



# the hassle-free guide to dominating your next security incident

[trustwave.com](https://trustwave.com)

# contents

---



**01**

hoping for the best



**02**

know your attacker



**03**

hunkering down and getting ready



**04**

catch them if you can



**05**

the time has come to respond



**06**

picking up the pieces



**07**

learning from your mistakes



**08**

piecing it all together



# introduction

---

Boxer Mike Tyson famously quipped:  
“Everyone has a plan until they get punched in the mouth.”



As the youngest heavyweight champion in history, Tyson met many opponents who didn't have a plan. Or if they did, it wasn't substantive enough to overcome Iron Mike's devastating uppercut. A few rivals, however, fended off his ferocious style, giving them enough time to discover weaknesses, which they exploited to victory. Such an occurrence was rare, but it happened.

In the world of cybersecurity, punches aren't flung by professional bruisers, but by professional cyberattackers. Like a boxer, their goal is to hurt you – but they don't want you to realize it until long after you've hit the canvas. The longer they can tip-toe around your databases, networks and applications without you detecting, responding and eradicating their presence, the more damage they will cause.

Which brings us back to that quote from Tyson. Every organization is a target, but not every organization is equipped with a thorough

and well-rehearsed incident readiness and response (IR) plan. Without one, you're setting yourself up for failure and preventing your best chance at success. Experts and studies agree: Arguably the best way to reduce the cost of a breach is with an IR team.

But effective IR isn't accomplished overnight, especially in a fast-moving discipline like security with so many variables at play. That's why we created this handy guide, to help infuse some stability into the frenzied process of preparing for and responding to an incident. We want to slow things down for you, so you know exactly what actions you should take now and aren't scrambling like a fish out of water when the inevitable happens.

Some of the content in this guide, especially in later chapters, will be more technical in nature. We tried to strike a balance between laying the groundwork in straightforward terms with offering deeper guidance that you can use now and in the time of crisis.



# hoping for the best (but expecting the worst)

"They'll always take care of it tomorrow. And then a breach happens.  
When they're not ready, that's when the real trouble starts."

— BRIAN HUSSEY, VP OF CYBER THREAT DETECTION AND RESPONSE, TRUSTWAVE

Let's start by understanding how we reached the point of talking about incidents in terms of absolutes, as opposed to possibilities. Nowadays, no company is completely secure. Breaches are unstoppable. You need only consider the laundry list of high-profile companies that were gutted in the weeks and months leading up to this guide being published.

But companies remain slow in addressing incidents, especially ones that are externally detected, versus internally identified. As we mentioned earlier, intruders don't want to be spotted. The more time they can spend inside a compromised environment, the more reconnaissance they can conduct, the more data they can steal and the more money they can cost your organization.

## Median Time Between Compromise Milestones

### Intrusion to Detection



### Detection to Containment



### Intrusion to Containment



Durations varied greatly in the incidents investigated. The median number of days from the first intrusion to detection of the compromise decreased to 49 days in 2016 from 80.5 days in 2015, with values ranging from zero days to almost 2,000 days (more than five years)



# where do incidents commonly happen?

---



## **CORPORATE/INTERNAL NETWORKS**

Corporate and internal network environments comprise enterprise networks in general and can be home to payment card data, personally identifiable information, medical and patient records, and proprietary information, such as intellectual property.



## **POINT-OF-SALE**

POS environments include dedicated “cash registers,” where businesses accept payment for in-person retail transactions. POS terminals process payment cards using magnetic stripe scanners and EMV chip card readers. Most run versions of the Windows Embedded or Linux operating systems customized for POS device, usually networked to transmit card and sale data to a centralized location and/or a financial institution.



## **E-COMMERCE**

E-commerce environments include web-server infrastructures dedicated to websites that process payment information and/or personally identifiable information (PII).



# 5 factors that drive incident readiness and response

---

01

## ADVANCED THREATS

Cybercriminals are hitting companies from all sides, and their assaults have evolved from acts of opportunity into more organized affairs that target specific organizations thanks to easily accessible tools that, while available to all, are super sophisticated and make detection as difficult as ever.

---

02

## GROWING ATTACK SURFACES

Miscreants prefer the path of least resistance, and the ever-expanding perimeter, combined with the growing transformation of data into a digital format, make it easier and more enticing than ever to find a cushy pathway into your environment. Rising numbers of endpoints and applications, vulnerable business partners, mobile devices and Internet of Things technologies all represent countless more entry points.

---

03

## SKILLS SHORTAGES

Multiple studies have shown the cybersecurity workforce is understaffed and under skilled. You may be feeling it yourself. This chasm leaves companies vulnerable when defending themselves against an adversary who is as capable as ever given the abundant supply of services available to them on the dark web in malware rental shops.

---

04

## LIMITATIONS OF PREVENTION TECHNOLOGIES

Firewalls, anti-virus and intrusion prevention systems offer a familiar first line of defense against threats. But in the same way you wouldn't take a knife to a gunfight, you need to significantly intensify your arsenal to confront today's cyber enemy. The services you should turn to are more offensive-focused and will integrate with your IR. They include:

- **Security Penetration Testing**
- **Enhanced Threat Intelligence**
- **Threat Hunting**
- **Endpoint Detection and Response**

Where problems come in is that resource-starved organizations may not have the adequate skill sets and bandwidth to adopt and deploy these technologies. That is where external forces, like managed security services providers, can assist.

---

05

## COMPLIANCE CONSIDERATIONS

Security-related mandates (for example, the Payment Card Industry Data Security Standard and the impending EU General Data Protection Regulation) typically all include requirements around IR. Specifically, PCI DSS compels an independent forensic investigation to be completed following a breach of cardholder data.





# so, you think you've been breached?

a checklist of questions needing answers



How did the breach occur?



Has any personal information  
(CDE/PII/IP/PHI) been  
accessed or exfiltrated?



Which systems are affected?



How long has the attacker  
been in my network?



How do I contain this breach?



How much is this going  
to cost me?



How can I stop it from  
happening again?





# know your attacker

## how your foes look and act

---

Most response plans rarely include how to handle the specific person(s) who may be behind an incident.

But every enemy is different, and each necessitates a different response. While determining motivation and attribution is difficult – and often unable to be accomplished in the initial stages of a response – your IR team can speed up the process by better understanding the psyche of the attacker.

If you can build a profile of your adversary, you will better know what you're up against. Of course, teams that specialize in vulnerability management, threat intelligence and hunting, and security operations can assist IR to fill out this description by assessing indicators of compromise and other actions being taken by the infiltrator.





5<sup>6</sup>5<sup>0</sup>4<sup>6</sup>4<sup>0</sup>3<sup>6</sup>3<sup>0</sup>6<sup>0</sup>5<sup>6</sup>5<sup>0</sup>4<sup>6</sup>4<sup>0</sup>3<sup>6</sup>3<sup>0</sup>

As a starter exercise, let's categorize those threat actors who are likeliest to cause a major incident. It'll be up to your internal or external security teams (managed security services providers) to get more detailed in the profile.

### **CYBERCRIMINALS**

Organized and diverse in their capabilities, they want to steal data that can be turned into dollars, typically through credit card hacking or ransomware.

### **NATION-STATES**

Often motivated by nationalism first and money second, they want to spy on your operations to steal intellectual property and trade secrets.

### **HACKTIVISTS**

Politically motivated, these adversaries want to wreak havoc on your organization – from data exposure to denial-of-service – to promote their own agendas.

### **MALICIOUS INSIDERS**

This is typically a disgruntled employee who acts out by stealing (perhaps to be used at a next job) or destroying sensitive data.

### **ACCIDENTAL INSIDERS**

This type of worker unwittingly places the company at risk due to poor security practices, such as clicking on suspicious phishing links or attachments contained in emails, or losing a laptop.



# types of incidents

Each incident requires its own response strategy. Threat vectors will vary, from web- and email-based attacks to lost laptops, but every incident can generally fall into one of the following categories (based on US-CERT definitions for federal agencies):



## UNAUTHORIZED ACCESS

In this category an individual gains logical or physical access without permission to a network, system, application, data or other resource.



## DENIAL-OF-SERVICE (DoS)

An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.



## MALICIOUS CODE

Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.



## IMPROPER USAGE

A person violates acceptable computing-use policies.



## SCANS/PROBES/ATTEMPTED ACCESS

This category includes any activity that seeks to access or identify a computer, open ports, protocols, service or any combination for later exploit. This activity does not directly result in a compromise or denial of service.



# when cybercriminals attack

(and the stages in which they do it)

---

## phases of the kill chain

01

### RECONNAISSANCE

The attackers research and select targets.

---

02

### WEAPONIZATION

The attackers join remote access malware with an exploit to create a deliverable payload.

---

03

### DELIVERY

The attackers distribute the weapon – such as an email attachment – to the victim.

---

04

### EXPLOITATION

Code is executed on the victim's systems.

---

05

### INSTALLATION

Malware is installed on the victim's systems.

---

06

### COMMAND AND CONTROL

The attackers have a remote connection into the victim's systems.

---

07

### ACTIONS

The attackers siphon out data, destroy data or take some other action.





# hunkering down and getting ready

---

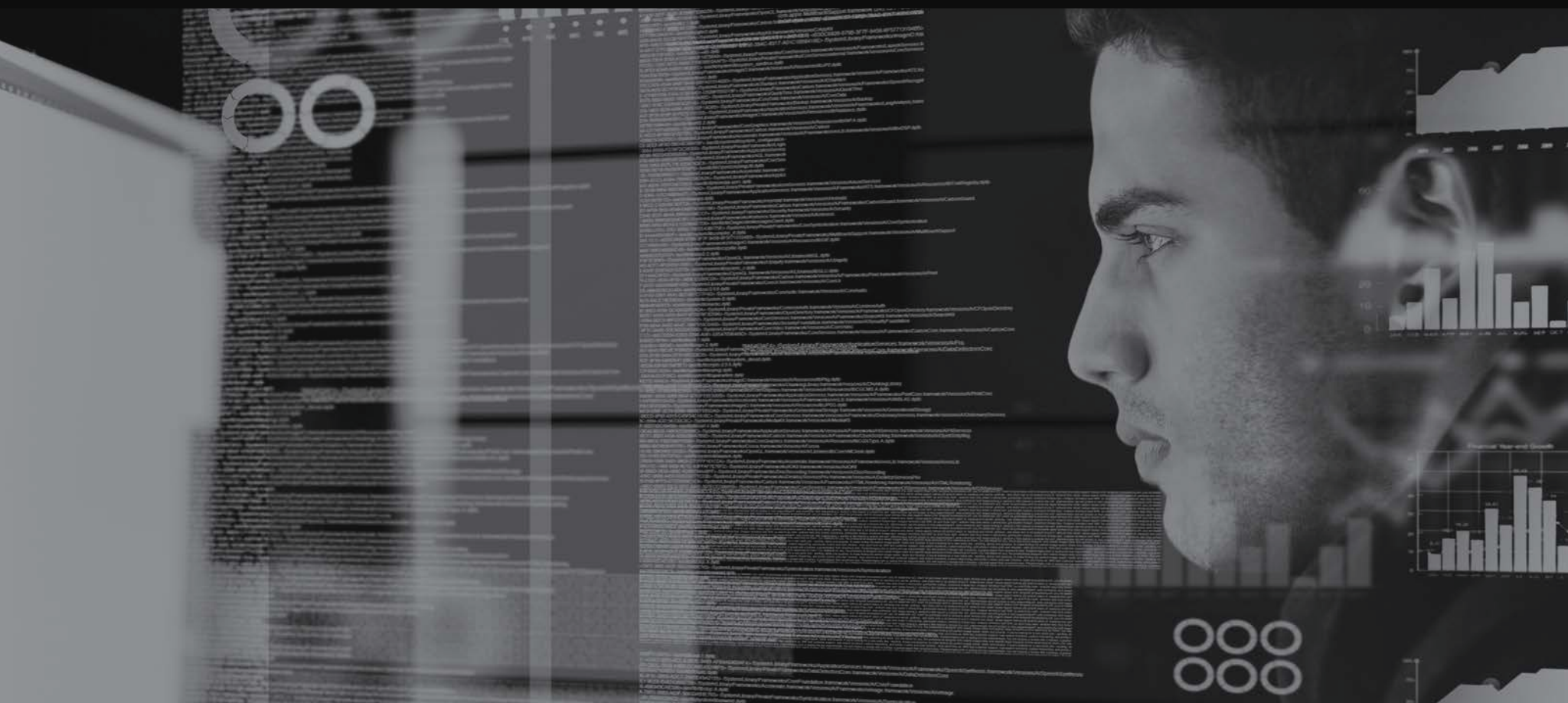
Let's back up a bit. What should you be doing before the attacker gets the point in the kill chain that directly affects you? What if you could act now before any exploitation happens?

Effectively preparing for an incident requires a lot of work, but the scope of your efforts can be reduced if you already have a strong security framework in place. That said, first and foremost, you must perform a risk assessment, which involves documenting system inventories (If you don't know what your assets are or where they live, how will you defend them?), identifying possible risks and determining what can be done to minimize exposure going forward.

Incident readiness also must include regular internal security scans and penetration tests to understand your internal attack surfaces and weaknesses. Remember, your adversaries are having no problem getting past most perimeter defenses, so internal security is critical.

Also, get your non-IT employees, from senior executives on down to rank-and-file workers, trained in security best practices. The more your personnel thinks about security, the more instinctually inclined they will be to report something fishy (no pun intended) that could indicate a brewing incident.

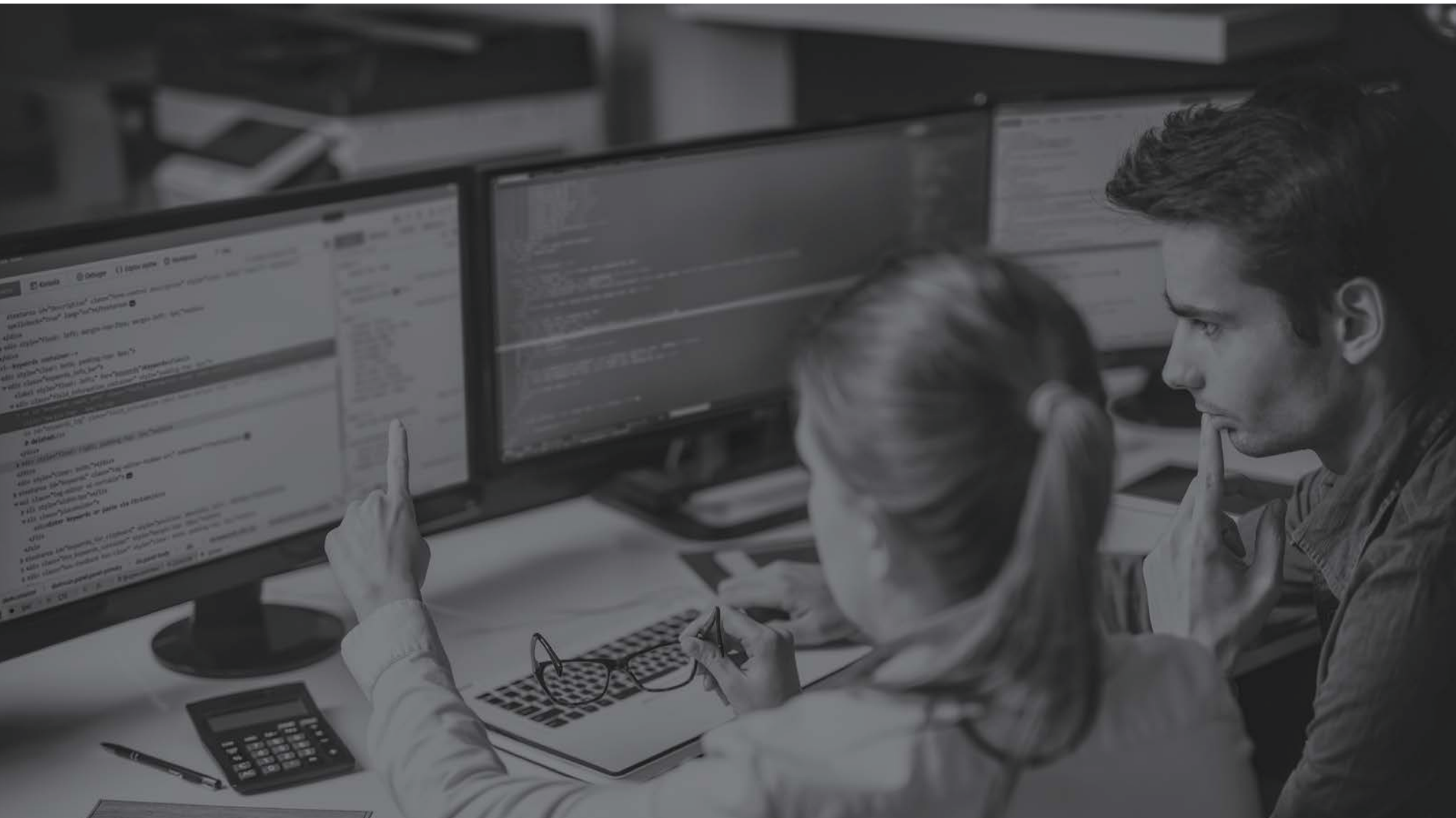
As previously mentioned, you also must shift your focus from prevention-oriented thinking to much more of a detection-oriented mindset. This includes using proactive threat hunting techniques to uncover malicious behaviors that are being missed by preventive security controls, like traditional firewalls or anti-virus.









# creating a team and a plan

A true IR team requires a membership that is much broader than most people realize.



The IT and security team members are obvious, but you also need coverage in many other areas, including:

-  Audit, to assess compliance related issues with a potential breach.
-  Legal counsel, for potential exposures and how to mitigate them.
-  Human resources, to address potential incidents of insider attacks or abuse.
-  Public relations, for managing external communications, including those with customers.

Essentially, the IR team must act as a well-coordinated unit not only in the context of technical security related issues but also in all the “softer” non-technical issues that oftentimes can be even more vexing, particularly when public notifications are involved. The IR plan in this context must be detailed enough that all the cross-functional parties involved understand their roles and under what scenarios they need to be active.

## A TYPICAL IR PLAN WILL ADDRESS THESE KEY AREAS:

- Roles and responsibilities in the event of an incident
- The ability to define security incidents and likely scenarios for response
- Incident handling procedures (technical and administrative)
- Communications plan for internal and external efforts
- Detailed training plans for team members
- Team testing





# mock exercises

---

Don't underestimate the human freak-out component following an incident. Anxiety, distress and panic can quickly short-circuit the decision-making process.

How can you prevent emotions from getting the better of you and your team? Mock exercises are by far the preferred method for evaluating the readiness of the IR plan. You typically select one of your most likely breach scenarios based upon your industry or risk profiles, and then employ either an inside team or external third-party to attempt the exploits and run the scenarios against your team.

Using an outside, third-party consultancy as your "attackers" introduces a degree of variability to your scenarios and results, which typically offers a much more effective and unbiased evaluation of your readiness. You obtain more realism to your exercises which allows not only the testing of individual team activities but also cross-functional communications and coordination, which can be critical during any kind of sustained attacker activity or breach.

# who you gonna call?

---

If a fire is raging through your office, the first thing you're doing is calling the Fire Department. Similar logic applies if you experience a major incident. Using outside consultants as your attackers is an optimal way to achieve realistic outcomes, but what if your team lacks certain skill sets or competencies to respond effectively to a full-out breach scenario? The answer is to diversify – diversify your "people portfolio" by enlisting the help of managed security services provider (MSSP) or perhaps a specialty provider for IR.

The key point here is to get these contracts and relationships in place before you need them, as hiring for these types of services during the heat of an active response is a bad idea and a recipe for disaster. The days of the classic incident response "smokejumpers", while still available, are declining because many more effective approaches are available, including managed security services. At the bare minimum, you should get an IR contract in place ahead of time, as these can be set up relatively inexpensively on a retainer basis, helping assure rapid response when you need it most.



# catch them if you can:

## the art of detection

---

Early detection of attacker activity before a full-scale breach occurs is key to helping minimize the scope and cost of IR operations, not to mention damages to your organization's reputation.

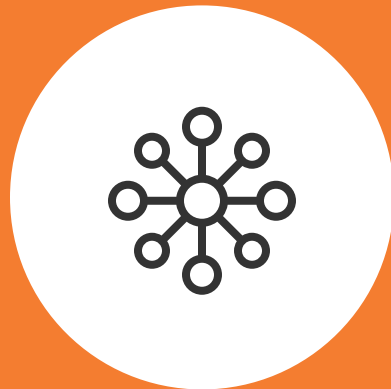
Methods typically fall into two categories: network-based detection or endpoint-based detection. With the former, you typically rely on log feeds from various infrastructure (net flow) devices and security devices to provide context for their monitoring and analysis. With the latter, an endpoint detection and response (EDR) tool set is often used, which requires the deployment of agents (also known as "sensors") onto the endpoints for monitoring behaviors, processes, memory and registry modifications, and user activity on laptops, desktops and servers.



# technology stack

## pros

Speed and ease of deployment  
Traffic pattern analysis and  
protocol anomalies



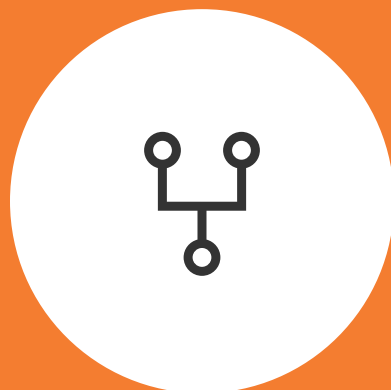
### NETWORK-BASED

## cons

Limited attacker visibility  
Log data consumption  
Limited response support

## pros

High-fidelity monitoring  
Remote tool sets  
Enables proactive threat  
hunting and response



### ENDPOINT-BASED

## cons

Deployment costs  
Endpoint overhead

You should understand the qualitative differences between these two approaches, as it has significant implications for how your IR operations will be enabled and supported. Network-based detection certainly has its benefits, chief among them the speed and ease at which they can be deployed. Threat hunting is accomplished primarily by looking at log feeds from various devices, as well as network traffic patterns for potential protocol anomalies or odd communications between devices across the network.

EDR platforms however, provide much higher-resolution monitoring of the endpoints themselves, offering the kind of visibility into an attacker's actions that allows potential threats to be detected much earlier in the kill chain, before the adversary can embed themselves within your operations.

These capabilities come by installing agent software on each monitored endpoint and then leveraging that presence for not only monitoring and detection, but a very broad range of response and remediation capabilities, significantly enhancing your IR operational capabilities.





# the time has come to respond

The timeliness of an initial response to a security incident makes all the difference to helping eliminate the threat quickly and minimize damages.





**The initial triage requires a complete assessment of the business processes that have been impacted, as well as the discrete systems, assets and data involved.**

Additional areas of concern include:

- Creation of a timeline for the attack and its potential origins
- Quarantine of all impacted systems
- Validation of log integrity and retention
- Initiation of communications to all affected parties, internal and external
- Performance of threat hunting on the network to ensure that the entire scope of the attacker's activities have been assessed and fully contained
- Full remediation of affected systems by removing all identified malware or attacker artifacts, but only after evidence gathering has been completed as described below.

Containment and eradication of the threat are of primary concern during initial response operations, which include a great deal of data acquisition and forensic analysis.

### **VERIFICATION**

For there to be an incident response, an incident must have taken place. Determine and confirm the breadth and scope of the incident, and assess the case in general.

### **SYSTEM DESCRIPTION**

Now that you know you're dealing with a full-blown incident, start gathering data about it and taking notes describing the system you are going to analyze, including what its role is in your network and your organization as a whole. Document the operating system and its general configuration, including RAM, disk format and the location of the evidence.

### **EVIDENCE ACQUISITION**

Next, identify potential sources of data; acquire volatile – or temporary – data stored on various devices, as well as non-volatile data stored on hard drives; and check the integrity of the data and ensure proper chain of custody throughout. After collecting the volatile memory, go into the next step of collecting non-volatile data such as the hard drive using an incident response and forensic toolkit.

These are challenging areas of work so that all available evidence throughout the impacted network and systems are retained in their unaltered state for comprehensive review and potential submission to authorities for more detailed investigation once operations have been stabilized.





# how to preserve evidence:

## nine need-to-do practices

---

**01**

**Back up all available logs, if possible (proxy, firewall, IDS, AV etc.)**

---

**02**

**Make detailed notes about the affected system's current behavior**

---

**03**

**Disconnect affected physical machines from the network**

---

**04**

**Do not reboot or turn on a system suspected of being within the scope of attack**

---

**05**

**Enable flight mode on mobile devices**

---

**06**

**Do not shutdown the machine unless there's no other option  
(Remember that many new malware families exist entirely in volatile memory)**

---

**07**

**Take forensic copies of disk and memory (Ask a forensic professional if unsure)**

---

**08**

**Securely store evidence in a safe or lockable cabinet so that you can  
assure chain of custody**

---

**09**

**Maintain chain-of-custody documentation. If anything is inadvertently done to  
the system, be sure to document exactly what those actions were so they can be  
accounted for during forensic analysis**



# picking up the pieces

---

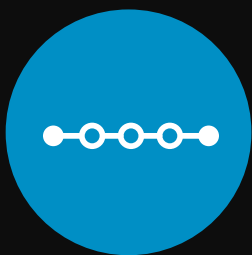
Identification of potential evidence can be time consuming, as it involves comprehensive log reviews, memory dumps of affected systems and a host of other forensic acquisition techniques.

Both the National Institute of Standards and Technology (NIST) and the SANS Institute have developed detailed approaches in these areas.





Here is a summary of five key areas in the recovery and investigation process:



### **TIMELINE ANALYSIS**

This is a crucial step, as it includes information such as when files were modified, accessed, changed and created in a human-readable format, also known as MAC time evidence. The data is gathered using a variety of tools and is extracted from the metadata layer of the file system and then parsed and sorted to be further analyzed later.



### **MEDIA AND ARTIFACT ANALYSIS**

Now it's time to learn what was touched. Which programs were executed, which files were downloaded, which files were clicked on, which directories were opened and which files were deleted. One technique used to reduce the massive data set you'll likely be working with here is to identify known good files and known bad files. (This can be done using databases like the Nation Software Reference Library from NIST and hash comparisons using open-source tools like "hfind" from the Sleuth Kit).



### **STRING OR BYTE SEARCHES**

This step will consist of using tools that will search the low-level raw data images. If you know what you are looking for, you can use this method to find it. You should use tools and techniques that will look for byte signatures of known files, known as the "magic cookies." You'll also want to perform string searches using regular expressions.



### **DATA RECOVERY**

Now you're ready to recover data from the file system. Some of the functionality that will help in this step are available in certain open-source tools, such as the aforementioned Sleuth Kit, and can be used to analyze the file system, metadata layer and data layers. Remember to analyze leftover space and unallocated space, and conduct an in-depth file system analysis to locate files of interest.



### **REPORTING RESULTS**

It's now time to report the results of your analysis. This may include describing the actions performed, determining what other actions need to be performed, and recommending improvements to policies, guidelines, procedures, tools and other aspects of the forensic process.





# learning from your mistakes

---

As painful as it may be to dredge up bad memories, conducting a post-mortem of the incident, including how much it cost and what lessons you learned from it, is one of the most important steps in the entire IR process.





# what's the damage?

---

Determining the price tag of downtime, lost productivity, overtime hours paid during response operations, consultants, etc. are relatively easy to calculate, but what about the costs to your businesses reputation and the impacts to your customers? The intangible costs of a breach are challenging for most organizations to quantify, but they must be considered, at some level, when determining the overall price tag for the breach.

# how can you learn from this?

---

The obvious lessons learned usually center around making the IR process more fluid in the future, but they should also involve the need to bolster internal detection capabilities, which are often misunderstood and underfunded, and sometimes completely lacking. Your adversaries rely on you missing them early in the intrusion kill chain, when they can still be driven out. Your lack of visibility and failure to eradicate the threat is what drives up the severity and costs of your response.

There is no denying that the IR process is complex. In fact, even those companies operating today's most proficient networks continue to struggle with getting it right. The good news is you don't have to do it alone, and you probably shouldn't anyway. Industry experts and analysts agree that teaming up with a company like a managed security services provider, with experienced IR capabilities, has rapidly become a necessity in today's threat environment, if not a security best practice.





# critical questions to ask when choosing your incident response service provider

---

- ❓ Can you provide the qualifications of your response consultants?
  - ❓ Can you describe the engagements you have worked?
  - ❓ What regions of the world do you cover?
  - ❓ How many investigators are on your team?
  - ❓ Is your incident response driven by threat intelligence?
  - ❓ What technologies do you offer as part of the response?
  - ❓ Do you provide on-site/remote support?
  - ❓ Do you have experience with cloud-based networks?
  - ❓ Are you familiar with PCI DSS, HIPAA and other regulations?
  - ❓ Do you have experience providing support with litigation, including expert witness testimony?
  - ❓ Can you handle data storage?
  - ❓ Can you offer status updates and reporting capabilities?
  - ❓ Can you provide blue team (defense) and red team (offense) exercises?
  - ❓ Once we have eliminated the threat and recovered our operations, can you assist with ongoing managed security services, such as threat hunting?
- 

Diversifying your “people portfolio” by adding managed security services into the mix not only extends your security team’s capabilities, but also dramatically lowers operational risk by leveraging the scale and scope of expertise that only a global MSSP can provide. Whenever a threat shows up on your doorstep, it’s highly likely that the MSSP has already dealt with it in some other part of the world. That experience translates into very low latencies in incident response operations, and that means your costs are dramatically lower. Visit [www.trustwave.com](https://www.trustwave.com) to learn more about how we can help fortify your incident readiness and response plan.



# conclusion

## piecing it all together

---

If you've gotten this far, you seem ready to take the first step: admitting that you need to build a battle-tested incident response program

Now, your challenge moves to putting the information contained in this guide to practical use to help create plans, teams and processes.

The final product won't look the same for every organization – and as we mentioned, few companies can do it all on their own – but regardless of your size or industry, your output should contain several key elements. To conclude, we've compiled a convenient checklist of what actions you need to take. You can reference it at any time



**UNDERSTAND THE BASICS**, including how incidents happen, what drives the need for incident response and what questions need answers in case a breach occurs.



**BECOME FAMILIAR WITH DIVERSE TYPES OF INCIDENTS**, so you have a baseline awareness of the episodes that may occur within your company and the motivations of the people behind them.



**BRACE YOUR ORGANIZATION FOR THE INEVITABLE INCIDENT**, which includes testing your systems for vulnerabilities, assembling an IR team and arranging external assistance to help amplify your readiness or response in time of crisis.



**FINE-TUNE YOUR DETECTION MECHANISMS**, concentrating on the endpoints, so you can sniff out active attacks before they develop into full-blown incidents



**DEVELOP A SYSTEMATIC PROCESS FOR RESPONDING TO AN INCIDENT**, from verifying its existence to acquiring, preserving and analyzing evidence.



**GRADE YOUR INCIDENT RESPONSE** so that you can consistently improve your methods, noting that this may include seeking additional assistance from an IR service provider.

