Incident Response & Preparedness Guide

red canary

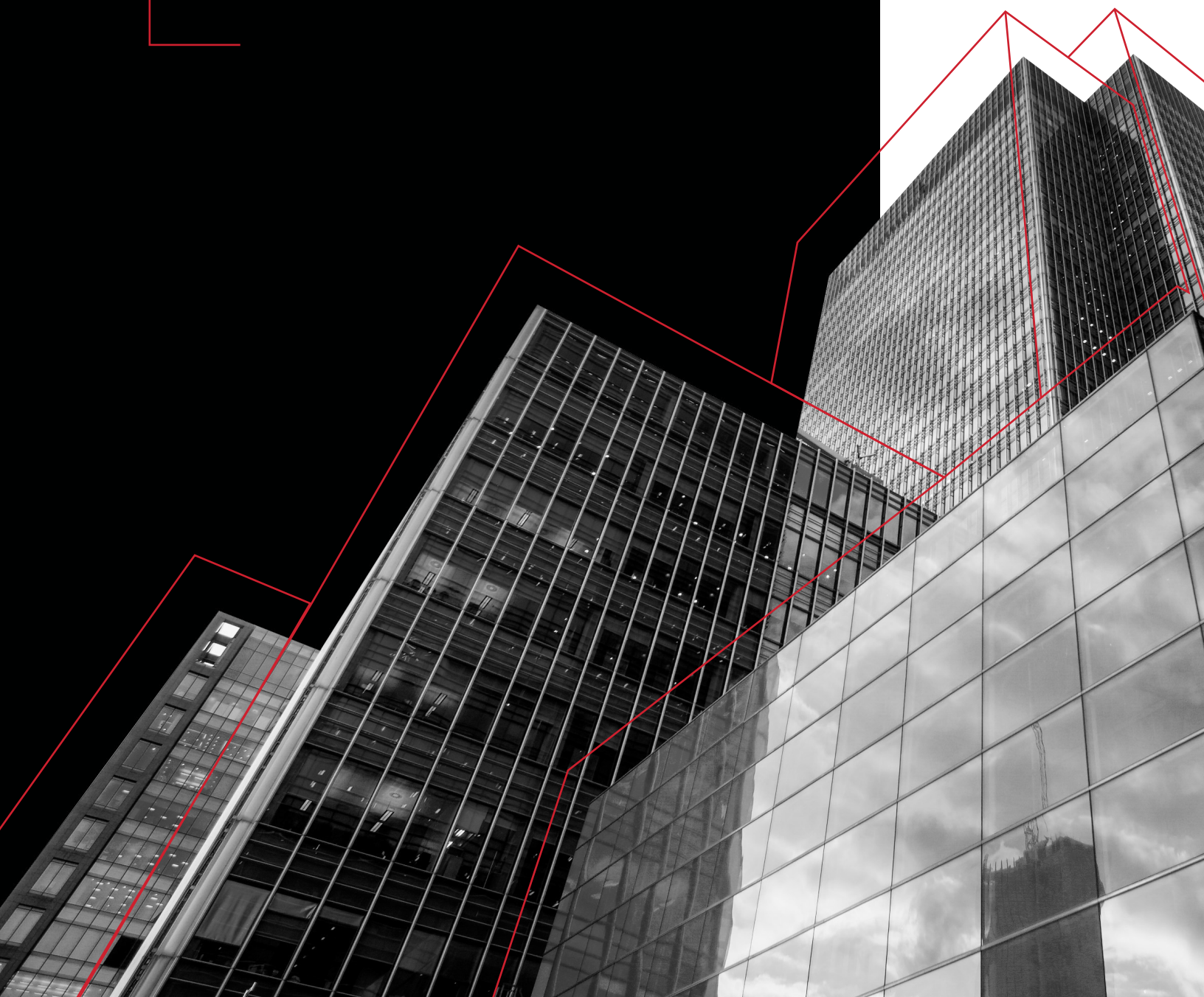
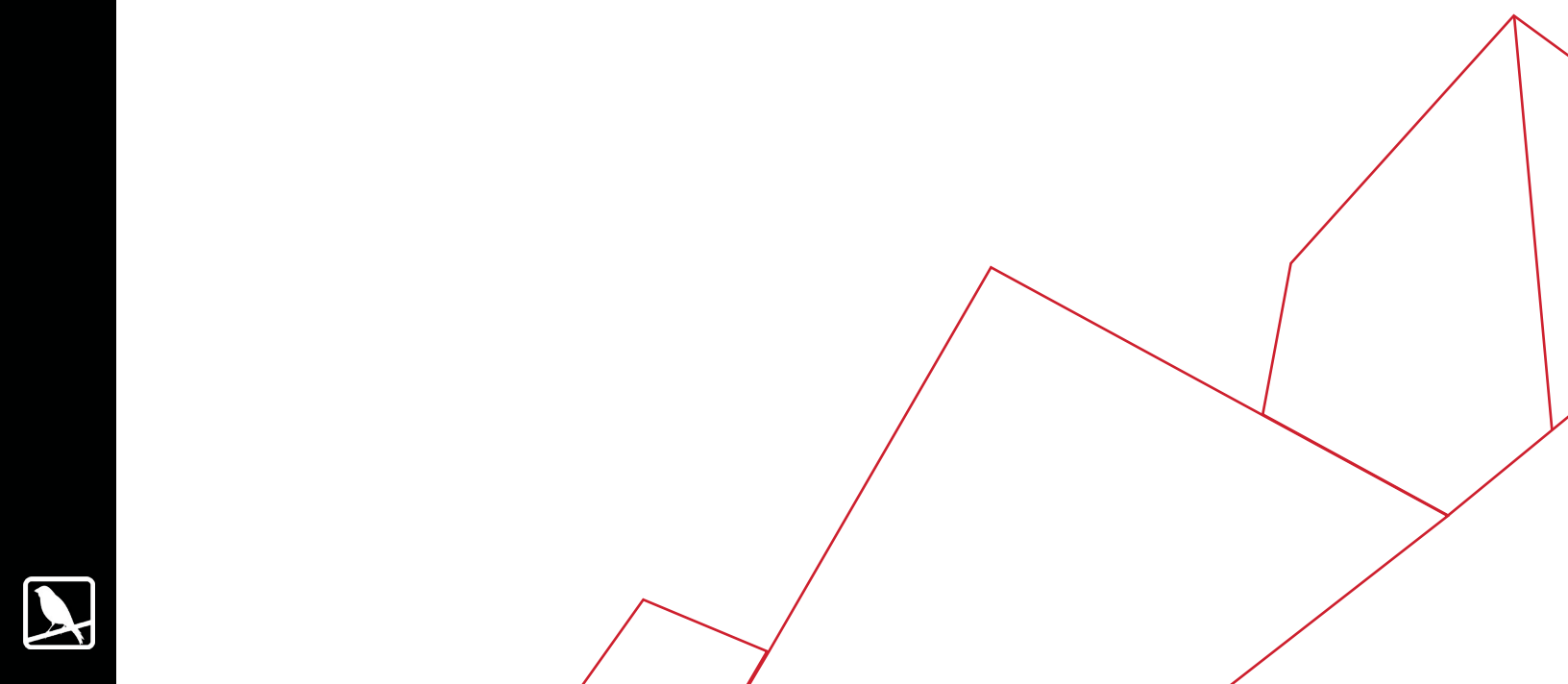


Table of contents



Introduction

When staring down a cybersecurity incident, you can't afford to improvise. All hands on deck won't do much good unless everyone knows what to do. Fortunately, you don't have to start from scratch. This guide will arm you with requisite knowledge and resources to jumpstart your incident response efforts, and better prepare your organization to respond.

What's the problem?

Threats and attacks in this hybrid world are becoming more maleficent and coordinated by the day. We've even seen the rise of adversarial "as-a-service" models that provide pre-packaged malicious tools to execute attacks on targeted organizations. According to the **2021 State of Incident Response Report**, a staggering 92% of security leaders aren't confident in their organization's ability to identify the root cause of an attack. By extension, that means only a fraction of the leaders polled feel confident in their company's preparedness when it comes to incident response (IR). While their concerns run deep, an overwhelming majority of security leaders reported that their top blind spots and worries involved the following:

- **ransomware**
- **remote work challenges**
- **budget constraints**

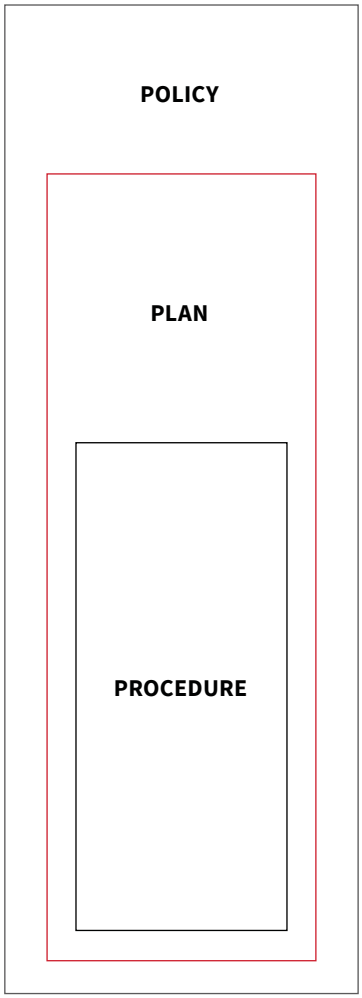
Such fears reflect the current defender's quandary. It's hard to know how to deal with the madness and where to begin. Adversaries are finding clever ways in—whether via misconfigurations, stolen credentials, or numerous other techniques used for initial access. From a defensive perspective, there just doesn't seem to be enough capital nor manpower to adequately fortify your network from those who are trying to besiege it. In today's world, it's not a matter of *if* your organization is going to be attacked, but *when*. The real question is: will you be ready to respond?

Why does this matter for business?

The tentacles of a cyber attack can reach the farthest, most guarded nooks of an organization: areas that safeguard customer and partner data. Worse yet, a sophisticated attack can disrupt operations far beyond the targeted business. Take the **2021 Kaseya VSA attack**, for example. Adversaries compromised VSA by exploiting zero-day vulnerabilities in the remote management and monitoring platform and then used the tool to deliver ransomware payloads to Kaseya's downstream customers. As a result, it's estimated that up to 1,500 small to medium-sized businesses experienced a ransomware incident due to the trickle-down nature of that operation.

While the motives behind attacks vary, the reason they should matter to you is quite simple: Any disruption to operations or loss of data can adversely affect your customers, your business, and your reputation. In other words, IR is a business problem. It embodies several layers of complexity: policy, plan, and procedure. Those components make up the whole of an effective **IR program**.

IR PROGRAM



For the purposes of this guide, we'll be focusing on the middle layer—the plan. There's a lot of nuance in responding to a security event, and the best incident response plans (IRPs) will consider an organization's processes, tooling, expertise, and external parties. The guidance listed below is not intended as a comprehensive playbook, but is meant to foster a high-level crash course in building out your response strategy. The rest is up to you. We're simply here to steer you toward a more prepared future.

Pillars of preparedness

With the **SANS Incident Response Cycle (PICERL)** serving as the backbone, these major organizational steps will enable you to prepare for and respond effectively to incidents while also serving as the primary tenets of an IRP.

Incident management

Tends to be organization-wide and type-agnostic.

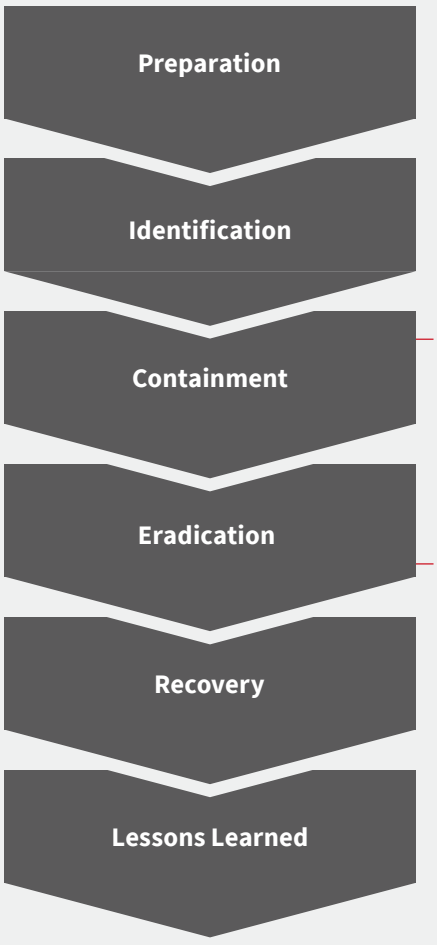
The process of identifying, analyzing, and determining an organization's response to incidents.

SANS INCIDENT RESPONSE CYCLE (PICERL)

Incident response

Triage, in-depth analysis, technical recovery actions, and more.

Teams and processes (playbooks) tend to specialize based on incident type, such as cyber incident response.



Incident handling

Analyzing incident-related data and determining the appropriate response to each incident.

Incident management

Incident management is the overarching, often organization-wide approach to ensuring a standard lifecycle for incidents. Critically, your incident management practices determine how you define, communicate, and respond to incidents. The degree to which you prescribe these and other aspects of incident management depends on your regulatory, compliance, and policy requirements. However, most organizations can approach incident management simply by defining the terms that are used to describe and track incidents.

Incident severity

Incident severity is the single most important element of incident management. Severity is the one place where the nature, scope, and impact of an incident are all reflected in some manner. If defined thoughtfully, and in a way that isn't overly complex, incident severity can radically simplify incident-related communication and help to quickly determine who should be involved in the response. In particular, severity should determine which incidents require escalation to management, the executive team, the board, customers, regulators, or even the general public. Therefore, it's imperative that all internal stakeholders—including company leadership—understand what incident severity means in their environment as a first step to preparedness.

Severity	Description	Typical response
SEV-1 *Initiate response immediately*	Critical system failure preventing multiple customers from accessing services beyond acceptable downtime **or** widespread exposure of sensitive customer data	**Major incident response:** • Notify/invoke responsibilities for all stakeholders • Issue press release
SEV-2 *Initiate response immediately*	Suspected exploitation of security misconfiguration/vulnerability **or** exposure of sensitive customer data **or** sweeping malware infection involving multiple hosts	**Major incident response:** • Notify/invoke responsibilities for internal stakeholders • Monitor for potential escalation to SEV-1
SEV-3 *Initiate response within 5 minutes*	Issues preventing one or more customers from utilizing services **or** security misconfiguration without evidence of exploitation **or** commodity malware isolated to a single host/endpoint	**Normal incident response:** • Monitor for potential escalation to SEV-2
SEV-4 *Initiate response within 2 hours*	Issues requiring triage (not immediate attention)	**Triage workflow:** • Monitor status; escalate if not assigned within reasonable amount of time

Systems for tracking & reporting

Using a tracking system makes incidents far easier to communicate, respond to, and report to stakeholders. At its core, an incident management system (IMS) enables you to record incident metadata including the timeline of events and the incident severity. It can also be used to capture evidence that could ultimately aid in your investigation, root cause analysis, and any legal proceedings. This system acts as a workbench of sorts for practitioners, so it is wise to invest in a system that provides clarity for both responders and internal stakeholders.

Incident tracking & reporting

Must have

date/time
severity
unique ID
description
team members

Nice to have

automated workflows
API integration
access rights restrictions
analytics & reports
incident submission forms

Incident response

This involves the prompt and extensive action to manage the impact of a cyber incident. The step encompasses various, but specific, activities that take place in the context of an incident, from finding incidents to learning from them and preventing similar incidents from happening again. Ideally, it leverages historical data collections and telemetry to assess the situation, determines the overall impact, and ultimately builds and implements a plan to remove the unwanted guest and remediate the root cause. When incident responders describe this step, they often explain it as entering a network where the adversary is still active.

To keep in alignment, it is worth reiterating that we are using the SANS Incident Response Cycle (PICERL) as the authority here. Specifically, we're covering the middle steps that comprise the active incident response actions.

Identification

Detecting suspicious and malicious activity is a critical step in the response process. After all, there will be no action if an incident goes undetected.

Many different tools detect threats and generate alerts or notifications. Security products might include native detection logic or require security teams to develop custom detection analytics. Some detectors are signature-based and rely on static indicators of compromise (IOCs) like IP addresses, binary hashes, and other forensic artifacts. Others are behavioral and based on adversary actions, like suspicious process relationships, command-line parameters, or any combination of these and other endpoint or network activities. Signatures are great for detecting known malicious activity, but typically offer fleeting detection value because adversaries can readily render a signature useless by changing a hash or moving to a new domain. Detecting a behavior is more complex, generally requiring sophisticated tooling and operational maturity. However, the cost is counterbalanced by the relative durability of behavioral analytics.

Mature security teams rely extensively on a combination of signature and behavior-based detections, developing them in-house with the help of third parties.

Signature-based detections

Often depend on explicit indicators of compromise, such as static lists of IPs, hashes, or other forensic artifacts.

Behavior-based detections

Identify malicious and suspicious patterns based on changes in endpoint and network telemetry such as process relationships and command-line parameters.

Advanced detection capabilities

By pairing signature-based and behavioral detection methodologies, security teams can achieve greater defense-in-depth against known malicious indicators and common adversary actions.

Containment

This is the point at which the response team begins to engage with affected hosts. The ultimate goal during this phase is to keep adversaries or malicious software from wreaking further havoc on the already compromised network. Common containment actions might include isolating an endpoint, banning executables based on their hash, or blocking traffic to an IP address. Containment is a complex step in the incident response process during which responders have to balance risk and operational considerations such as:

- What risk does this pose to our customers and our organization?
- What is the business impact of taking a system offline?
- Will isolating an endpoint alert an adversary that we've detected them and hinder further investigation?

Eradication

Once a response team has contained a threat, it must be cleared from an endpoint and/or network completely. This typically involves removing malicious code, revoking tokens for unauthorized access, rebuilding endpoints, and ultimately validating that the eradication steps were fully and effectively carried out.

Recovery

While many assume this explicitly means recovering data or an entire system (one that has been reimaged, validated, and brought back to baseline), recovery can also mean recovery of function. In other words, if you replace a compromised system with a new one, that's also considered a form of recovery. The same applies if your organization decides to part ways with a SaaS provider that was determined to be too great a risk. Restoration of function is what leads to services coming back online and a return to normal operations.

Incident handling

This includes a granular subset of incident response activities that are focused on containment and eradication of identified threats, as detailed above. The handling of an incident is largely informed by threat intelligence—which, in turn, helps responders understand where to look and what to do.

Threat intelligence

Intelligence resources enable a deeper understanding of adversarial tactics, techniques, and procedures (TTPs), goals/trends, and threats. Sources of intelligence can include but are not limited to:

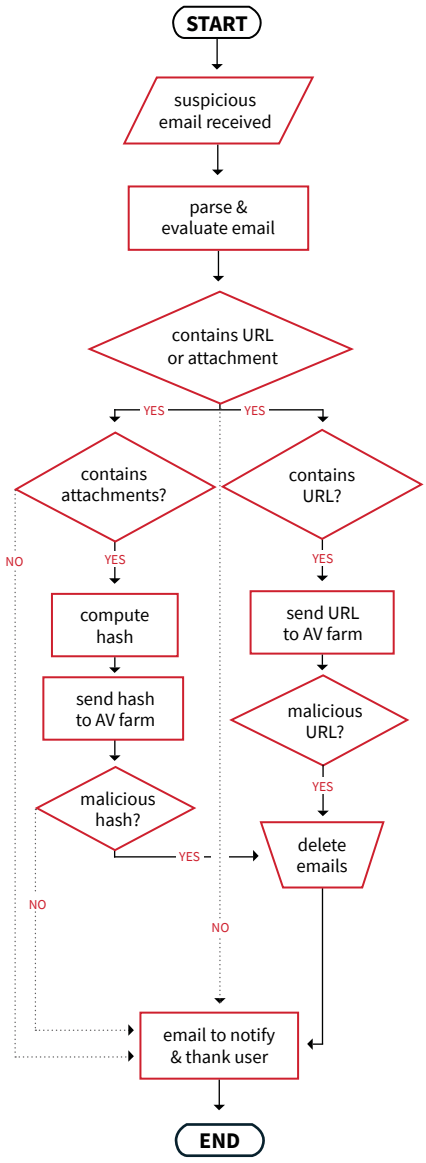
- internal detections
- open source reports, blogs, and social media
- trusted information-sharing and analysis centers (**ISACs**, **ISAOs**, or similar)
- malware analysis
- third-party intelligence sources
- sandboxes

The information may be disseminated to different audiences—from practitioners to executives—through different products. These threat intelligence products may include technical reports, talking points, briefs, and advisory bulletins. The main goal of the products is to create actionable intelligence that informs decision makers, most notably the handlers themselves, and helps them mitigate risk.

Playbooks

These help to establish formalized processes and procedures for incident response actions based on the threat identified. A phishing playbook will look vastly different than a ransomware playbook since the root cause and adversary TTPs tend to diverge. The playbook to the right is a notional example that organizations can leverage and tweak accordingly.

EXAMPLE:
PHISHING PLAYBOOK



Putting it into practice

This brings us to the third and final component of an effective IR program: the procedures.

You want to know who on your team needs to be involved in a major incident and when. But that information can be difficult to assign without first referencing a proven framework. We've found that a RACI matrix is the easiest, most straightforward way to pull this information together.

Our team has developed a fully customizable **Incident Response RACI matrix** to help you visualize and manage the delegation of responsibilities as they relate to SEV-1 or SEV-2 incidents. This matrix is also a useful tool for understanding incident response in the context of business, while pinpointing areas for improvement.

> ***The RACI acronym indicates the four levels of involvement for various parties during an incident: Responsible, Accountable, Consulted, and Informed.***

DOWNLOAD THE RACI MATRIX TEMPLATE →

SEE A COMPLETED EXAMPLE →

How to get started

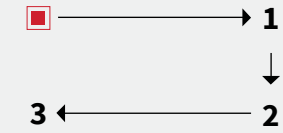
1 **Download the template** and define roles.

Leadership	
Support Team	
Response Team	
External Stakeholders	

2 Fill in responsibilities. Define objectives, items to be vetted (RACI), and outcomes.

IR Plan	R	C	I	C
Tabletop exercises	C	A	R	I
Routine backups	R	C	A	C

3 Create a realistic scenario. For ideas check out **Tabletop Scenarios on Twitter**.



4 Gather internal stakeholders and run the exercise.

5 Review outcome and identify internal process shortcomings.

Methodology

We've provided an example of how an organization with a mature IR function would fill the matrix, but also understand that organizations come in all shapes, sizes, and maturity levels. We encourage you to use this blueprint to fill the matrix in according to your organization's unique structure. Before jumping in, there are some things to know:

Response steps. We've integrated the SANS IR framework into the above matrix and provided necessary response actions/tasks for a major incident.

Roles. During every SEV-1 or SEV-2 engagement, multiple "teams" or stakeholders are involved in the overall IRP and are responsible during various steps of the cycle. Roles should be defined and communicated prior to assigning tasks. We've outlined functional descriptions of required roles.

Your turn. Examine the description of each and match each to a similar role that exists within your organization. In your environment, one person may fulfill the description of two functional roles and that's ok.

INTERNAL IR ROLES

	Function	Example
LEADERSHIP	Executive who serves as the voice of the organization in collaboration with public affairs or communications department, responds to inquiries from external parties during major incidents	**CEO**
	In charge of all security-related processes that protect confidentiality, integrity, and availability of an organization's data	**CISO**
	Head of technology and tools that help keep an organization secure	**CTO**
	Spearheads external communication and legal representation as it pertains to a major incident	**Legal Counsel**
RESPONSE	Liasion between leadership and technical team	**SOC Manager**
	Incident SME and manager of response team	**Incident Commander**
	Individual who analyzes incident data and handles specific response actions	**Security Analyst**
	Includes various people of an IT unit: sys admin, network admin, database admin, exchange admin, etc.	**IT Admin**
SUPPORT	Tracks threat, determines adversarial trends, and develops post-activity testing	**Threat Hunter**
	Deconstructs a malicious payload to determine tactics and techniques	**Reverse Engineer**
	Detects weaknesses in network and takes measures to correct them	**Vulnerability Specialist**

Responsibilities. In case you're wondering how and to whom tasks are delegated, we created this handy chart to help. Study these justifications and limitations before assigning tasks.

RACI KEY

R — Responsible
Who is doing the task?
Who is the assignee?

A — Accountable
Who's in charge?
Who makes the call?

Only one person can be acountable and responsible for each task; in some cases it may be the same person.

C — Consulted
Who can give valuable input?
Stakeholders of this task?

I — Informed
Whose work depends on this?
Who needs to be updated on progress?

Multiple people can be consulted and informed for a given task, but designate at least one person for each.

Canary insights. We'd like to share the top three takeaways we've learned while working thousands of incidents over the past decade in hopes they will inspire you in preparing your matrix.

Leadership should be involved in every step during a major incident.

There should be a shift in responsible and accountable parties as stakeholders work through the IR cycle.

During a major incident, it is often necessary to notify external parties (sometimes even by law).

Jumpstart your incident response readiness with Red Canary

By now you've spent a considerable amount of time thinking about your organization's incident response gaps and opportunities. But actually fixing them? Well, that can be a challenge for even the most mature security programs.

As your security ally, Red Canary is here to help.

Our **security operations platform** and human expertise prevent incidents from happening in the first place. By removing your need to build and manage a threat detection operation, we help you focus on running your business securely and successfully. However, when or if things do go wrong, our incident handling team offers 24-hour support helping customers respond to threats and remediate incidents.

And if you're looking to reduce risk by expanding your incident management strategy, our trusted alliance of partners can assist you with cyber insurance, incident response retainers, proactive security assessments, and incident response preparedness.

hxxps://www[.]linkedin[.]com/company/threathunting

Red Canary MDR

Augment your team and immediately improve your ability to detect, investigate, and respond to advanced threats.

See our MDR in action →

Expert reinforcements

Get connected with our network of experts who can help you navigate all things incident management.

Connect to allies →