Automate Response

Congratulations on selecting **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 - "Root Access"

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." [3]

Did you know?

In **2014**, incidents **increased by 78% since 2013.**[1]

1,023,108,627 records were breached in **2014**.[1]

54% of the breaches consisted of **Identity Theft**.[1]

$3.5 million is the **average cost of a breach** for a company.[2]

Companies experience an average of **10 unauthorized access incidents per month.**[2]

Malicious insiders and **criminal attacks** are the top causes for breaches.[2]

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/reocvery, and post-incident activity. Descriptions for each are included below:

Prepare

The initial phase where organizations will perform preparatory measures to ensure that they can responsd effectively to incidents if and when they are uncovered.

Detect & Analyze

The second phased where organizations should strive to detect and validate incidents rapidly because infections can spread through an organization within a matter of minutes. Early detection can help an organization minimize the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organization sustains as a result of the incident.

Contain, Eradicate & Recover

The third phase, containment, has two major components: stopping the spread of the attack and preventing further damage to systems. It is important for an organization to decide which methods of containment to employ early in the response. Organizations should have strategies and procedures in place for making containment-related decisions that reflect the level of risk acceptable to the organization.

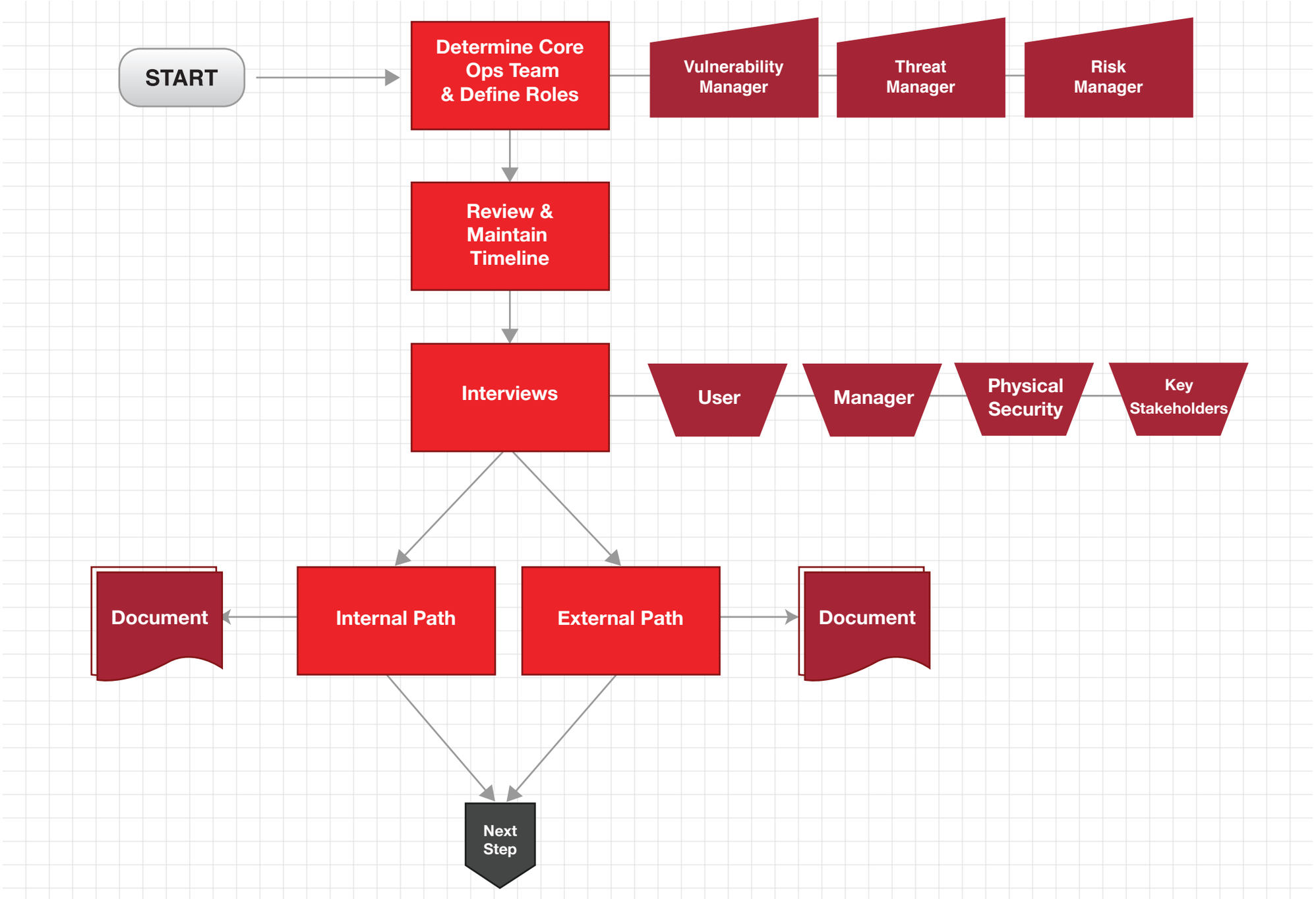
Post-Incident Handling

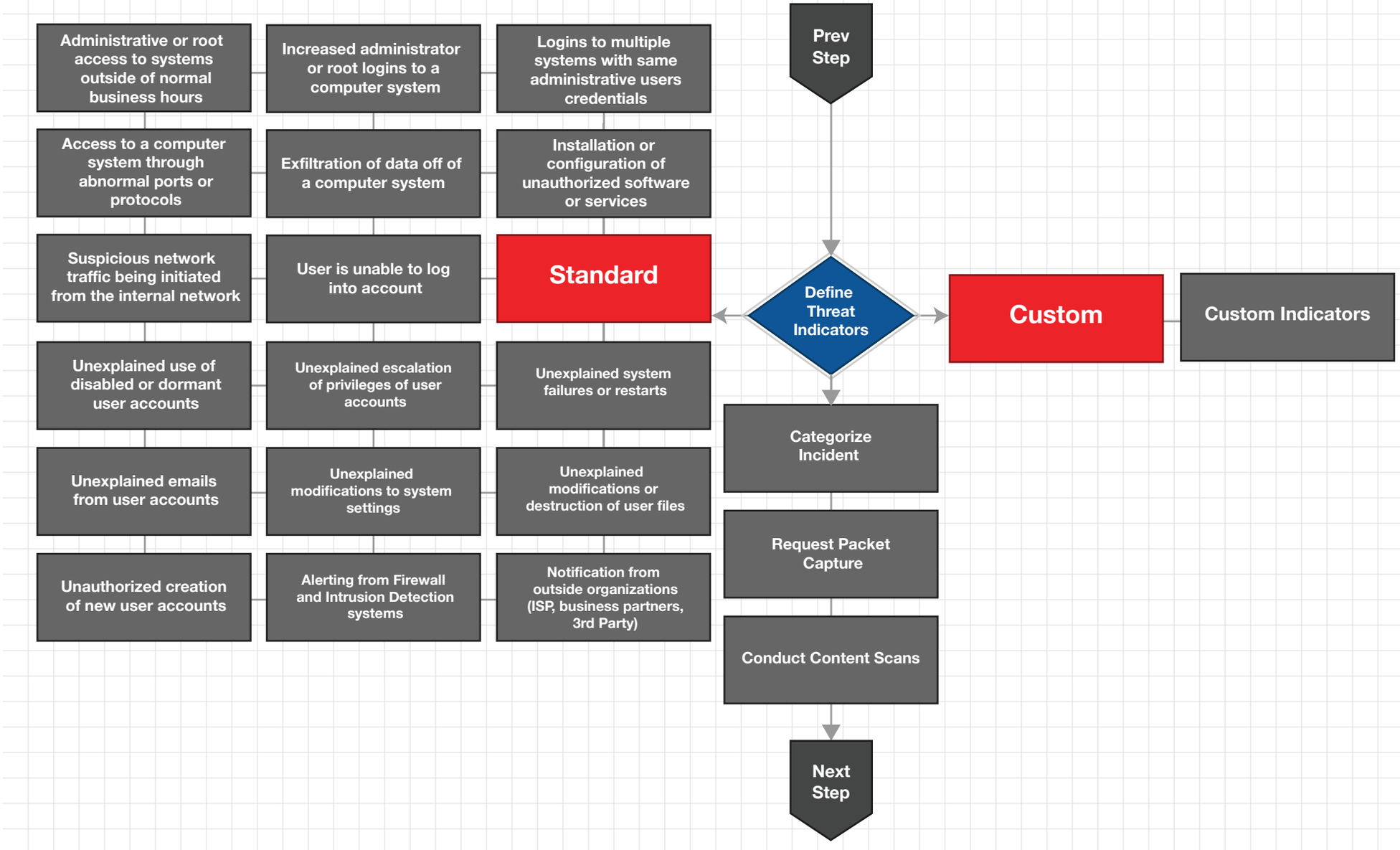
Because the handling of malware incidents can be extremely expensive, it is particularly important for organizations to conduct a robust assessment of lessons learned after major malware incidents to prevent similar incidents from occurring.

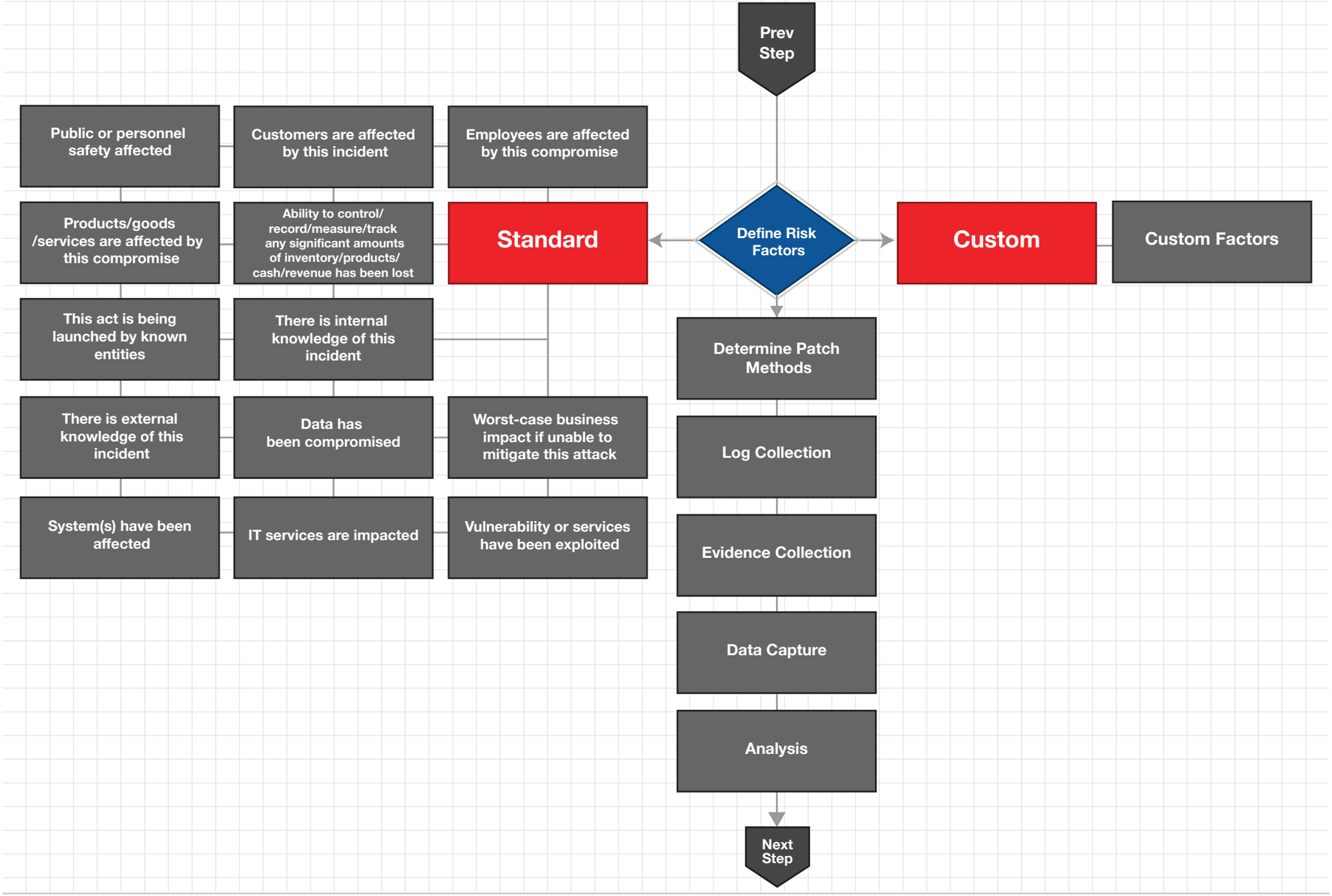
Root Access

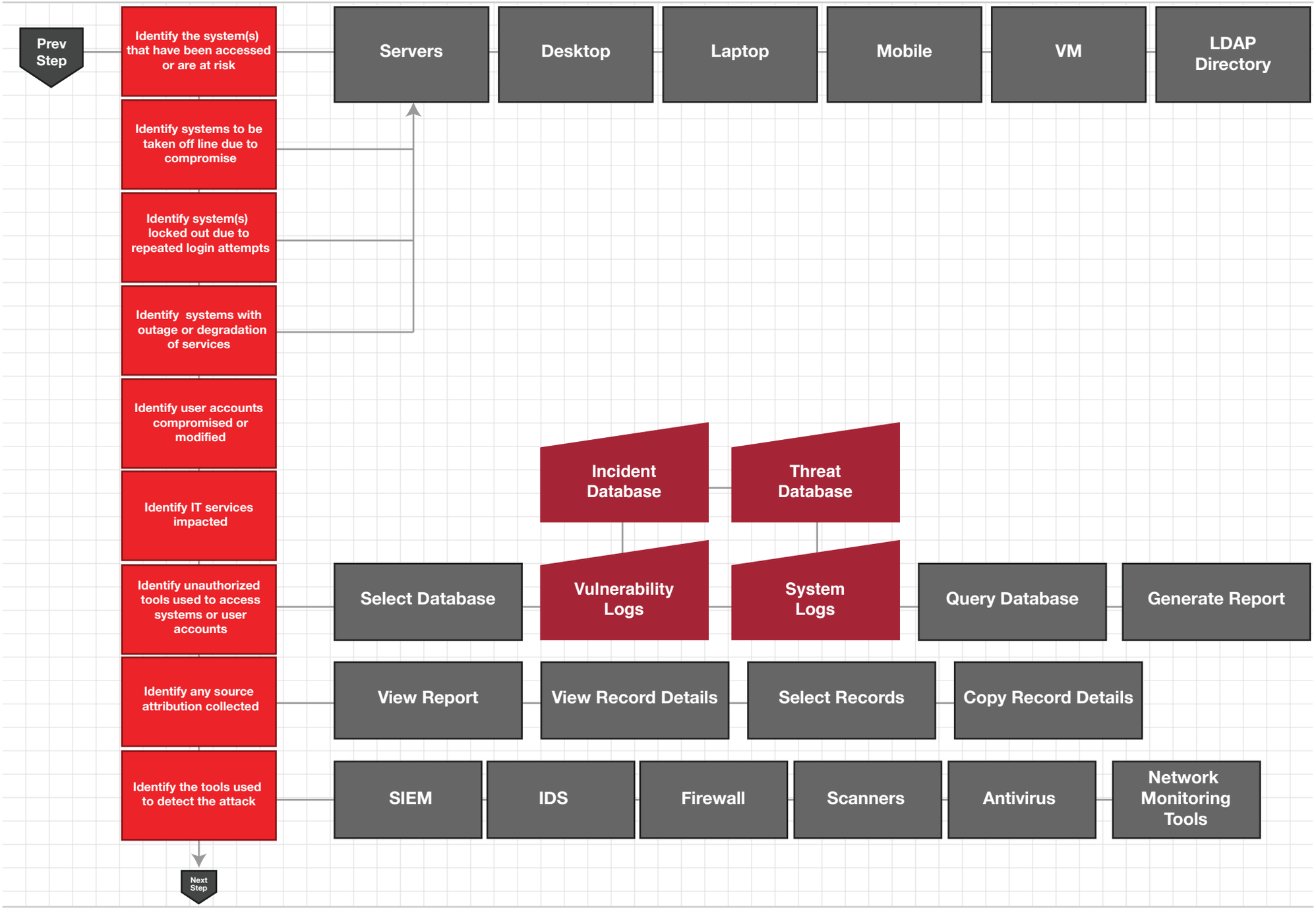
You've selected the "**Root Access**" playbook. On the pages that follow, you will find your incident response playbook details broken down by the NIST incident handling categories.

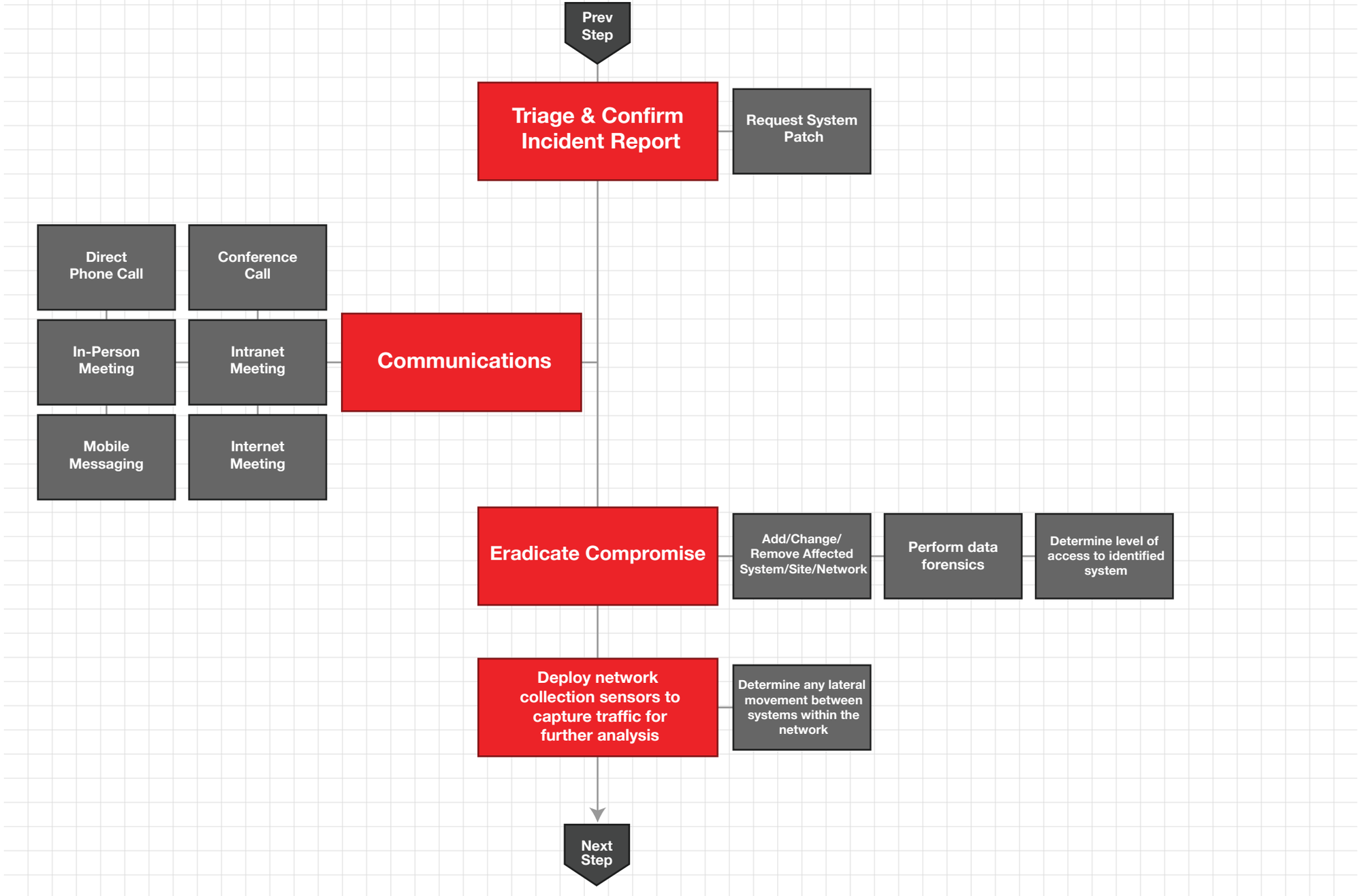
To view your playbook online, visit **https://incidentresponse.com/playbooks/root-access**

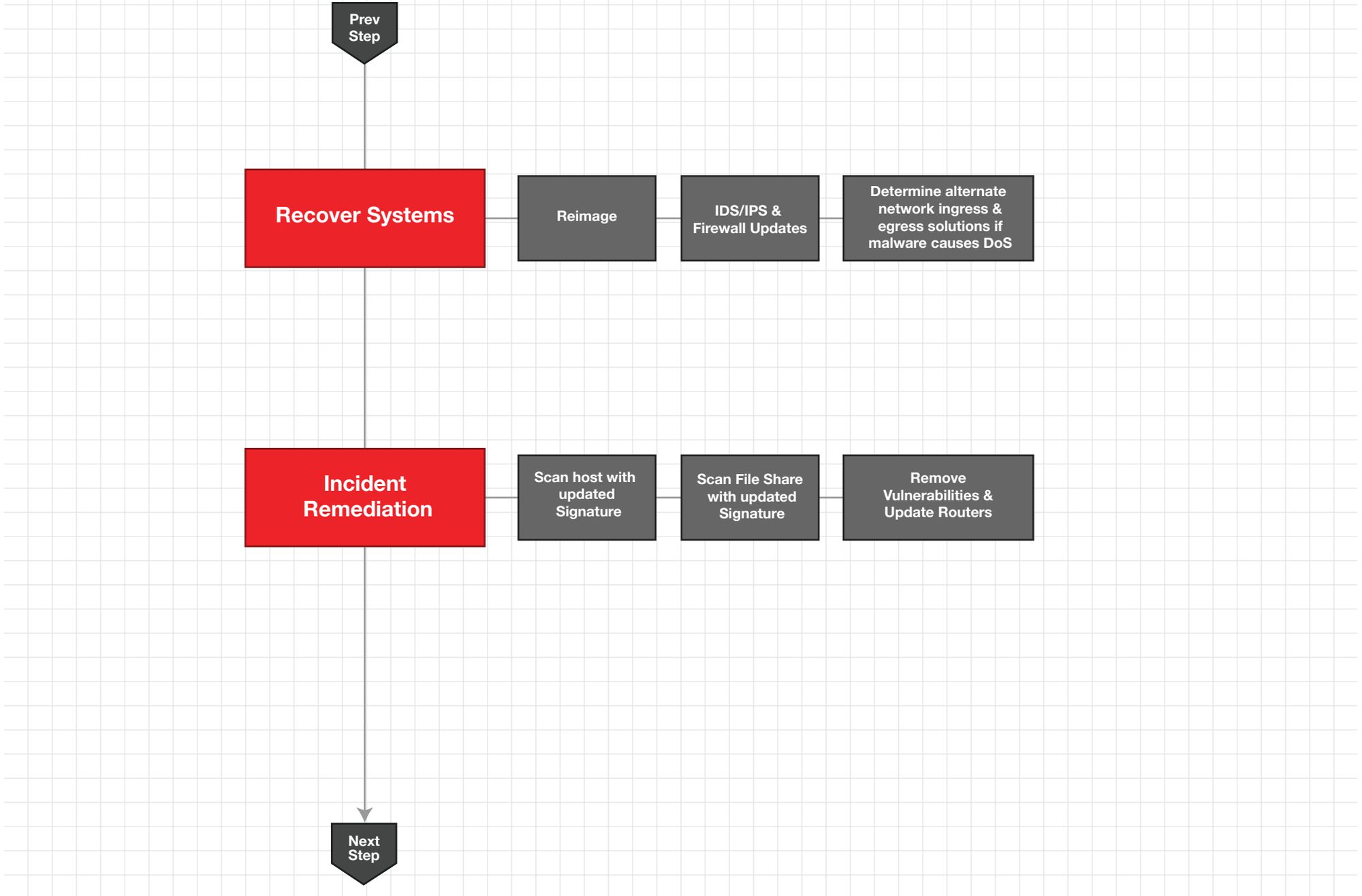

START
Determine Core Ops Team & Define Roles
Vulnerability Manager
Threat Manager
Risk Manager
Review & Maintain Timeline
Interviews
User
Manager
Physical Security
Key Stakeholders
Document
Internal Path
External Path
Document
Next Step

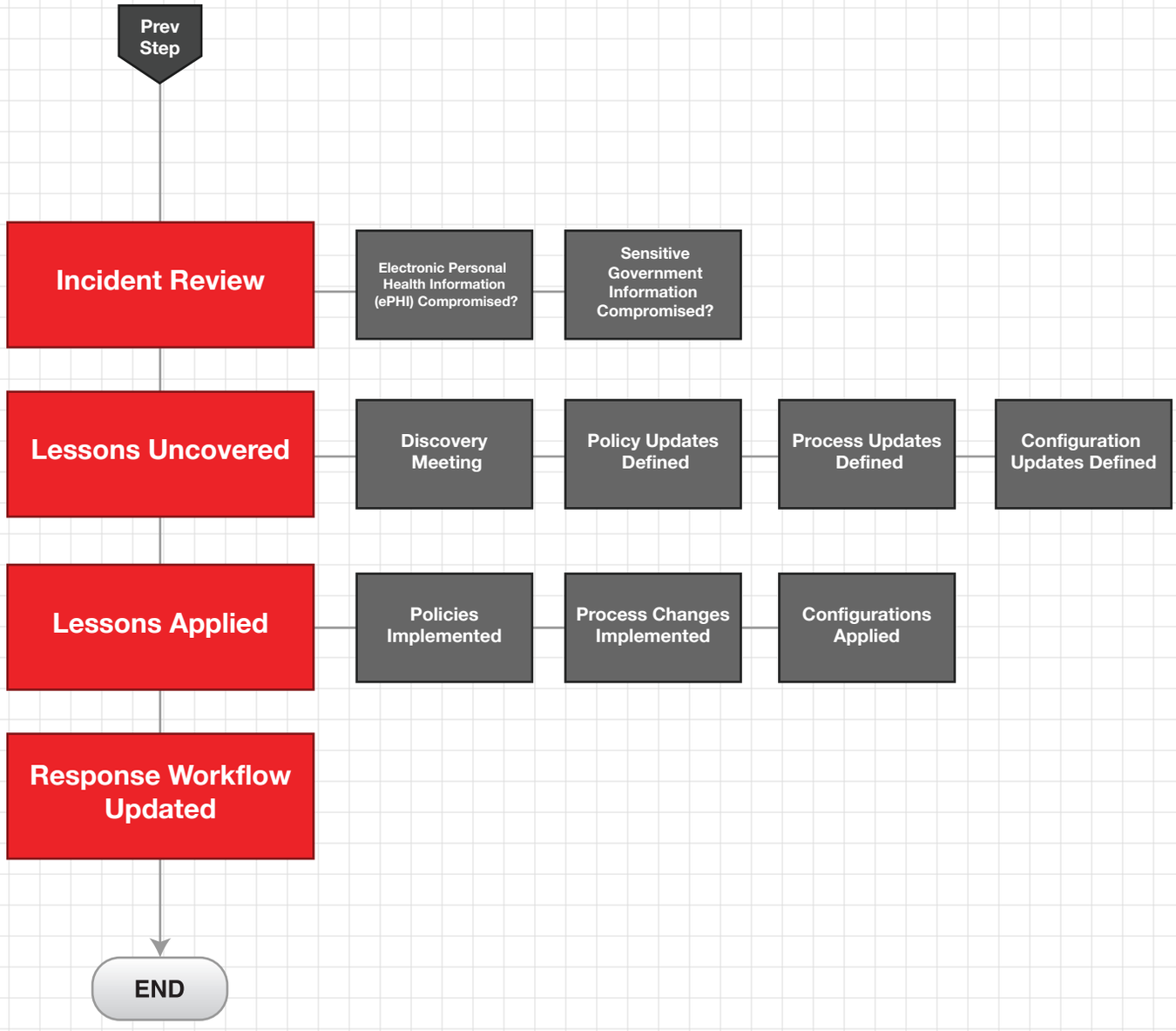

Prev Step
Define Threat Indicators
Standard
Custom
Custom Indicators
Administrative or root access to systems outside of normal business hours
Increased administrator or root logins to a computer system
Logins to multiple systems with same administrative users credentials
Access to a computer system through abnormal ports or protocols
Exfiltration of data off of a computer system
Installation or configuration of unauthorized software or services
Suspicious network traffic being initiated from the internal network
User is unable to log into account
Unexplained use of disabled or dormant user accounts
Unexplained escalation of privileges of user accounts
Unexplained system failures or restarts
Unexplained emails from user accounts
Unexplained modifications to system settings
Unexplained modifications or destruction of user files
Unauthorized creation of new user accounts
Alerting from Firewall and Intrusion Detection systems
Notification from outside organizations (ISP, business partners, 3rd Party)
Categorize Incident
Request Packet Capture
Conduct Content Scans
Next Step


Prev Step
Public or personnel safety affected
Customers are affected by this incident
Employees are affected by this compromise
Products/goods /services are affected by this compromise
Ability to control/ record/measure/track any significant amounts of inventory/products/ cash/revenue has been lost
Standard
Define Risk Factors
Custom
Custom Factors
This act is being launched by known entities
There is internal knowledge of this incident
Determine Patch Methods
There is external knowledge of this incident
Data has been compromised
Worst-case business impact if unable to mitigate this attack
Log Collection
System(s) have been affected
IT services are impacted
Vulnerability or services have been exploited
Evidence Collection
Data Capture
Analysis
Next Step


Prev Step
Identify the system(s) that have been accessed or are at risk
Identify systems to be taken off line due to compromise
Identify system(s) locked out due to repeated login attempts
Identify systems with outage or degradation of services
Identify user accounts compromised or modified
Identify IT services impacted
Identify unauthorized tools used to access systems or user accounts
Identify any source attribution collected
Identify the tools used to detect the attack
Next Step
Servers
Desktop
Laptop
Mobile
VM
LDAP Directory
Incident Database
Threat Database
Vulnerability Logs
System Logs
Select Database
Query Database
Generate Report
View Report
View Record Details
Select Records
Copy Record Details
SIEM
IDS
Firewall
Scanners
Antivirus
Network Monitoring Tools


Prev Step
Triage & Confirm Incident Report
Request System Patch
Direct Phone Call
Conference Call
In-Person Meeting
Intranet Meeting
Communications
Mobile Messaging
Internet Meeting
Eradicate Compromise
Add/Change/ Remove Affected System/Site/Network
Perform data forensics
Determine level of access to identified system
Deploy network collection sensors to capture traffic for further analysis
Determine any lateral movement between systems within the network
Next Step


Prev Step
Recover Systems
Reimage
IDS/IPS & Firewall Updates
Determine alternate network ingress & egress solutions if malware causes DoS
Incident Remediation
Scan host with updated Signature
Scan File Share with updated Signature
Remove Vulnerabilities & Update Routers
Next Step


Prev Step
Incident Review
Electronic Personal Health Information (ePHI) Compromised?
Sensitive Government Information Compromised?
Lessons Uncovered
Discovery Meeting
Policy Updates Defined
Process Updates Defined
Configuration Updates Defined
Lessons Applied
Policies Implemented
Process Changes Implemented
Configurations Applied
Response Workflow Updated
END

Proactive Response

An automated playbooks 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