

INSIDER'S GUIDE  
— TO —  
  
**INCIDENT  
RESPONSE**  
◆ EXPERT TIPS ◆



ALIEN VAULT

*welcome, earthling!*

## Navigate Your Journey



The Introduction

1

Arming & Aiming  
Your Incident  
Response Team

2

Incident Response  
Process &  
Procedures

3

The Art of Triage:  
Types of Security  
Incidents

4

Incident  
Reponse Training

5

Incident  
Response Tools

---

*the*

# Introduction

---

The fight to protect your company's data isn't for the faint of heart. As an embattled IT warrior, with more systems, apps, and users to support than ever before, keeping everything up and running is a battle in itself. When it comes to preventing the worst-case scenario from happening, you need all the help you can get, despite your super-hero status.

That's why we've developed this incident response guide. We've collected and curated decades of infosec war stories and intelligence — from across the galaxy — so that you're better armed in the fight against cybercrime. You'll have an insider's perspective on how to build an incident response plan and team, and what tools and training you can use to arm those team members.



*what exactly is*

---

# Incident Response?

---

We're not Wikipedia or Webster's, so if you're looking for a dictionary definition, this isn't the right place. But if a five year old asked us, we might just say, incident response is sort of like a fire drill for the IT guy. When the worst-case scenario becomes reality, it's essential to have the right plan in place, the right people on the job, and the right tools and training to remain vigilant. And that's what reading this incident response guide can give you.

# 6

---

## KEY PHASES OF AN

INCIDENT RESPONSE

---

### *plan*

---



### *Preparation*

Preparing users and IT to handle potential incidents in case they happen (and let's face it, we know they will)



### *Eradication*

Finding and eliminating the root cause (removing affected systems from production)



### *Identification*

Figuring out what we mean by a "security incident" (which events can we ignore vs. which we must act on right now?)



### *Recovery*

Permitting affected systems back into the production environment (and watching them closely)



### *Containment*

Isolating affected systems to prevent further damage (automated quarantines are our favorite)



### *Lessons Learned*

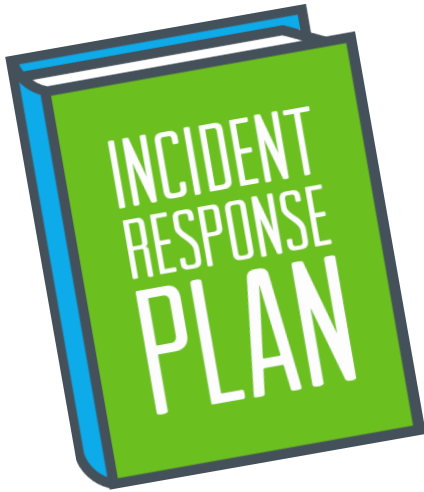
Writing everything down and reviewing and analyzing with all team members so you can improve future incident response efforts



---

# Do I Need an Incident Response Plan?

---

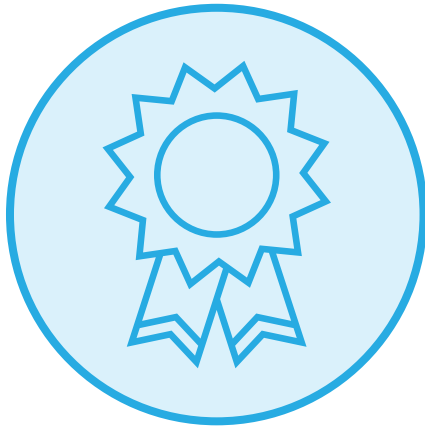


The problem with plans is that they are designed to sit on the shelf until the day when the proverbial oxygen masks drop from the ceiling. Otherwise, they just gather dust except for the occasional auditor visits or executive reviews.

In this guide, we take the active approach because we know that the investment of time and resources spent enhancing incident response will have immediate and ongoing benefits to IT operations. After all, security is a subset of reliability – and everyone wants their systems to be more reliable.

We will walk you through building a basic incident response plan and security monitoring process, covering skills to acquire and helpful resources along the way.

## Straight from the Incident Response Front Lines



### On Defining Incident Response Success.

“There are many levels of success in defensive work... the common wisdom is that the attacker only has to be right once, but the defender has to be right every time, but that’s not always true. Attacks are not all-or-nothing affairs — they happen over time, with multiple stages before final success. To remain undetected against an attentive defender, it is the attacker who must make every move correctly; if an astute defender detects them even once, they have the possibility to locate and stop the whole attack. You aren’t going to immediately detect everything that happens during an attack — but as long as you detect (and correctly identify) enough of an attack to stop it in its tracks, that’s success.”



### Don’t Panic. Stay Focused.

“Execution is key — the range of ways to attack a target can seem limitless — expecting to be an expert on all of them is pointlessly unrealistic. The most important part of incident response is to handle every situation in a way that limits damage, and reduces recovery time and costs. At the end of the day, that’s how you’ll be measured on a job well done... not that you’ve covered every angle of every potential vulnerability.”



### Start with Simple Steps. Attackers are Lazy.

“Attackers have technical and economic imperatives to use the minimum amount of effort and resources to breach their targets — the more you remove the low-hanging fruit on your network, the more you raise the actual level of work an attacker has to expend to successfully infiltrate it.”



**ONTO CHAPTER 1 >**  
**ARMING & AIMING YOUR INCIDENT RESPONSE TEAM**

# CHAPTER *one*

## Arming & Aiming Your Incident Response Team

As much as we may wish it weren't so, there are some things that only people, and in some cases, only certain people, can do. As one of the smartest guys in cyber security points out below, some things can't be automated, and incident response is one of them. That's why having an incident response team armed and ready to go – before an actual incident needs responding to, well, that's a smart idea.

There are several things we'll cover in this chapter of the Insider's Guide to Incident Response. First of all, your incident response team will need to be armed, and they will need to be aimed. Even though we cover true "armature" in terms of incident response tools in Chapter 4, we'll share some of the secrets of internal armor – advice that will help your team be empowered in the event of a worst-case scenario.

And second, your incident response team will need to be aimed. In any team endeavor, goal setting is critical because it enables you to stay focused, even in times of extreme crisis and stress.

In this chapter, you'll learn how to assemble and organize an incident response team, how to arm them and keep them focused on containing, investigating, responding to and recovering from incidents.



Incident Response needs people,  
because successful Incident  
Response requires thinking.”

— Bruce Schneier, Schneier on Security

# Who's on the Incident Response Team?

## Team Leader

Drives and coordinates all incident response team activity, and keeps the team focused on minimizing damage, and recovering quickly.



## Lead Investigator

Collects and analyzes all evidence, determines root cause, directs the other security analysts, and implements rapid system and service recovery.



## Communications Lead

Leads the effort on messaging and communications for all audiences, inside and outside of the company.



## Documentation and Timeline Lead

Documents all team activities, especially investigation, discovery and recovery tasks, and develops reliable timeline for each stage of the incident.



## HR/Legal Representation

Just as you would guess. Since an incident may or may not develop into criminal charges, it's essential to have legal and HR guidance and participation.



We've put together the core functions of an incident response team in this handy graphic. Since every company will have differently sized and skilled staff, we referenced the core functions vs. the potential titles of incident response team members. So you might find that a single person could fulfill two functions, or you might want to dedicate more than one person to a single function, depending on your team makeup. That said, here are a few other key considerations to keep in mind:

## IT leads with strong executive support & inter-departmental participation.

When it comes to cyber security incident response, IT should be leading the effort, with executive representation from each major business unit, especially when it comes to Legal and HR. While the active members of the incident response team will likely not be senior executives, plan on asking executives to participate in major recruitment and communications efforts.

## Clearly define, document, & communicate roles & responsibilities of each team member.

While we've provided general functions like documentation, communication, and investigation, you'll want to get more specific when outlining your incident response team member roles. Make sure that you document these roles and clearly communicate them, so that your incident response team is well coordinated and knows what is expected of them — before a crisis happens.

## Establish, confirm, & publish communication channels & meeting schedules.

Effective communication is the secret to success for any project, and it's especially true for incident response. Print out team member contact information and distribute it widely (don't just rely on soft copies of phone directories. Chances are, you may not have access to them during an incident). Include important external contacts as well, and make sure to discuss and document when, how, and who to contact at outside entities, such as law enforcement, the media, or other incident response organizations like an ISAC.

*tell me...*

## What Does an Incident Response Team Do?

An incident response team analyzes information, discusses observations and activities, and shares important reports and communications across the company. The amount of time spent on any of one of these activities depends on one key question: Is this a time of calm or crisis? When not actively investigating or responding to an incident, the incident response team should meet at least quarterly, to review current security trends and incident response procedures. The more information that an incident response team can provide to the executive staff, the better, in terms of retaining executive support and participation when it's especially needed (during a crisis or immediately after).



*i wonder...*

## Where Should Incident Response Team Members Be Located?



Most companies span across multiple locations, and unfortunately, most incidents do the same. While you might not be able to have a primary incident response team member onsite at every location, strive to have local presence where the majority of business and IT operations happen. The likelihood that you'll need physical access to perform certain investigations and analysis activities is pretty high... even for trivial things like rebooting a server or swapping out a HDD.

# What's the Goal of an Incident Response Team?

The incident response team's goal is to coordinate and align the key resources and team members during a cyber security incident to minimize impact and restore operations as quickly as possible. This includes the following critical functions: investigation and analysis, communications, training, and awareness as well as documentation and timeline development.

## INVESTIGATION / ANALYSIS

### *key questions*

Is this an incident that requires attention now? Which assets are impacted?

### *key tactics*

Determine and document the scope, priority, and impact.

## REPORTING / COMMUNICATIONS

### *key questions*

Which types of security incidents do we include in our daily, weekly, and monthly reports? Who is on the distribution list? What information can we provide to the executive team to maintain visibility and awareness (e.g. industry reports, user behavioral patterns, etc.)?

### *key tactics*

Define and categorize security incidents based on asset value/impact. Document and educate team members on appropriate reporting procedures. Collect relevant trending data and other information to showcase the value the IR team can bring to the overall business.

## RESPONSE / IMPROVEMENT

### *key questions*

What's the most effective way to investigate and recover data and functionality? How do we improve our response capabilities?

### *key tactics*

Investigate root cause, document findings, implement recovery strategies, and communicate status to team members.

*i wonder...*

# How Should I Choose the Right Incident Response Team Members?

In terms of incident response team membership recruitment, here are three key considerations based on NIST's recommendations from their [Computer Security Incident Handling guide](#).



## Aim for 24/7 Availability

Chances are, your company is like most, and you'll need to have incident response team members available on a 24x7x365 basis. In fact, from my experience and those of other insiders, Friday afternoons always seemed to be the “bewitching” hour, especially when it was a holiday weekend. Please note that you may need some onsite staff support in certain cases, so living close to the office can be a real asset in an incident response team member.



## Consider Virtual or Volunteer Team Members (if full-time isn't an option)

You may not have the ability to assign full-time responsibilities to all of your incident response team members. With a small staff, consider having some team members serve as a part of a “virtual” incident response team. A virtual incident response team is a bit like a volunteer fire department. When an emergency occurs, the team members are contacted and assembled quickly, and those who can assist do so. Typically, the IT help desk serves as the first point of contact for incident reporting. The help desk members can be trained to perform the initial investigation and data gathering and then alert the incident response team if it appears that a serious incident has occurred.



## Monitor & Bolster Employee & Team Morale

Incident response work is very stressful, and being constantly on-call can take a toll on the team. This makes it easy for incident response team members to become frazzled or lose motivation and focus. It is important to counteract staff burnout by providing opportunities for learning and growth as well as team building and improved communication. You may also want to consider outsourcing some of the incident response activities (e.g. SIEM monitoring) to a trusted partner or MSSP.

*could you explain...*

## Why Participate on an Incident Response Team?

OVERHEARD AT INFOSEC



“THE DIFFERENCE BETWEEN IT AND IR IS LIKE THE DIFFERENCE BETWEEN BEING A DERMATOLOGIST AND AN ER DOCTOR....

**GIVE ME A CASE OF BAD ACNE ANYTIME OVER A GUN SHOOTING AT 2 AM.”**

As we pointed out before, incident response is not for the faint of heart. It takes an extraordinary person who combines intellectual curiosity with a tireless passion for never giving up, especially during times of crisis. This description sounds a lot like what it takes to be a great leader. And that’s what attracts many of us insiders to join the incident response team. The opportunity to become and be seen as a leader inside and outside of your company is one that doesn’t come often, and can reap more benefits than can be imagined at first. You’ll learn things you’ve never learned inside of a data center (e.g. disclosure rules and procedures, how to speak effectively with the press and executives, etc.) and you’ll be seen as a leader throughout your company.

*tell me...*

## How Can the Team be Armed?



**ONE WORD: EMPOWERMENT**

If an incident response team isn’t empowered to do what needs to be done during a time of crisis, they will never be successful. That’s why it’s essential to have executive participation be as visible as possible, and as consistent as possible. Otherwise, the incident response team won’t be armed effectively to minimize impact and recover quickly... no matter what the scope of the incident.

The key is to sell the incident response team to the executive staff. No matter the industry, executives are always interested in ways to make money and avoid losing it. The stronger you can tie your incident response team goals and activities to real, measurable risk reduction (in other words cost reduction), then the easier it will be for them to say yes, and stay engaged.

Quantifiable metrics (e.g. number of hours of work reduced based on using a new forensics tool) and reliable reporting and communication will be the best ways to keep the incident response team front-and-center in terms of executive priority and support.

**68%**

OF RESPONDENTS TO A RECENT SAN SURVEY CITED A SKILLS SHORTAGE AS BEING AN IMPEDIMENT TO EFFECTIVE INCIDENT RESPONSE



[See the Survey: Maturing and Specializing: Incident Response Capabilities Needed >](#)



*for those who are new to cyber security & incident response,*

## What skills are needed?

The incident response team's goal is to coordinate and align the key resources and team members during a cyber security incident to minimize impact and restore operations as quickly as possible. This includes the following critical functions: investigation and analysis, communications, training, and awareness as well as documentation and timeline development.

Security Analysis is detective work – while other technical work pits you versus your knowledge of the technology, Security Analysis is one where you're competing against an unknown and anonymous person's knowledge of the technology. Detective work is full of false leads, dead ends, bad evidence, and unreliable witnesses – you're going to learn to develop many of the same skills to deal with these.

*Here are five lessons we're happy to share:*

### LOOK FOR THE COMMON DENOMINATORS. LOOK FOR THE COMMON EXCEPTIONS.

Security analysis inevitably involves poring over large sets of data – log files, databases, and events from security controls. Finding leads within big blocks of information means finding the 'edge cases' and 'aggregates' – what is most common and what is least common?

A system may make 10,000 TCP connections a day – but which hosts did it only connect to once? When following a trail of logs, look for things that can be grouped by something they have in common, and then find the one that stands out.

### MAKE ASSERTIONS, NOT ASSUMPTIONS.

In an effort to avoid making assumptions, people fall into the trap of not making assertions. In order to find the truth, you'll need to put together some logical connections and test them.

"If I know that this system is X, and I've seen alert Y, then I should see event Z on this other system."

This is an assertion – something that is testable. If it proves true, you know you are on the right track (assuming your assertion is based on correct information). Always be testing.

### ELIMINATE THE IMPOSSIBLE.

According Sherlock Holmes, "When you have eliminated the impossible, whatever remains, however improbable – must be the truth."

You will encounter many occasions where you don't know exactly what you are looking for... and might not even recognize it if you are looking directly at it. In these circumstances, eliminate the things that you can explain away until you are left with the things that you have no immediate answer to – and that's where to find the truth.

### ALWAYS LOOK FOR A SIMPLER EXPLANATION.

"Never attribute to malice, that which is adequately explained by stupidity." – Hanlon's Razor.

What makes incident response rewarding is the promise of stopping an attack before it can do real damage. When your job involves looking for malicious activity, it's easy to see it everywhere you look. Sometimes the attack you're sure you have discovered is just someone clicking the wrong configuration checkbox, or specifying the wrong netmask on a network range.

### IMAGINE THINGS FROM THE ATTACKER'S PERSPECTIVE. WHAT WOULD YOU DO IN THEIR POSITION?

Experienced security analysts have a skill that cannot be taught, nor adequately explained here. By gaining experience administrating and building systems, writing software, and configuring networks – and also knowing how to break into them – you develop an ability to ask yourself "what would I next do in their position?" and make an assertion that you can test. (It may often prove right, allowing you to 'jump ahead' several steps in the investigation successfully).

Bottom line: Study systems, study attacks, study attackers – understand how they think – get into their head. Be smarter than your opponent.





# FROM THE INSIDER'S VAULT

## *Can you share some of the lessons you've learned from surviving a data breach?*

Here are the things you should know about what a breach looks like, from ground zero, ahead of time. Stress levels will be at an all-time high, interpersonal conflicts will boil to the surface, that dry-run disaster planning drill you've been meaning to do for months, but never found the time for? That one minor change request your senior engineers have had sitting on the table for weeks that consistently got deferred in favor of deploying that cool new app for the sales team? You betcha, good times.

Here are some of the things you can do, to give yourself a fighting chance:

## *Don't Let Security Be an Island*

IT departments (and engineers) are notorious for the 'ivory tower' attitude, we invented the term 'luser' to describe the biggest problem with any network. Create some meetings outside the 'IT Comfort Zone' every so often; the first time you meet the legal and PR teams shouldn't really be in the middle of a five-alarm fire.

Bring some of the people on the ground into the incident response planning process — soliciting input from the people who maintain the systems that support your business processes every day, can give much more accurate insight into what can go wrong for your business than any book full of generic examples can. These are the people that spend their day staring at the pieces of the infrastructure that are held together with duct-tape and chicken wire.

## *Give people a place to talk*

Nondisclosure agreements will be flying left and right, stress levels will be high, and the PR and legal secrecy machine will be in full force. Many employees may have had such a bad experience with the whole affair, that they may decide to quit. Keeping secrets for other people is a stress factor most people did not consider when they went into security as a career choice. Invite your HR department staff to join any NDA discussions, and give employees a place to vent their concerns confidentially and legally. You'll be rewarded with many fewer open slots to fill in the months following a breach.

## *Let others learn from your mistakes*

If you are required to disclose a breach to the public, work with PR and legal to disclose information in a way that the rest of the world can feel like they have learned something from your experiences. Adam Shostack points out in [The New School of Information Security](#) that no company that has disclosed a breach has seen its stock price permanently suffer as a result. However the fallout of intentionally vague and misleading disclosures may hang over a company's reputation for some time. Sharing lessons learned can provide enormous benefits to a company's reputation within their own industries as well as the broader market.

## *It gets better*

Famously overheard at a recent infosec conference, "We're only one more breach away from our next budget increase!" There's nothing like a breach to put

security back on the executive team’s radar. Take this as an opportunity for new ideas and approaches, not just “We’re finally getting that thing we’ve been asking for, all year” — Use the opportunity to consider new directions beyond the constraints of the ‘old normal’. Now is the time to take “Misfortune is just opportunity in disguise’ to heart.

### *Test for Impact, not vulnerabilities*

If you are spending money on third-party penetration testing, you should be expecting more in return than the output of a vulnerability scanner and some compromised systems. Expect reports that show results in terms of impact to business operations, bottom lines and branding — these are the things your executives need to be aware of. Either you look for and determine them ahead of time, or your attacks do.

### *Don’t Panic!*

Murphy’s Law will be in full effect. The information the executive team is asking for was only being recorded by that one system that was down for its maintenance window, the report you need right now will take another hour to generate and the only person with free hands you have available hasn’t been trained on how to perform the task you need done before the lawyers check in for their hourly status update. Panic generates mistakes, mistakes get in the way of work. This advice works from both ends of the command chain — if your executive team is expecting a fifteen-minute status update conference call every hour, that’s 25% less work the people on the ground are getting done. Calm Heads Rule The Day — set expectations early on and don’t go into a disaster recovery plan that principally operates on impossible expectations.



## ONTO CHAPTER 2 >

### INCIDENT RESPONSE PROCESS & PROCEDURES

# CHAPTER *two*

## Incident Response Process & Procedures

When most of us hear terms like “incident response process and procedures” our eyes tend to wander, and our attention starts to drift. Yawn, right?

But, at the same time, it’s a necessary evil these days. How many times do you have to hear that data breaches are inevitable in a single day? Especially at an RSA conference, not to mention your LinkedIn news feed or the front page of USA Today.

Consider this chapter your resource guide for building your own incident response process, from an insider who’s realized — the hard way — that putting incident response checklists together and telling other people about them can honestly make your life easier. In fact, it may even help you keep your sanity. Believe me.

### So, what is an incident response process?

At the end of the day, it’s a business process. In fact, an incident response process is a business process that enables you to remain in business. Quite existential, isn’t it?

Specifically, an incident response process is a collection of procedures aimed at identifying, investigating and responding to potential security incidents in a way that minimizes impact and supports rapid recovery.

Take it from me and many of my friends who wear these battle scars... the more you can approach an incident response process as a business process — from every angle, and with every audience — the more successful you will be.

### What’s the difference between an incident response process and incident response procedures?

Even though the terms *incident response process* and *incident response procedures* are often used interchangeably, we’ve used them in specific ways throughout this guide. An incident response process is the entire lifecycle (and feedback loop) of an incident investigation, while incident response procedures are the specific tactics you and your team will be involved in during an incident response process.

# Incident Response Process: Preparation

## Prioritize your assets, capture baselines

Ask yourself and your leadership, what are our most important assets? In other words, what servers, apps, workloads, or network segments could potentially put us out of business if they went offline for an hour? A day? What information could do the same if it fell into the wrong hands?

Assets that you consider as important to the business may not be the ones that your attacker sees as important (more on that concept in Chapter Three).

Develop a list of the top tier applications, users, networks, databases, and other key assets based on their impact to business operations should they go offline, or become compromised in other ways.

- Quantify asset values as accurately as possible because this will help you justify your budget.
- Finally, capture traffic patterns and baselines so that you can build an accurate picture of what constitutes “normal.” You’ll need this foundation to spot anomalies that could signal a potential incident.

## Connect, communicate & collaborate

Meet with executive leadership, share your analysis of the current security posture of the company, review industry trends, key areas of concern, and your recommendations. Set expectations on what the IR team will do, along with what other companies are doing, as well as what to expect in terms of communications, metrics, and contributions. Find out the best way to work with the legal, HR, and procurement teams to fast track requests during essential incident response procedures.

## Direct & document actions, deliver regular updates

Answer these questions for each team member:

- What am I doing?
- When am I doing it?
- Why am I doing it?

The incident response team members — especially those who are outside of IT — will need ample instruction, guidance, and direction on their roles and responsibilities. Write this down and review it individually and as a team. The time you spend doing this before a major incident will be worth the investment later on when crisis hits. Everyone involved, especially the executive team, will appreciate receiving regular updates, so negotiate a frequency that works for everyone and stick to it.

*OVERHEARD AT BLACKHAT*



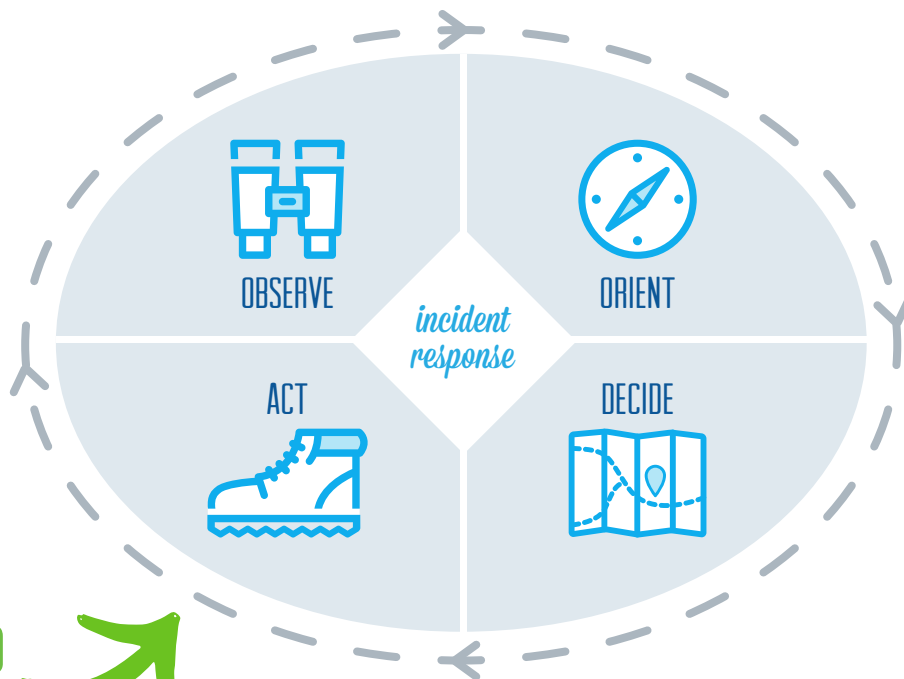
**“BECOME FRIENDS WITH YOUR CFO. IT’S THE BEST ADVICE I’VE HEARD HERE SO FAR.”**

let's talk about...

# Methodology: The OODA Loop

It's not unusual to see a lot of InfoSec warriors use military terms or phrases to describe what we do. Things like DMZ and "command and control" are obvious examples, but one of the best that I've seen for incident response is the OODA Loop. Developed by US Air Force military strategist John Boyd, the OODA loop stands for Observe, Orient, Decide, and Act.

Imagine you're a pilot in a dogfight. You need a tool to determine the best way to act as quickly as possible when you're under attack. It's a useful analogy when applied to an incident response process.



## THE OODA LOOP

### Putting the OODA Loop into Your Incident Response Process



**OBSERVE:** USE SECURITY MONITORING TO IDENTIFY ANOMALOUS BEHAVIOR THAT MAY REQUIRE INVESTIGATION.

#### tools & tactics

Log Analysis; SIEM Alerts; IDS Alerts; Traffic Analysis; Netflow Tools; Vulnerability Analysis; Application Performance Monitoring

#### questions to ask

What's normal activity on my network? How can I capture and categorize events or user activity that aren't normal? And that require my attention now? How can I fine-tune my security monitoring infrastructure?

#### key takeaways

The more observations you can make (and document) about your network and your business operations, the more successful you'll be at defense and response.

**Bonus tip:** Share additional observations with executives that could improve overall business operations and efficiencies — beyond IR.



## ORIENT: EVALUATE WHAT'S GOING ON IN THE CYBER THREAT LANDSCAPE & INSIDE YOUR COMPANY. MAKE LOGICAL CONNECTIONS & USE REAL-TIME CONTEXT TO FOCUS ON PRIORITY EVENTS.

### *tools & tactics*

Incident Triage; Situational Awareness; Threat Intelligence; Security Research

### *questions to ask*

Is our company rolling out a new software package or planning layoffs? Have we (or others in our industry) seen attacks from this particular IP address before? What's the root cause? What's the scope and impact?

### *key takeaways*

Get inside the mind of the attacker so that you can orient your defense strategies against the latest attack tools and tactics. These are constantly changing so make sure you have the latest threat intelligence feeding your security monitoring tools to ensure that they are capturing the right information and providing the necessary context.

**Bonus tip:** Avoid the distraction (and lunacy) of “attack back” strategies... you have enough work to do.



## DECIDE: BASED ON OBSERVATIONS & CONTEXT, CHOOSE THE BEST TACTIC FOR MINIMAL DAMAGE & FASTEST RECOVERY.

### *tools & tactics*

Your Company's Corporate Security Policy ; Hard copy documentation (notebook, pen, and clock)

### *questions to ask*

What do we recommend doing based on the facts available to us?

### *key takeaways*

Document all aspects of the incident response process, especially communications regarding data collection and the decision-making processes.

**Bonus tip:** Use incident response checklists for multiple response and recovery procedures: the more detailed, the better. We cover the essential ones in Chapter Three.



## ACT: REMEDIATE & RECOVER. IMPROVE INCIDENT RESPONSE PROCEDURES BASED ON LESSONS LEARNED.

### *tools & tactics*

Data capture and forensics analysis tools; System backup & recovery tools; Patch mgmt. and other systems mgmt; Security Awareness Training tools and programs

### *questions to ask*

What's the quickest way to remedy affected systems and bring them back online? How can we prevent this in the future? How can we train users better so that these things don't happen again? Does our business process get adjusted based on these lessons?

### *key takeaways*

Training, communication, and continual improvement are the keys to success in acting effectively during an incident. Team members should know what is expected of them and that means in-depth training, detailed run-throughs, and keen attention on how to continually improve teamwork and the overall process.

**Bonus tip:** Use incident response checklists for multiple response and recovery procedures. The more detailed, the better.

### *how about...*

## Incident Response Procedures: The Need for Checklists

One of my former bosses was also a former pilot, and so of course, we had a checklist for everything. And after going through one too many real fires (not to mention fire drills), I can safely say I'm really glad we had them. And I can also safely say that they were constantly being edited for clarity and efficiency – after training exercises, and after real incidents. There was always a better way to do something, and certainly a better way of explaining how to do it.

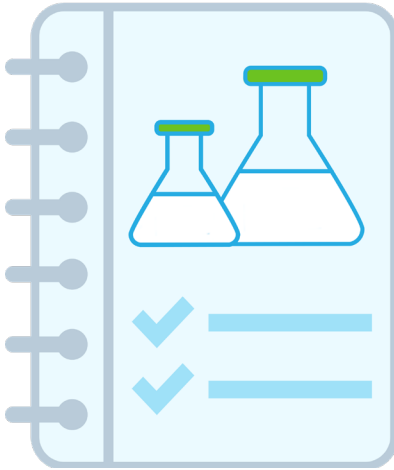
### So... what kind of incident response checklists will I need?

Yes, that's the right question. Because there will definitely be more than one single incident response checklist. The best checklists are those that apply to specific scenarios and break

down a specific task or activity into bite-size chunks. They may also involve a few meandering offshoots – or “if then” – branches off your main checklist, and that's likely where the richest detail will be necessary. Keep in mind though that you may not be able to predict all incident scenarios, and these checklists won't necessarily capture everything that could happen.

Every business operation will dictate what's considered essential for that specific business, because the critical business systems and operations to recover first will be different. That said, there are a few general types of checklists that can be considered essential for any business. Here are a few examples, along with a few references for additional information.

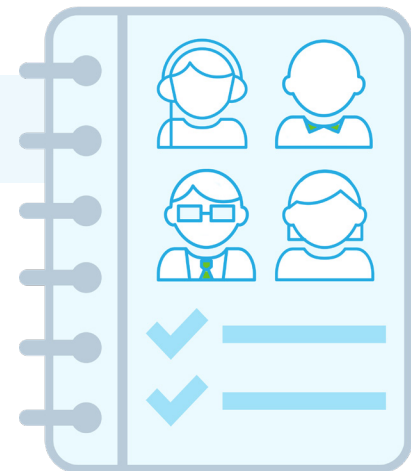




## *Forensic analysis checklists (customized for all critical systems)*

During the process of investigating an incident you'll likely need to look deeper at individual systems. A checklist that provides useful commands and areas to look for strange behavior will be invaluable. And if your company is like most, you'll have a mix of Windows and Unix flavors. Customize each checklist on an OS basis, as well as on a functional basis (file server vs. database vs. webserver vs. domain controller vs. DNS).

**Some useful references: SANS Incident Handling Handbook and Lenny Zeltser's Security Checklists**



## *Emergency contact communications checklist*

Don't wait until an incident to try and figure out who you need to call, when it's appropriate to do so, how you reach them, why you need to reach them, and what to say once you do. Instead, develop a detailed communication plan with the specifics of when to put it into place and don't forget to get overall consensus on your approach. The entire incident response team should know whom to contact, when it is appropriate to contact them, and why. In particular, review the potential worst case scenarios (e.g. an online ordering system going down right in the middle of Cyber Monday) and identify the essential staff who can get these critical systems back online, as well as the management team who will need to remain updated throughout the crisis.

**Bonus tip: You'll also need to document when it is or is not appropriate to include law enforcement during an incident, so make sure you get the necessary input and expertise on these key questions.**



## *System backup and recovery checklists (for all OSes in use, including databases)*

Each system will have a different set of checklist tasks based on its distinct operating system and configurations. It's also important to note the time it takes for each step required to restore operations, and also test full system backup and full system recovery while you're documenting each checklist. There should also be specific steps listed for testing and verifying that any compromised systems are completely clean and fully functional.



## *“Jumpbag” checklists*

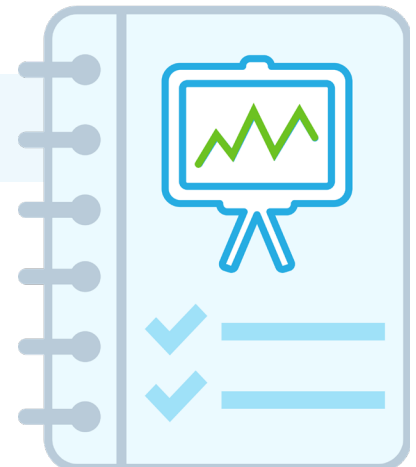
SANS, one of the premier sources of information for the incident responder, recommends that each incident response team member have an organized and protected “jump bag” all ready to go that contains the important tools needed for a quick “grab-and-go” type of response. Their recommended items include:

- An Incident Handlers Journal to be used for documenting the who, what, where, why, and how during an incident
- Your incident response team contact list
- USB drives
- A bootable USB drive or Live CD with up-to-date anti-malware and other software that can read and/or write to file systems of your computing environment (and test this, please)
- A laptop with forensic software (e.g. FTK or EnCase)
- Anti-malware utilities
- Computer and network tool kits to add/remove components, wire network cables, etc. and hard duplicators with write-block capabilities to create forensically sound copies of hard drive images

## *Security policy review checklist (post-incident)*

The most important lessons to learn after an incident are how to prevent a similar incident from happening in the future. In addition to potential updates to your security policy, expect incidents to result in updates to your security awareness program because invariably, most incidents result from a lack of user education around basic security best practices. At the very least, this checklist should capture:

- When the problem was first detected, by whom, and by which method
- The scope of the incident
- How it was contained and eradicated
- The work performed during recovery
- Areas where the incident response teams were effective
- Areas that need improvement:
  - Which security controls failed (including our monitoring tools)?
  - How can we improve those controls?
  - How can we improve our security awareness programs?



*one last thing...*

## The Need for Incident Response Forms & Surveys



As we've mentioned several times already, you'll need to document many things during your job as an incident responder. The best way we've seen to capture an accurate, standard, and repeatable set of information is to do it with a form. And, thankfully, [SANS has provided a form](#) for every type of security incident tidbit you'll need from contacts to activity logs with specific forms for handling intellectual property incidents.



ONTO CHAPTER 3 >

THE ART OF TRIAGE: TYPES OF SECURITY INCIDENTS



FROM THE  
—  —  
INSIDER'S VAULT

## Incident Response Myth Busting for Executives

---

### *Myth #1: An incident response process begins at the time of an incident*

**Truth:** Actually, an incident response process never ends. It's a continual process, like other business processes that never end.

**Advice:** Give your executives some analogies that they'll understand. For example, an incident response process is like a subscription-based business model, e.g. software-as-a-service. It's always on. It's important to point out that there will be stages of criticality for incidents, some that will require more serious reporting and external involvement, and some that won't. See Chapter 3 for more details on this.

---

### *Myth #2: Each "incident" is a discrete, monolithic event, which may occur 1-2 times a year*

**Truth:** As many of us know, we're constantly working on incidents. Evaluating log files, investigating outages, and tweaking our monitoring tools at the same time. Some of these are related to each other, and some aren't. And again, it's constant, daily work.

**Advice:** Explain — at a high level — how incident response works. As a continual process, it's a daily activity, that moves from high level investigations and pivots to specific abnormalities or outages, sometimes developing into something more significant, and sometimes not. Share an example of a specific investigation and offer to provide weekly updates on incident response process metrics, cyber security threat trends, system performance data, user activity reporting, or any other information that would be relevant for the executive team.

---

### *Myth #3: We haven't had any incidents yet, so why do we even need this tool or that resource?*

**Truth:** It's hard to believe, but there are still skeptics about the very real cyber security risks facing us, and the even more real possibility of becoming the next victim. When it comes to cyber security, looking at past experience reveals nothing about what could happen in the future, particularly considering the pace of innovation happening in cyber crime.

**Advice:** Time for more executive education. Point out that you've done your best to mitigate major risks up until this point, but the adversary continues to up their game. It's sort of like that moment in Jaws, "you're going to need a bigger boat!"

# CHAPTER *three*

## The Art of Triage: Types of Security Incidents



**NOT EVERYTHING IS AN EMERGENCY, BUT ANYTHING COULD BECOME ONE.**

Understanding whether an event is an actual incident reminds me of that common expression, “I know it when I see it” made famous by US Supreme Court Justice Stewart. He was talking about pornography, not obscenity, but a common misperception of “knowing it when you see it” can often plague the most well intentioned incident responders.

The uncomfortable truth is that you may not know it when you see it, because the latest attacker tools and techniques are increasingly stealthy, and can often hide in plain sight. The trick is to view your network and operations from the perspective of an attacker, looking for key indicators and areas of exposure before they’re exploited. And it all comes down to how artfully you can do incident triage.

Typically used within the medical community, effective triage saves lives by helping emergency medical personnel rapidly assess wound or illness severity and establish the right protocols, in the right order, to reduce trauma and sustain patient health and recovery. All in the midst of crisis, when every second counts.

In this chapter, we’ll give you the tools to craft your ability to triage information security incident types. You’ll learn how to identify the various types of security incidents by understanding how attacks unfold, and how to effectively respond before they get out of hand.



### SECURITY INCIDENTS VS. INFORMATION SECURITY INCIDENTS

A quick note on the difference between a security incident and an information security incident... In this guide, the assumption is that we’re focused on the various types of information security incidents vs. your standard security incident, which might not involve digital information and could be completely contained within the physical world (e.g. physical assault). That said, there may be occasions that mix things up — types of information security incidents or attacks that do involve a physical component (e.g. laptop theft).

why do...

# Different Types of Security Incidents Merit Different Response Strategies

So what are you protecting against? The best way to determine the appropriate incident response in any given situation is to understand what types of attacks are likely to be used against your organization. For example, [NIST](#) has provided the following list of the different attack vectors:



## *External/Removable Media:*

An attack executed from removable media (e.g., flash drive, CD) or a peripheral device.



## *Email:*

An attack executed via an email message or attachment (e.g. malware infection).



## *Attrition:*

An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.



## *Improper Usage:*

Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.



## *Web:*

An attack executed from a website or a web-based application (e.g. drive-by download).



## *Loss or Theft:*

The loss or theft of a computing device or media used by the organization, such as a laptop or smartphone.



## *Other:*

An attack that does not fit into any of the other categories.

## BONUS TIP



REVIEW THE ABOVE LIST WITH AN EYE TOWARDS ENSURING THAT YOUR SECURITY POLICIES AND CONTROLS HAVE MITIGATED THE MAJORITY OF THE RISKS PRESENTED BY THESE VARIOUS ATTACK VECTORS. YOU'LL ALSO USE THIS LIST TO GUIDE YOUR TEAM IN DETERMINING HOW TO CLASSIFY THE VARIOUS TYPES OF SECURITY INCIDENTS.

## BONUS TIP



IDENTIFY WHICH PIECES OF EQUIPMENT WOULD CAUSE THE GREATEST RISK TO THE COMPANY IN THE EVENT OF LOSS OR THEFT. IN MOST COMPANIES, THE CFO'S LAPTOP WOULD BE INCLUDED ALONG WITH ANY SERVER HDD CONTAINING IP OR OTHER SENSITIVE DATA.



# Categorize Information Security Incident Types by Getting Inside the Mind of the Attacker

One of the biggest fallacies with traditional information security is the underlying assumption that you know which path an attacker will take through your network. For example, attackers rarely come through your front door, or in this context, your gateway firewall. But each attack does generally work through a certain pattern, or what Lockheed Martin has called the “cyber kill chain.”

The “cyber kill chain” is a sequence of stages required for an attacker to successfully infiltrate a network and exfiltrate data from it. Each stage demonstrates a specific goal along the attacker’s path. Designing your monitoring and response plan around the cyber kill chain model is an effective method because it focuses on how actual attacks happen.

## the cyber kill chain stages: how attacks progress



### ATTACKER'S GOALS:

- Find target
- Develop plan of attack based on opportunities for exploit

stage 1



### ATTACKER'S GOALS:

- Place delivery mechanism online
- Use social engineering to induce target to access malware or other exploit

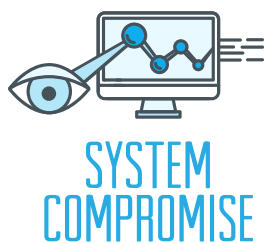
stage 2



### ATTACKER'S GOALS:

- Exploit vulnerabilities on target systems to acquire access
- Elevate user privileges and install persistence payload

stage 3



### ATTACKER'S GOALS:

- Exfiltrate high-value data as quietly and quickly as possible
- Use compromised system to gain additional access, “steal” computing resources, and/or use in an attack against someone else









stage 4

tell me...

# Which Security Events Do I Really Need to Worry About?











Which security events develop into the type of information security incident that requires my attention now? And... what do I do about it? To help categorize each incident type, align each one against the cyber kill chain to determine appropriate priority and incident response strategy. You can use this table as a start.

## INCIDENT TYPES & RECOMMENDED ACTIONS





<i>incident type</i>	<i>kill chain stage(s)</i>	<i>priority level</i>	<i>recommended action</i>
<b>PORT SCANNING ACTIVITY*</b> <b>[PRE-INCIDENT]</b>	 <b>RECONNAISSANCE &amp; PROBING</b>	 <b>LOW</b>	Ignore most of these events UNLESS the source IP has a known bad reputation, and there are multiple events from this same IP in a small timeframe.  <b>Bonus tip:</b> AlienVault's OTX is an excellent way to check on an IP's reputation score.
<b>MALWARE INFECTION</b>	 <b>DELIVERY &amp; ATTACK</b>	 <b>LOW-MEDIUM</b>	Remediate any malware infections as quickly as possible before they progress. Scan the rest of your network for indicators of compromise associated with this outbreak (e.g. MD5 hashes).
<b>DISTRIBUTED DENIAL OF SERVICE [DDoS]</b>	 <b>EXPLOITATION &amp; INSTALLATION</b>	 <b>HIGH</b>	Configure web servers to protect against HTTP and SYN flood requests. Coordinate with your ISP during an attack to block the source IPs.
<b>DISTRIBUTED DENIAL OF SERVICE DIVERSION</b>	 <b>EXPLOITATION &amp; INSTALLATION</b>	 <b>HIGH</b>	Sometimes a DDoS is used to divert attention away from another more serious attack attempt. Increase monitoring & investigate all related activity, and work closely with your ISP or service provider.



# INCIDENT TYPES & RECOMMENDED ACTIONS

<i>incident type</i>	<i>kill chain stage(s)</i>	<i>priority level</i>	<i>recommended action</i>
<b>UNAUTHORIZED ACCESS</b>	 <p><b>EXPLOITATION &amp; INSTALLATION</b></p>	 <p><b>MEDIUM</b></p>	Detect, monitor and investigate unauthorized access attempts – with priority on those that are mission-critical and/or contain sensitive data.
<b>INSIDER BREACH</b>	 <p><b>SYSTEM COMPROMISE</b> (An inside job doesn't require much Recon)</p>	 <p><b>HIGH</b></p>	Identify the privileged user accounts for all domains, servers, apps, and critical devices. Ensure that monitoring is enabled for all systems, and for all system events, and also make sure it's feeding your log monitoring infrastructure (your USM or SIEM tools).
<b>UNAUTHORIZED PRIVILEGE ESCALATION</b>	 <p><b>EXPLOITATION &amp; INSTALLATION</b></p>	 <p><b>HIGH</b></p>	Configure your critical systems to record all privileged escalation events and set alarms for unauthorized privilege escalation attempts.
<b>DESTRUCTIVE ATTACK (SYSTEMS, DATA, ETC.)</b>	 <p><b>SYSTEM COMPROMISE</b></p>	 <p><b>HIGH</b></p>	Backup all critical data and systems. Test, document, and update system recovery procedures. During a system compromise – capture evidence carefully, and document all recovery steps as well as all evidentiary data collected.
<b>ADVANCED PERSISTENT THREAT (APT) OR MULTISTAGE ATTACK</b>	 <p><b>ALL STAGES</b></p>	 <p><b>HIGH</b></p>	Any one of the singular events that are listed here could actually be a part of the worst type of security incident imaginable... the dreaded APT. The important thing is to view each event through a larger context, one that incorporates the latest threat intelligence (see below for more on the need for threat intelligence).

# INCIDENT TYPES & RECOMMENDED ACTIONS

<i>incident type</i>	<i>kill chain stage(s)</i>	<i>priority level</i>	<i>recommended action</i>
<b>FALSE ALARMS**</b>	 <p>ALL STAGES</p>	 <p>LOW</p>	<p>Much of the incident responder's job is spent eliminating irrelevant information and removing false positives. You'll be constantly fine-tuning the radio of security monitoring to get to just the right signal.</p>
<b>MALWARE INFECTION</b>	 <p>ALL STAGES</p>	 <p>HIGH</p>	<p>Incident response is a discipline of continual improvement. As you see more and more events turn into incidents, you'll discover new ways to categorize those incidents, as well as new ways to prevent them from ever happening in the first place.</p>

## \* A NOTE ABOUT PORT SCANNING:

Even if you're sure that an attacker is getting no useful information back from their scanning, if they seem to be doing a detailed and comprehensive scan of your external systems, it is reasonable to interpret this as intent to follow-up the recon with attack attempts later on. If the scanning originates from a legitimate organization's networks, then contacting their security team (if they have one) or network management personnel is usually the best approach.

As a last resort, if no contact details are apparent, try the contact details listed in the WHOIS information for the domain. The email address `abuse@domain` is often a contact email for this kind of communication, but may not be available for smaller or younger organizations. BTW, blocking the source address may be counterproductive, and merely cause the attacker to use a different source address.

## \*\* A NOTE ABOUT FALSE ALARMS:

We've expressed the need to "concentrate on what you know" many times in this guide – much of the work that security monitoring discovers is mundane yet vital.

- ➔ **Controls Failure:** Firewall ports that shouldn't be open to the world, categories of websites that should be blocked at the proxy, hosts that were compromised because they didn't have endpoint security installed. Incident Response work is best thought of as "quality assurance" for the rest of your security efforts.
- ➔ **Noise Reduction:** If security analysis is about finding the 'needle in a haystack,' one of the best ways to make the job easier is to make a smaller haystack. Remove unnecessary traffic, unwanted services, outdated client software, and easily-patched vulnerabilities.
- ➔ **Policy Violation:** Ideally, you hope to be spending more of your time locating the things happening that put your network at risk, not cleaning up the results of that risk being exploited by a hostile party.

be sure to...

# Combine Local & Global Threat Intelligence for Effective Triage

We often think of incident response as being detailed, meticulous forensic work, looking closely at one system at a time. However, the great majority of security monitoring work can be addressed through seeing a larger more holistic picture of the state of, and activity on, your infrastructure.

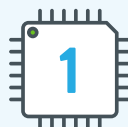
Understanding where, which, and how your systems are communicating with other systems, and the changes being made to them, can reveal attacks that other security controls cannot.

Threat intelligence allows you to move away from a focus on vulnerabilities, exploits and patches, and focus on the things that are actively causing damage to your company's data confidentiality, integrity, and availability.

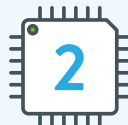
The first step is to understand as much as possible about your current computing environment. Some people refer to this as environmental awareness or situational awareness or even contextual awareness. We like to think of it as local threat intelligence.

Once you combine rich information about your own network with the latest global threat intelligence (specifics on attacker tools, techniques, and trends), you'll achieve effective triage. You'll put your immediate focus on the types of security incidents that matter vs. wasting your time on false positives or irrelevant noise.

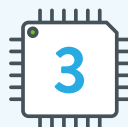
## TOP 5 TRUTHS ABOUT ENVIRONMENTAL AWARENESS



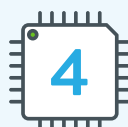
Unless your infrastructure is entirely static and unchanging, new vulnerabilities and exposures are being created all the time.



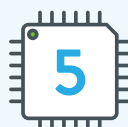
Good IT and Security management processes will do its best to minimize these, but the security analyst still needs to be aware of them to place other things into context.



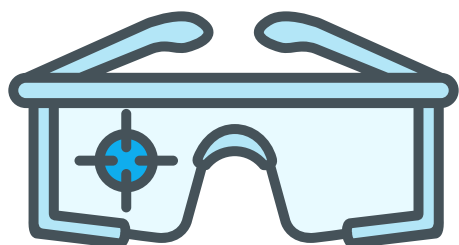
Unexpected configuration changes to systems can reveal when a hostile party has control of the system through valid credentials and methods.



Many configuration options are related to certain compliance standards – alerting (or reporting) on these is a far better way to manage them than waiting for them to be discovered during your next audit.



You can't do security just by looking for attacks and exploits – you have to look into what's happening on your network and know the systems you have deployed.



**GLOBAL THREAT INTELLIGENCE BRIDGES THE GAP BETWEEN DETECTING KNOWN METHOD OF ATTACK, AND DETECTING KNOWN THREAT ACTORS. EVEN IF WE DON'T KNOW ALL THE METHODS THEY MAY CURRENTLY BE USING, WE CAN SEARCH OUR OWN NETWORK FOR KEY INDICATORS THAT OTHERS MIGHT HAVE SEEN OUT IN THE WILD.**

---

*so here's...*

---

## The Bottom Line

---

By understanding what is happening on your network (environmental awareness) and connecting it to information about known sources of malicious activity (Global Threat Intelligence), it becomes simple to get large-scale reports on active threats within your infrastructure. For example, instead of searching through massive lists of alerts from various security controls to determine possible exploits and attacks, and attempting to prioritize them based on asset value, we look at environmental awareness data that can be connected to the indicators of compromise associated with threat actors.

Today, computing resources are cheap and plentiful – attacks can come from anywhere – especially from compromised systems on otherwise legitimate remote networks. Attackers fight a constant battle trying to make it difficult to locate the systems that control their malware, while still allowing their malware to reach these systems to receive execution instructions.

See our next chapter – Chapter Four — Incident Response Tools for how-to instructions on uncovering more information on attack sources.



**ONTO CHAPTER 4 >**  
INCIDENT RESPONSE TOOLS



## The Importance of Attribution

*Let me tell you a tale from the front lines*

We were hunting down an active attack, endpoints had been compromised and they had migrated to using stolen credentials to access the network directly — without further use of the RAT (remote access tool) on the compromised system. As we watched our attackers access the network from multiple locations we began to build our profile of them — what hours were they active, could we determine a particular time zone they may be located in? How many people were acting together? Finally we realized something from the connection authentication information... The connections we saw from multiple remote locations were actually only from a single host — a cloud-provisioned host. As the host was brought online to stage attacks from it, it was being relocated to lower-load hardware clusters with an entirely different upstream connectivity. We noticed that the host had used many different IP addresses and physical connectivity sets (spanning three different countries), but it was still the same virtual machine instance the entire time.

We were well prepared to do identification of remote hosts on VPS - style co-location arrangements, but the global motility of hosts on cloud providers had temporarily thrown us for a loop — we realized that the game had once again changed right before our eyes.

In this case, we had an obvious advantage that we had pre-existing data points to correlate together that allowed us to uncover what was happening behind the curtain; but it would have been much better if we had the ability to easily identify this beforehand. And I realized that the network identification tools we have today are all built for a pre-cloud Internet — a world where IP addresses are tied to physical hosts in physical locations owned by identifiable registered organizations. Now

anyone that remembers the Internet pre-1999 will remember the venerable Ident() protocol (rapidly made obsolete as it represented a security risk in the open untrusted Internet).

Yet couldn't a tokenized, anonymous version of this provide some measure of utility in a cloud-served public Internet? The ability to query Amazon's web services and know that all three EC2 instances currently attacking me are all operated by Tokenized Amazon Customer F8E993C?

Until an initiative to create something of this sort arises and gets implemented, I'll have to stick with more abstruse methods of remotely fingerprint cloud instances post facto. As cloud computing offers ever more copious amounts of utility computing: OS instances that can be launched, operated, and deleted in a matter of minutes, we on the defensive end of things need some way to keep up with the increasing complexity of attribution.

The increasing need for attribution techniques in incident response is not just some by-product of a Security Analyst wanting to play counter-intelligence agent. Attribution is vital for correlating and prioritizing the tidal wave of data we need to pour through to make informed response decisions. Being able to correlate two seemingly unrelated minor attack attempts on different parts of the infrastructure launched from two random hosts on the same multinational cloud computing provider can make a huge difference.

There is much work in progress on establishing reputation between cloud service providers and their customers — but the need to establish reputation information from cloud instances to the rest of the world is essential in the world of the Incident Responder.”

# CHAPTER *four*

## Incident Response Tools



IT'S NOT JUST ABOUT THE GEAR. IT'S ABOUT HOW, WHEN, AND WHY TO USE IT.

Any discussion of incident response deserves a close look at the tools that you'll need for effective incident detection, triage, containment and response. We'll cover the best tools for each function, we'll share resources for how to learn how and when to use them, and we'll explain how to determine the attack source. That way, you'll know the right decision to make at each stage of the investigation.

### The Three A's of Incident Response

In order to be effective in defending your company's network, you'll need the right Ammunition, you'll aspire to identify proper Attribution, and you'll focus on increasing Awareness as a way to reduce the volume and impact of cyber incidents on your company. Still not clear on the A's? Read on...

**Ammunition:** Most incident responders will want to spend most of their time here, downloading and customizing incident response tools — open source as well as proprietary. Why? Because it's fun, and that's what cyber geeks tend to like to do: code. We'll mostly cover open source incident response tools in this chapter, and we'll also use the OODA loop framework from Chapter Two so you'll know when to use which tool and why.

**Attribution:** Understanding where an attack is coming from can help you understand an attacker's intention as well as their technique, especially if you use real-time threat intelligence to do so. We'll cover the basics of attribution, and include some free and open resources to keep you updated on who might be attacking your company based on the latest collaborative threat intelligence.

**Awareness:** The most fundamental security control is an educated and aware user. While we plan to go deep into incident response training in the next chapter, in this chapter we'll cover some of the highlights you'll want to consider as you update your security awareness program. The biggest takeaway here is that every incident should be examined as a way to improve your overall security program, with awareness as a key part of that.

# Incident Response Tools & the OODA Loop

**Disclaimer:** Our preference is for open source incident response tools, and so we've provided recommendations on some of the best open source options. Keep in mind that your mileage may vary. In some cases, you may need to look at proprietary options for certain capabilities. That said, you'll have to go somewhere else for recommendations on vendor tools (unless they're built by aliens, in which case, you're in the right place. ;)).

**For a refresher on the OODA loop:** check out Chapter Two. Developed by US Air Force military strategist John Boyd, the OODA loop provides an effective framework for incident response.



## THE OODA LOOP



# OBSERVE: USE SECURITY MONITORING TO IDENTIFY ANOMALOUS BEHAVIOR THAT MAY REQUIRE INVESTIGATION.

<i>type of IR tool</i>	<i>why you need it</i>	<i>open source options</i>
Log Analysis, Log Management, SIEM	Logs are your richest source for understanding what's going on in your network, but you'll need an IR tool that makes sense of all of those logs, and that's what log analysis is all about.	<ul style="list-style-type: none"> <li>➔ <a href="#">AlienVault OSSIM™</a> — open source security information management</li> </ul>
Intrusion Detection Systems (IDS) — Network and Host-based	HIDS and NIDS monitor server and network activity in real-time, and typically use attack signatures or baselines to identify and issue an alert when known attacks or suspicious activities occur on a server (HIDS) or on a network (NIDS).	<ul style="list-style-type: none"> <li>➔ <a href="#">Snort</a></li> <li>➔ <a href="#">Suricata</a></li> <li>➔ <a href="#">BroIDS</a></li> <li>➔ <a href="#">OSSEC</a></li> </ul>
Netflow Analyzers	Netflow analyzers examine actual traffic within a network (and across the border gateways too). If you are tracking a particular thread of activity, or just getting a proper idea of what protocols are in use on your network, and which assets are communicating amongst themselves, netflow is an excellent approach.	<ul style="list-style-type: none"> <li>➔ <a href="#">Ntop</a></li> <li>➔ <a href="#">NfSen</a></li> <li>➔ <a href="#">Nfdump</a></li> </ul>
Vulnerability Scanners	Vulnerability scanners identify potential areas of risk, and help to assess the overall attack surface area of an organization, so that remediation tasks can be implemented.	<ul style="list-style-type: none"> <li>➔ <a href="#">OpenVAS</a></li> </ul>
Availability Monitoring	The whole point of incident response is to avoid downtime as much as possible. So make sure that you have availability monitoring in place, because an application or service outage could be the first sign of an incident in progress.	<ul style="list-style-type: none"> <li>➔ <a href="#">Nagios</a></li> </ul>
Web Proxies	Web Proxies are thought of as being purely for controlling access to websites, but their ability to log what is being connected to is vital. So many modern threats operate over HTTP — being able to log not only the remote IP address, but the nature of the HTTP connection itself can be vital for forensics and threat tracking.	<ul style="list-style-type: none"> <li>➔ <a href="#">Squid Proxy</a></li> <li>➔ <a href="#">IPFire</a></li> </ul>





# ORIENT: EVALUATE WHAT'S GOING ON IN THE CYBER THREAT LANDSCAPE & INSIDE YOUR COMPANY. MAKE LOGICAL CONNECTIONS & USE REAL-TIME CONTEXT TO FOCUS ON PRIORITY EVENTS.

<i>type of IR tool</i>	<i>why you need it</i>	<i>open source options</i>
Asset Inventory	In order to know which events to prioritize, you'll need an understanding of the list of critical systems in your network, and what software is installed on them. Essentially, you need to understand your existing environment to evaluate incident criticality as part of the Orient/Triage process. The best way to do this is to have an automated asset discovery and inventory that you can update when things change (and as we know, that's inevitable).	→ <a href="#">OCS Inventory</a>
Threat Intelligence Security Research	Threat intelligence gives you global information about threats in the real world. Things like Indicators of Compromise (IoCs), bad reputation IP addresses, command-and-control servers and more, can be applied against your own network assets, to provide a full context for the threat.	→ <a href="#">AlienVault® OTX™</a> → <a href="#">AlienVault Labs</a>



# DECIDE: BASED ON OBSERVATIONS AND CONTEXT, CHOOSE THE BEST TACTIC FOR MINIMAL DAMAGE & FASTEST RECOVERY

<i>type of IR tool</i>	<i>why you need it</i>	<i>open source options</i>
Your Company's Corporate Security Policy*  Hard Copy Documentation (notebook, pen, and clock)	If this section looks familiar, it's not deja vu... it's because it <b>IS</b> familiar... These are the same recommendations we made in the Decide section in Chapter Two.  <b>Insider secret:</b> There are no "Decide" tools, and until AI is truly a "thing," we'll keep having to do what humans do, use our brains. Decide based on the information you have at your disposal, which includes the tools above, as well as your own company's security policy.	→ <a href="#">Your good ol' noggin</a>



# ACT: REMEDIATE AND RECOVER. IMPROVE INCIDENT RESPONSE PROCEDURES BASED ON LESSONS LEARNED.

<i>type of IR tool</i>	<i>why you need it</i>	<i>open source options</i>
Data Capture & Incident Response Forensics Tools	Data Capture & Incident Response Forensics tools is a broad category that covers all types of media (e.g. memory forensics, database forensics, network forensics, etc.). Incident Response Forensics tools examine digital media with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information, all designed to create a legal audit trail.	<ul style="list-style-type: none"> <li>➔ <a href="#">SANS Investigative Forensics Toolkit (SIFT)</a></li> <li>➔ <a href="#">Sleuthkit</a></li> </ul>
System Backup & Recovery Tools Patch Management and Other Systems Management	System backup and recovery and patch management tools might be something you've already got in place, but it's important to include them here since an incident is when you'll likely need them most.	<ul style="list-style-type: none"> <li>➔ <a href="#">AMANDA</a></li> <li>➔ <a href="#">OPSI (Open PC Server Integration)</a></li> </ul>
Security Awareness Training Tools and Programs	Security awareness training tools and programs are an essential way to improve your overall security posture and reduce the likelihood of incidents.	<ul style="list-style-type: none"> <li>➔ <a href="#">SANS' Securing the Human</a></li> </ul>

\* If you haven't written a corporate security policy yet, and need assistance, you can contact a few associations for free resources and guidance like [Educause](#). In addition to Charles Cresson Wood's [Information Security Policies Made Easy](#), there are also a number of vendors who sell information security policy templates, here's one [example](#).

*attribution:*

# Identifying Ownership on the Anonymous Internet

One of the most underrated IR tools is one of the most obvious, if you start thinking about infosec like Sherlock Holmes would. Uncovering a mystery for Sherlock started and ended with the motivation and attribution of the criminal under investigation.

## Who is this & what do they want?

The challenge for the incident responder is that someone's "identity" on the Internet is exceedingly difficult to determine

with any reliability and certainty on your own. IP address and domain ownership aren't terribly easy to interpret, and as you likely know, anyone can easily anonymize their connection through proxies and other means.

That said, there are certain tricks and tools you can deploy to get better insight into who and where these nefarious characters are, and more on what they want and the techniques they deploy to get it.

## Q: WHICH NETWORK DOES AN IP ADDRESS BELONG TO?

### *Answer:*

Public IP addresses are sold to organizations in blocks of varying sizes. Just as how Domain names have their registration information listed with a registrar, public IP networks have the information available publicly via network registrars.

- ARIN (North America)
- APNIC (Asia-Pacific)
- RIPE (Europe, Russia and the Middle East)
- AFRINIC (Africa)
- LACNIC (Latin America)

These registrars maintain their own WHOIS services, but for networks instead of Domains. Here's a query against ARIN for the address 192.168.3.56

- NetRange: 192.168.0.0 - 192.168.255.255
- CIDR: 192.168.0.0/16
- OriginAS:
- NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED\*
- NetHandle: NET-192-168-0-0-1
- Parent: NET-192-0-0-0-0
- NetType: IANA Special Use

### *Resources:*

You're likely familiar with the concept of RFC 1918 addresses that are dedicated for use on trusted networks, behind firewalls and other gateway devices vs. the open Internet. If not, you can read more about this here:

[http://en.wikipedia.org/wiki/Regional\\_Internet\\_registry](http://en.wikipedia.org/wiki/Regional_Internet_registry)



## Q: HOW DO I FIND ALL NETWORKS THAT BELONG TO AN ORGANIZATION?

### *Answer:*

Organizations are free to use their assigned IP space wherever they wish, but to make it reachable over the Internet, they must inform other major Internet-connected routers how to reach that IP space, via **Border Gateway Protocol (BGP)**.

**BGP** assigns traffic destinations on the Internet by mapping IP networks to **Autonomous System (AS)** numbers. Each Internet-connected organization receives an **AS** number to identify them by.

**AS** numbers are assigned to a legal entity (e.g. a corporation) – though a company may own more than one AS, this is uncommon exception for backbone carriers.

### *Resources:*

The **CIDR Report website** is the easiest publicly accessible tool for listing all networks currently assigned to an Autonomous System.



## Q: HOW DO I FIND WHAT DOMAINS POINT TO AN IP ADDRESS?

### *Answer:*

Because the resolution of a domain name to an IP address is controlled by the owner of the domain, there is no central registry of mappings.

There are however independent projects that map the Internet and maintain public registries of the most recently-seen mapping of domain to address.

### *Resources:*

<https://www.robtext.com/> is an excellent multi-purpose tool for information about domains, addresses, and networks

<http://domainbyip.com/> provides a free lookup service for domains pointing to a single IP address

<http://www.domaintools.com/> is a commercial service that provides a wealth of information (including historical information) about domains.



## Q: HOW DO I FIND THE LOCATION OF AN IP ADDRESS?

### *Answer:*

Several services attempt to maintain registries of approximate mappings of the physical location of the organization, network or system an IP address is currently assigned to.

**Insider tip:** Physical Location of an IP address is of somewhat limited value to the DFIR analyst in most aspects of their work. The organization that owns the address space is usually of more relevance for identifying connections between addresses. Information networks are not limited by geographic boundaries.

### *Resources:*

<http://www.maxmind.com> is recognized as somewhat of the defacto industry leader for this service – they offer a limited free service with more detailed information offered on a subscription basis.

<http://freegeoip.net/> is a community-funded service that provides automation services and detailed location information.



## Q: HOW ACCURATE IS GEOLOCATION INFORMATION?

### *Answer:*

IP addresses are, by their nature, a logical not physical identifier – networks can be re-assigned from one side of the planet to another, within a few hours at the very most.

Most location information about IP addresses is derived from the location of the organization that owns it. A multinational corporation may have networks across 5 continents, but all its address space will likely be registered to the location of the company's HQ.

Like all information kept up to date through the aggregation of data from multiple sources, geolocated Information accuracy will vary from point to point, IP address to IP address.

### *Resources:*

**AlienVault® Open Threat Exchange® (OTX™)**



**OPEN THREAT EXCHANGE**

# Security is Everyone's Job

FROM WIKIPEDIA



**“SECURITY AWARENESS IS THE KNOWLEDGE & ATTITUDE MEMBERS OF AN ORGANIZATION POSSESS REGARDING THE PROTECTION OF THE PHYSICAL, & ESPECIALLY INFORMATIONAL ASSETS OF THAT ORGANIZATION.”**

Security awareness is sort of like motherhood. It's one of the hardest jobs because it's the most important yet least respected, and if everyone did it properly, we'd likely put an end to war around the world, right?

In all seriousness, every post-incident examination should include an assessment of your overall security posture especially, the security awareness program. Regardless of the root cause of the incident, it's still important to revisit how a more security-savvy employee community could have averted the crisis.

This isn't the part of the guide where we bash dumb users. Seriously. Phishing and spearphishing campaigns can fool even the most sophisticated users. In fact, an estimated 91% of hacking attacks begin with a phishing or spearphishing email.\*

So examine each investigation with the perspective of understanding where your security awareness program could have prevented that incident, or minimized its impact, if only those lessons, guidelines, or tips were shared with your employees ahead of time.

And speaking of security awareness lessons, guidelines, and tips, read more in our next chapter, Incident Response Training.

\* Source: <http://www.wired.com/2015/04/hacker-lexicon-spearphishing/>



**ONTO CHAPTER 5 >**  
INCIDENT RESPONSE TRAINING

# CHAPTER *five*

## Information Security Awareness Training: The Key to Optimizing Incident Response



### SECURITY IS EVERYONE'S JOB. SERIOUSLY.

Despite the great leaps in innovation we've witnessed over the past few decades, nothing beats a human being's common sense and good judgment. In fact, pragmatism, common sense and good judgment are a few values that aren't yet possible to develop in software code or artificial intelligence.

The truth is, you can't automate intuition. And much of the incident responder's job comes down to relying on your and each employee's intuition that something in that email just doesn't look quite right (as an example). Your goal is to reduce the number and impact of cases when someone's bad judgment, mistakes, and oversights open the gate to a possible breach. It could happen from clicking on an embedded link in an email, or a social engineering scam over the phone.

However it happens, you won't find the answer in some sort of magic pill, like information security awareness software downloaded to your brain a la Trinity in the Matrix. That's why you need an information security awareness training program. And yes, like many things in incident response, hearing that phrase is likely to inspire a yawn or two. And a sigh, and maybe throw in a few eyerolls too, while you're at it.

But it doesn't have to. There are a few tools, resources, and program ideas that can make information security awareness training effective and engaging for your employees. And that's what we'll cover in this chapter.

---

*what's the difference...*

---

## Incident Response Training vs. Security Awareness Training

---

FROM A 2015 SANS SURVEY



**IR TEAM TRAINING  
AND CERTIFICATION WAS CITED AS  
THE SECOND MOST COMMON AREA  
FOR IR IMPROVEMENT (57%)**

See the Survey: [Maturing and Specializing: Incident Response Capabilities Needed >](#)

We recommend having two different training programs: one for the overall employee population and one that's specifically for the incident responder. As for any specialized set of skills, incident response training should focus on all aspects of the job, the IR process, as well as the specific technical skills (programming, systems administration, and code analysis) to support whatever technologies or computing contexts that are relevant for your company.

Within this guide, we're focused on the more broad topic of security awareness training, because we've seen that improving the security awareness of everyone in your company will have a big impact on reducing the number and cost of security incidents. We're also hoping that this entire guide provides a rich foundational resource for training the members of your IR team.

---

*let's chat about...*

---

## What Exactly Do Employees Need to Know About Security? How Much Is Too Much?

---

It's a great question and one that requires we return to our primary goal for security awareness training: to reduce the number and impact of high risk security incidents. So let's focus on the biggest risk first: phishing and spearphishing.

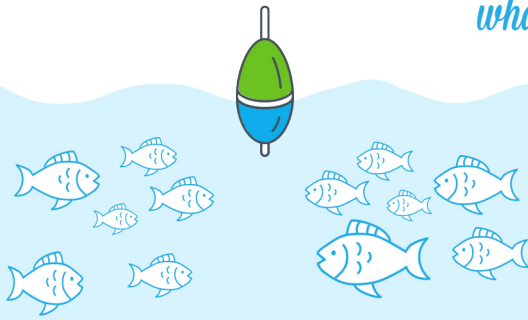
Phishing and spearphishing attacks are the most common way that employees can be manipulated into exposing your company to risk. These social engineering scams are responsible for many of the high profile breaches you've likely already heard of. The key difference between phishing and spearphishing is that spearphishing is customized and targeted to a specific employee and company, whereas phishing is more broad and automated, less sophisticated and less specific.

Defending against both types of attacks requires vigilance and awareness on the part of every employee. Remember to keep your training content and approach focused on teaching skills and good judgment vs. teaching the technical aspects of how phishing works on the back end, or esoteric topics like the differences between a rootkit, a bot, and a keystroke logger.

Show employees a few examples of phishing and spearphishing scams, and encourage them to be suspicious, even if an email may appear to be from someone they know. You may also wish to consider incorporating simulated phishing attacks to educate employees about appropriate security behaviors, measure the effectiveness of your training program, and identify any knowledge gaps.

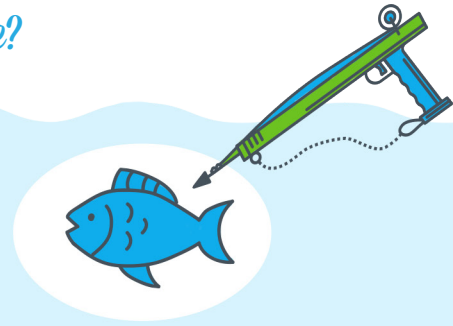


*what's the difference?*



## PHISHING

IS A BROAD, AUTOMATED ATTACK THAT IS LESS SOPHISTICATED.



## SPEARPHISHING

IS A CUSTOMIZED ATTACK ON A SPECIFIC EMPLOYEE & COMPANY

*how about...*

# Security Awareness Training Goals & Metrics

Trying to increase “awareness” around any topic is somewhat dubious. How do you measure how “aware” someone is? Hopefully by their behavior, and with any luck, by the reduction in the number of incidents and exposures you keep having to respond to.

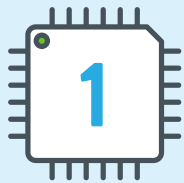
Creating good security metrics is an art unto itself, and while there are many things that generate numbers that can be tracked, good metrics don't just speak to what has been done, but how well it was done – they enable the future, not recount the past.

That said, here are a few sample indicators for increased awareness and effective training:

- ✓ **Track help desk tickets**, and expect to see an increase in employees reporting suspicious events and activity. This wouldn't necessarily be because there are more suspicious events happening, simply that employees are more sensitive to them, and feel confident in reporting them.
- ✓ **Explore non-traditional training methods** like simulation exercises to test an employee's resistance to social engineering scams, and then measure progress on a quarter-by-quarter basis. However, work with your communications team to give everyone ample heads up, to maintain trust and transparency between employees and the infosec team.

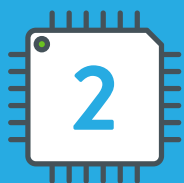
*and finally...*

# Information Security Awareness Training: Top Seven Tips



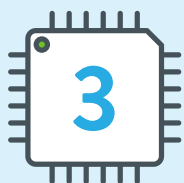
## GET EXECUTIVE BUY-IN. EARLY AND OFTEN.

It's a universal truth that the executive team sets the tone for the entire company, for every team, and every project. If you want your security awareness training program to be successful, involve the management team at every stage, and ask for their visible participation and support.



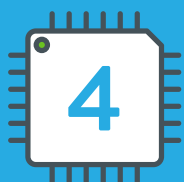
## CULTURE, CONTEXT & CONTINUITY ARE ESSENTIAL.

Encourage your management team to instill a security-aware culture where everyone sees security as a part of their job. Most insiders agree that "once and done" doesn't work for security so look for "teaching moments" in daily business operations. For example, attack simulation exercises provide the most realistic context for the actual risky situations that employees will find themselves in, and often provide one of the most valuable teaching methods.



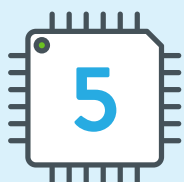
## BE CLEAR. USE REAL-WORLD SCENARIOS & APPLICATIONS.

You're trying to raise awareness and change behavior, and the more real, relevant, and compelling you can make it, the more traction you'll have. Don't overcomplicate things, and don't try to address every possible situation that could happen, because it's simply not possible.



## TRY TO AVOID A LONG BORING LIST OF "DON'T'S."

The "Just Say No" approach is old skool in a bad way, like Nancy Reagan and shoulder pads. And it doesn't work. Instead, show how to do something securely and opt for a scenario-based education approach. Remember, your goal is to instill good skills and habits vs. rote memorization. Keep the content fresh and engaging because if employees are bored, they won't remember anything.



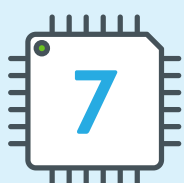
## GIVE GOOD REASONS. EXPLAIN SECURITY GUIDELINES.

Explain why user credentials are so valuable and how important it is to safeguard them. This is a much better approach than simply being frustrated when you hear user's complain about the password policy. Once an employee understands why there are certain security controls, they'll be more likely to respect them, and apply similar principles to any new "high risk" situations.



## CONSIDER ROLE-SPECIFIC RISK-BASED SECURITY TRAINING.

Training is at its most meaningful when it's tightly linked with an employee's role within the company, in the context of the risks they face in fulfilling that role. For example, someone in sales may need more training on how to protect company data and equipment while traveling than someone in engineering would.



## BE CREATIVE. INCLUDE MULTIPLE CHANNELS AND FORMATS.

There is no "one size fits all" approach to security awareness, and there's no one single training tool that will accommodate all topics or audiences. Most companies have also found that the annual "death by PowerPoint" approach no longer works. As long as it fits your company culture, think about incorporating a security awareness game at the next company retreat. Remember to use newsletters, posters, blogs, and other media as ways to get the message out.

*a quick word about*

# AlienVault Unified Security Management

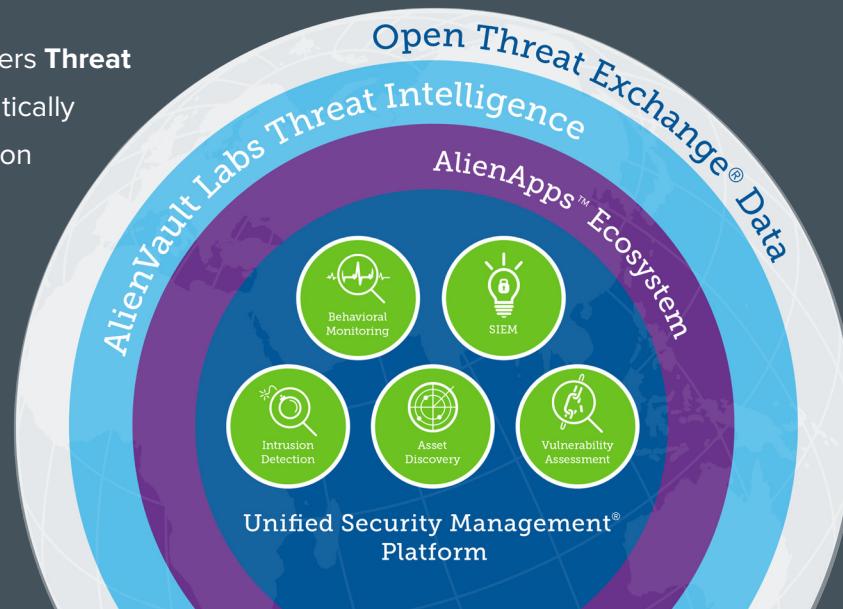
AlienVault Unified Security Management® (USM) is an all-in-one platform that accelerates and simplifies threat detection, incident response, and compliance management for IT teams with limited resources, on day one. With essential security controls and integrated threat intelligence built-in, AlienVault USM puts complete security visibility of threats affecting your network and how to mitigate them within fast and easy reach.

*A winning combination for better threat detection and incident response.*

**Multiple essential security capabilities** deliver complete security visibility across cloud, on-premises, and hybrid environments.

**AlienVault Labs Security Research Team** delivers **Threat Intelligence** updates continuously and automatically to the USM platform in the form of correlation directives, IDS signatures, IP reputation data, data source plugins, and report templates.

**Global threat data from Open Threat Exchange® (OTX™)** – the world’s largest crowd-sourced threat intelligence network – identifies malicious hosts communicating with your systems.



*Don't take our word for it – see what your peers and industry experts are saying:*



GARTNER MAGIC  
QUADRANT



CUSTOMER  
STORIES



FREE TRIAL



WATCH A  
DEMO

# Good Luck!

## REFERENCE RESOURCES:

- SANS Securing the Human - Security Awareness Planning Kit
- Tips from the US Computer Emergency Response Team
- NIST's Computer Security Incident Handling Guide



### *About AlienVault:*

AlienVault® has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management®, with the power of AlienVault's Open Threat Exchange®, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.

WWW.ALIENVAULT.COM



@ALIENVAULT