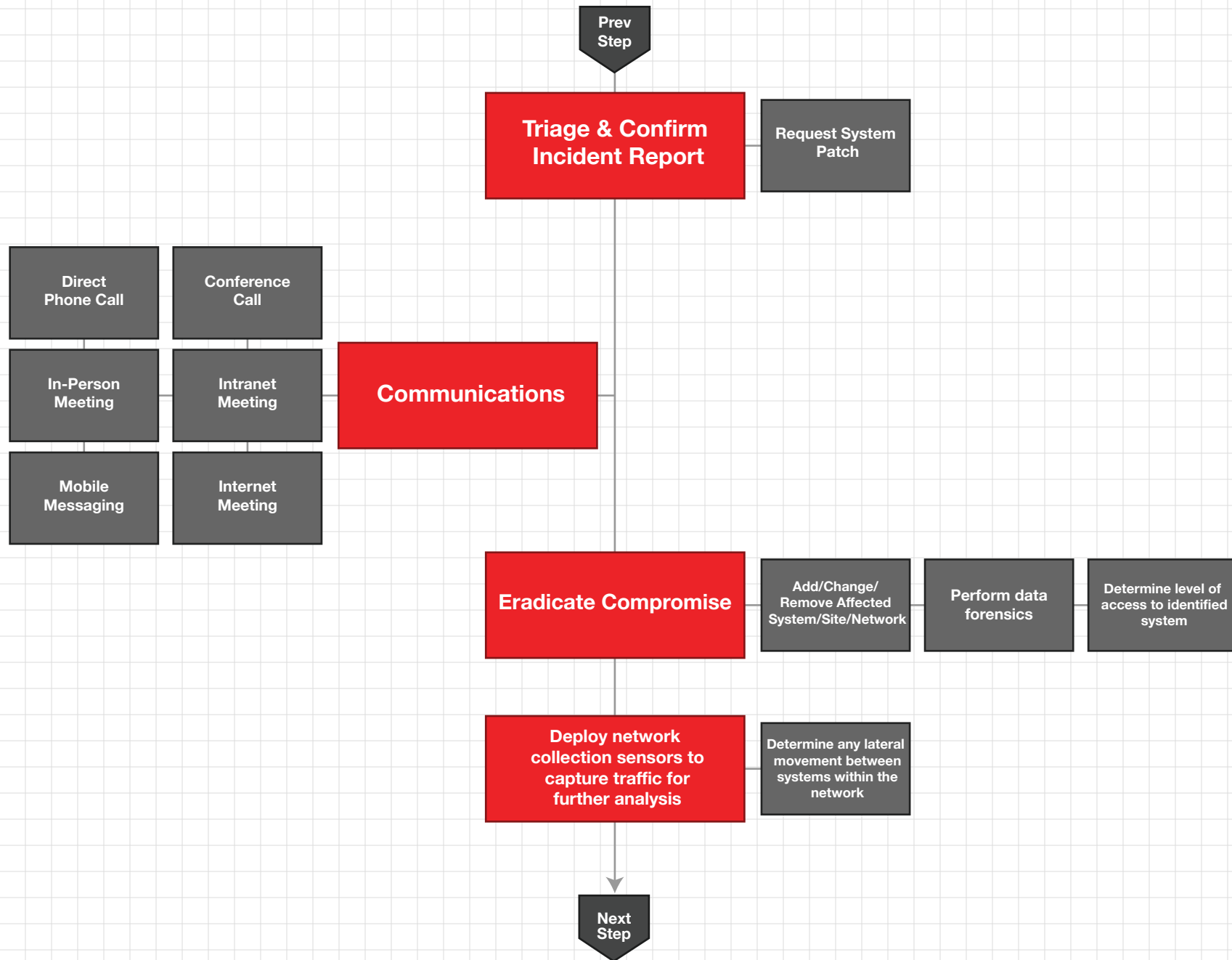


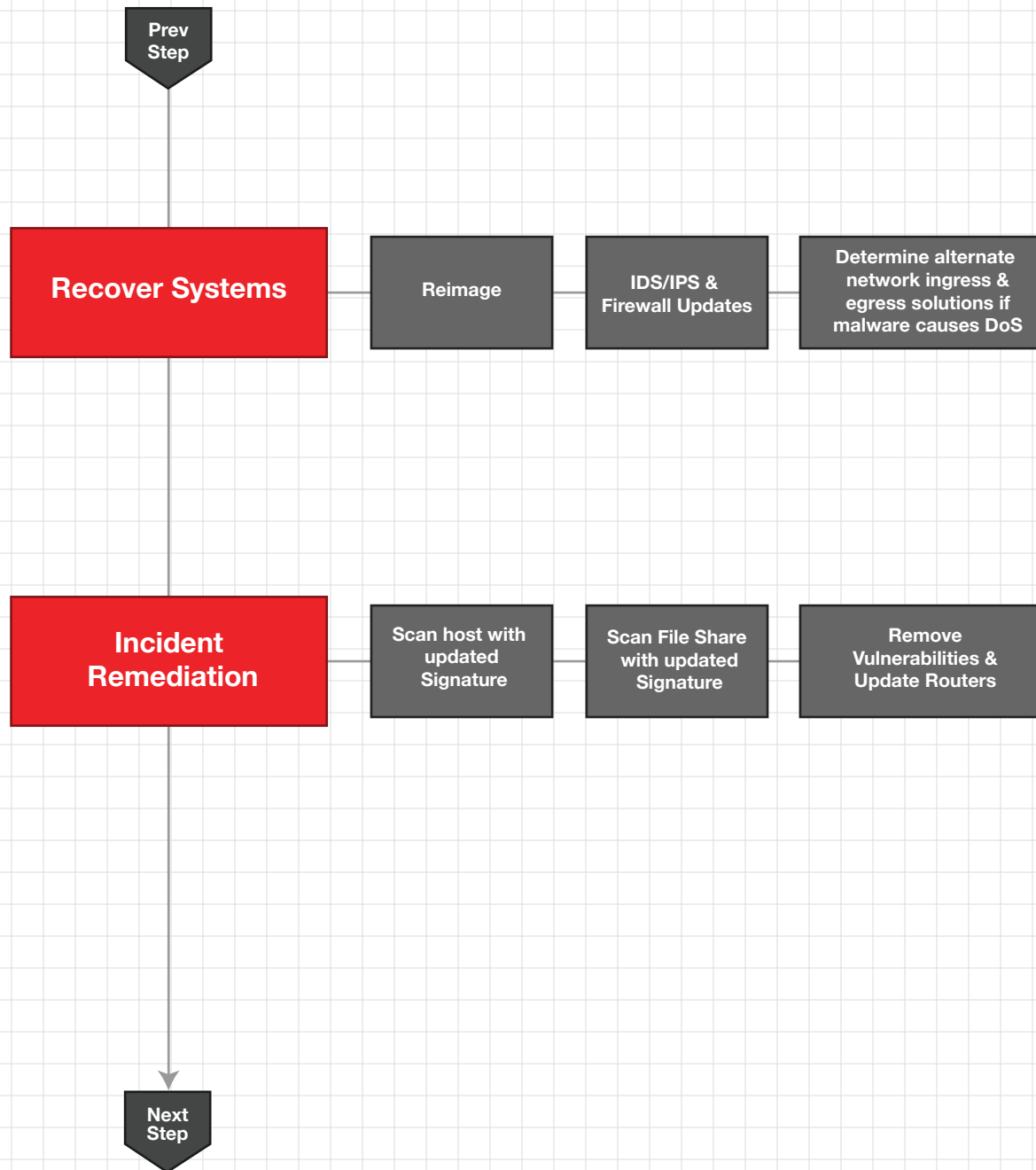




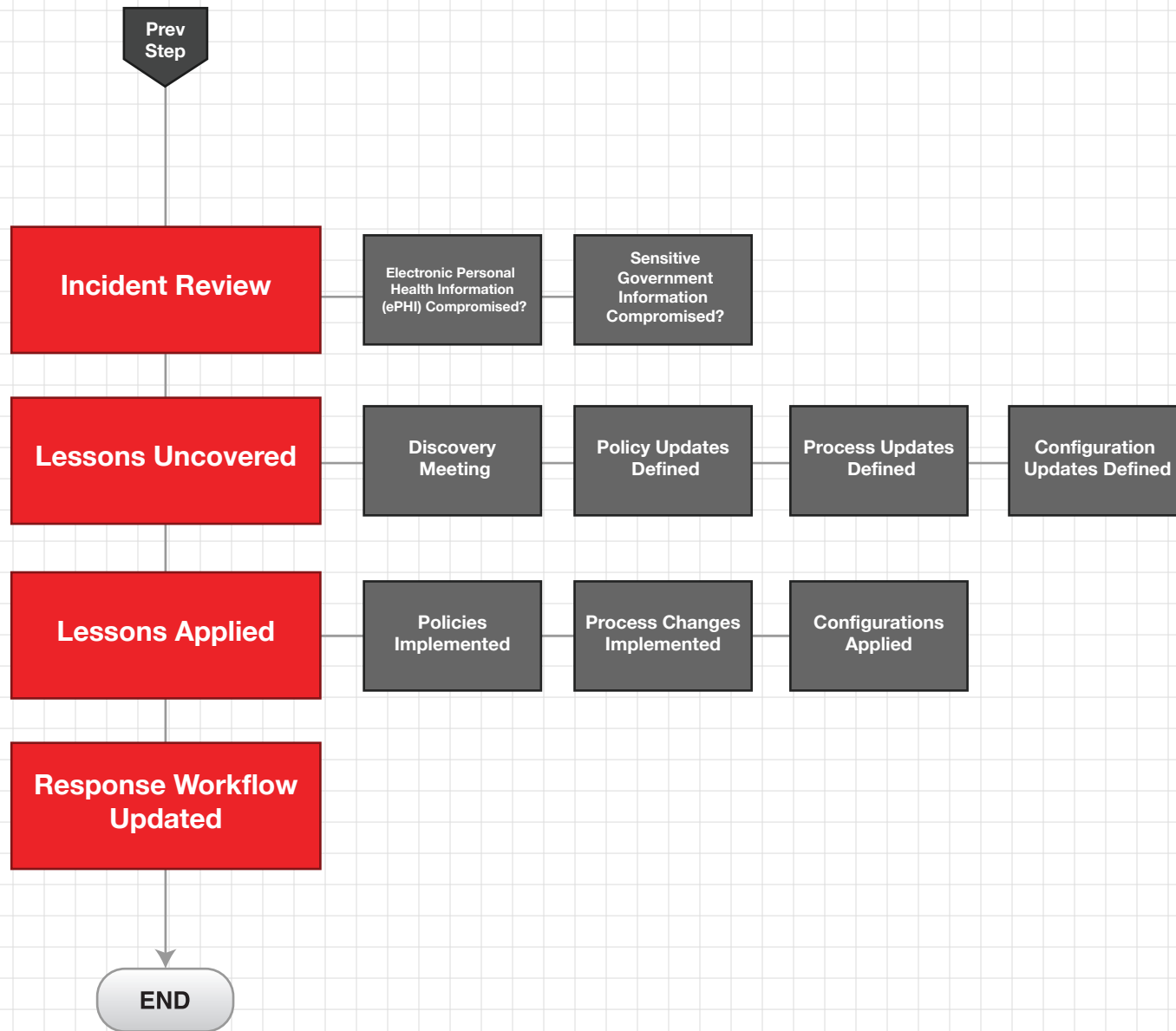












## Proactive Response

An automated playbook helps security teams optimize for efficiency and productivity. Your security team has the ability to analyze, detect and prioritize when all pertinent data and multiple security tools are integrated into one system. With one-screen visibility you can identify anomalies, assign tasks, access reporting and communicate across multiple departments effectively for quick responses.

## Quick Containment

Time and speed are crucial in assessing the environment and risk in the context of your business. Playbooks give a complete view of the necessary tasks to capture the data needed to support proper recovery and forensics. The efficiency a playbook brings to a security team allows for quick responses to finding the source of the attack, following lateral movement across the organization and taking the proper steps mitigate damage.

## Effective Remediation

Organization and automation are key benefits that result in effective remediation. Automated playbooks help to organize security processes, mitigation plans and smooth communication between multiple departments. By optimizing data collection, analysis, and communications you improve the odds for effective eradication, recovery with integrity and forensic-quality reporting.

---

## Action Plan

Having a view into what is possible is the first step in taking action. The next step is to bring your team together to drive it toward reality. Email this guide to your peers and managers to begin sharing your playbook with them.

With this playbook, you will be better prepared to handle the response. To help with the management and automation of this incident response playbook, consider working with CyberSponse and their partners. Come take a look at [\*\*what they do\*\*](#).

For additional incident response playbook examples, visit <https://www.incidentresponse.com/playbooks>

## Security Management Benefits

- Be prepared to handle any incident your team faces
- Control the situation, minimizing the impact to the business
- Efficiently manage your response across multiple departments

### Useful Links:

[NIST Incident Handling Guide](#)

[SANS Incident Handler's Handbook](#)

## Risk Management Benefits

- Communicate effectively to ensure risk mitigation methods are applied
- Prioritize resources and activities where they matter most
- Report and tune based on response learning, reducing risk moving forward

### Useful Links:

[NIST Risk Management Framework Guide](#)

[Sample Policies and Plans](#)