

# Ultimate Guide to Cybersecurity Incident Response



---

### In this e-guide

---

- Ultimate guide to cybersecurity incident response p. 2
- What is incident response p. 3
- Why do you need it? p. 3
- Building an IR team p. 6
- IR methodology p. 11
- Creating an incident response plan p. 11
- How, when and why to use IR tools p. 16
- A role for SOAR p. 19
- Incident response problem-solving p. 21
- Prevention is key p. 23
- Further reading p. 25

---

### In this e-guide:

Learn actionable incident response strategies that your IT and enterprise security teams can use to meet today's security threats and vulnerabilities more effectively.

**In this e-guide**

- Ultimate guide to cybersecurity incident response p. 2
- What is incident response p. 3
- Why do you need it? p. 3
- Building an IR team p. 6
- IR methodology p. 11
- Creating an incident response plan p. 11
- How, when and why to use IR tools p. 16
- A role for SOAR p. 19
- Incident response problem-solving p. 21
- Prevention is key p. 23
- Further reading p. 25

**Ultimate guide to cybersecurity incident response**

*Kevin Beaver, Principle Logic, LLC*

Here's why cybersecurity incident response is something your entire organization has to care about: Hackers are likely trying to invade your network, and security vulnerabilities likely make this easier than you would believe.

Indeed, we have evolved from a time when executive leaders were mostly disconnected from the information security function to an era where **cybersecurity is top of mind** for many such former naysayers. And for good reason: There's likely not a day that goes by that your organization isn't under attack or otherwise exposed to IT-related security risks.

**Security threats and vulnerabilities**, and the subsequent incidents and breaches that they can lead to, affect organizations of all kinds. Literally every business -- both large and small and across every industry -- is a target for criminal hackers and careless employees alike. The question is: What are you doing about it?

This is where **incident response (IR)** comes into play.

In this e-guide

- Ultimate guide to cybersecurity incident response p. 2
- What is incident response p. 3
- Why do you need it? p. 3
- Building an IR team p. 6
- IR methodology p. 11
- Creating an incident response plan p. 11
- How, when and why to use IR tools p. 16
- A role for SOAR p. 19
- Incident response problem-solving p. 21
- Prevention is key p. 23
- Further reading p. 25

## What is incident response?

Incident response is the process of detecting security events that affect network resources and information assets and then taking the appropriate steps to evaluate and clean up what has happened. Cybersecurity incident response is critical to today's businesses because, simply put, there is so much to lose. From the simplest of malware infections to unencrypted laptops that are lost or stolen to compromised login credentials and database exposures, both the short- and long-term ramifications of these incidents can have a lasting impact on the business.

## Why do you need it?

Security breaches can require notification, resulting in customer distrust, reputation loss, regulatory fines, legal fees and cleanup costs. And these can all come at once -- in ways that even the most financially secure of businesses can have trouble absorbing.

**446.5 million**  
Reported number of sensitive consumer records exposed in 2018.

SOURCE: IDENTITY THEFT RESOURCE CENTER (ITRC)  
©2019 TECHTARGET. ALL RIGHTS RESERVED

---

## In this e-guide

---

Ultimate guide to cybersecurity incident response	p. 2
What is incident response	p. 3
Why do you need it?	p. 3
Building an IR team	p. 6
IR methodology	p. 11
Creating an incident response plan	p. 11
How, when and why to use IR tools	p. 16
A role for SOAR	p. 19
Incident response problem-solving	p. 21
Prevention is key	p. 23
Further reading	p. 25

Networks, software and end users can only reach a certain level of resilience. Oversights will occur, and mistakes will happen. What matters is what you have done, in advance, to minimize the impact of a security incident on your organization. You can't prevent hackers from existing, but you can be proactive in prevention and response. That's why having a functional team, the proper technologies and a well-written incident response plan are essential for being able to respond to such events in a prompt and professional manner.

An important aspect of understanding incident response is fleshing out the necessary elements in your security program to differentiate between threats and vulnerabilities:

- **Threat:** An indication or stimulus, such as a criminal hacker or dishonest employee, that's looking to exploit a vulnerability for ill-gotten gains.
- **Vulnerability:** A weakness in a computer system, a business process or people that can be exploited.

Threats exploit vulnerabilities, which, in turn, create business risk. The potential consequences include unauthorized access to sensitive information assets, identity theft, systems taken offline, and legal and compliance violations.

Related terms include the following:

- **Breach:** An incident where sensitive information, such as intellectual property or customer records, is exposed.
- **Hack** (sometimes referred to as an *attack*): The act of a criminal hacker (or hackers) or a rogue user doing something such as taking your systems offline, planting or spreading malware, or stealing information assets.



**In this e-guide**

- ▶ [Ultimate guide to cybersecurity incident response](#) p. 2
- ▶ [What is incident response](#) p. 3
- ▶ [Why do you need it?](#) p. 3
- ▶ [Building an IR team](#) p. 6
- ▶ [IR methodology](#) p. 11
- ▶ [Creating an incident response plan](#) p. 11
- ▶ [How, when and why to use IR tools](#) p. 16
- ▶ [A role for SOAR](#) p. 19
- ▶ [Incident response problem-solving](#) p. 21
- ▶ [Prevention is key](#) p. 23
- ▶ [Further reading](#) p. 25

- **Incident:** An attack that's successful in draining computing resources, obtaining unauthorized access, or otherwise putting information assets and related network resources at risk.
- **Network (or security) event:** A term that lawyers often use to refer to potential security issues that haven't yet been confirmed or the details of which aren't ready to be released to outside parties or the public.

Attacks don't always lead to incidents, and incidents don't always lead to breaches. They're all considered network events and are often played down until the details can be obtained. It all depends on what took place and what can be determined after the fact.

**Take the proactive approach to incident response**












Incident response requires taking a systematic approach to monitoring, detecting and countering network security events to limit damage—and it doesn't happen accidentally. Get ahead of hackers with these five steps.

- 1 Build a team.
- 2 Create a plan.
- 3 Build a framework.
- 4 Decide on the right tools.
- 5 Anticipate problems/solutions.

ART BY ILLUSTRATION/GETTY IMAGES ©2019 TECHTARGET. ALL RIGHTS RESERVED. TechTarget

---

## In this e-guide

 <a href="#">Ultimate guide to cybersecurity incident response</a>	p. 2
 <a href="#">What is incident response</a>	p. 3
 <a href="#">Why do you need it?</a>	p. 3
 <a href="#">Building an IR team</a>	p. 6
 <a href="#">IR methodology</a>	p. 11
 <a href="#">Creating an incident response plan</a>	p. 11
 <a href="#">How, when and why to use IR tools</a>	p. 16
 <a href="#">A role for SOAR</a>	p. 19
 <a href="#">Incident response problem-solving</a>	p. 21
 <a href="#">Prevention is key</a>	p. 23
 <a href="#">Further reading</a>	p. 25

The purpose of this guide is to give IT and enterprise security teams actionable strategies to meet today's security threats and vulnerabilities more effectively. This is regardless of whether you have an existing IR program or you're just getting started. It can also serve to help [get business executives on board](#) with this critical function of a well-run information security program and highlight ways users may need more security training. You can use this information to improve your incident response capabilities, share it with executive management to further their understanding and get buy-in on your security initiatives, and even use it as a basis for your policies and ongoing user security awareness and training efforts.

---

## Building an IR team

A good incident response program starts with [building a great team](#). Without the right people, security policies, processes and tools mean very little. An IR team is made up of a cross-functional group of people from diverse parts of the business, including IT and security, operations, legal and public relations. One or more of these roles could -- and should -- be at the [executive management level](#). The reason for this is to ensure the highest level of decision-making and that the business's best interests are kept in mind.

### What does an IR team do?

The overall goal of an [incident response team](#) should be to detect and respond to security incidents in order to minimize their impact on the business. Such teams are often referred to as a computer security incident response team ([CSIRT](#)) or a computer

---

## In this e-guide

---

Ultimate guide to cybersecurity incident response	p. 2
What is incident response	p. 3
Why do you need it?	p. 3
Building an IR team	p. 6
IR methodology	p. 11
Creating an incident response plan	p. 11
How, when and why to use IR tools	p. 16
A role for SOAR	p. 19
Incident response problem-solving	p. 21
Prevention is key	p. 23
Further reading	p. 25

emergency response (or readiness) team ([CERT](#)). A larger group of IR professionals are often pulled together into a [security operations center](#) (SOC), whose scope is broader than incident response. The name of your IR team is largely irrelevant because its goals are the same.

Whatever the name, the IR team should be working to support its role in the overall incident response plan, which itself should complement the goals of your information security program and overall business. Team goals might include working on response times and impact minimization, conducting periodic meetings and performing tabletop exercises. In order for these goals to work, they need to be very specific, written in the present tense and include steps that must be accomplished along with deadlines to help with accountability. The following are examples of IR team goals that might be developed by the team itself or an overarching security committee:

- We develop metrics for analyzing our IR program initiatives that involve monitoring and alerting, communication among team members, and technology evaluations.
- We update our IR plan document periodically and consistently.
- We create and execute three separate tabletop exercises for IR simulations.
- We engage our security committee and executive management to report on incidents, actions taken and additional improvements needed for incident response.

The IR team -- or program manager -- would flesh out each of these goals with specific steps needed to meet each one, along with deadlines so that everyone on the team knows what's expected and what to aim for.



**In this e-guide**

- Ultimate guide to cybersecurity incident response p. 2
- What is incident response p. 3
- Why do you need it? p. 3
- Building an IR team p. 6
- IR methodology p. 11
- Creating an incident response plan p. 11
- How, when and why to use IR tools p. 16
- A role for SOAR p. 19
- Incident response problem-solving p. 21
- Prevention is key p. 23
- Further reading p. 25



Another thing to keep in mind with your incident response team goals is to make sure that they are both reasonable and achievable and, most importantly, that they are being reviewed and followed. Otherwise, they can become an afterthought and evolve into a liability rather than an asset. It's even more complicated if, after an incident or confirmed breach, someone finds that documented procedures were nonexistent or not followed at all.

**In this e-guide**

- [Ultimate guide to cybersecurity incident response](#) p. 2
- [What is incident response](#) p. 3
- [Why do you need it?](#) p. 3
- [Building an IR team](#) p. 6
- [IR methodology](#) p. 11
- [Creating an incident response plan](#) p. 11
- [How, when and why to use IR tools](#) p. 16
- [A role for SOAR](#) p. 19
- [Incident response problem-solving](#) p. 21
- [Prevention is key](#) p. 23
- [Further reading](#) p. 25

An essential part of cybersecurity incident response is understanding the various team member roles and responsibilities. After all, what good are goals if you don't have the right people on board, or you have people working on the team but their expectations are not clear? At a minimum, you should outline in your IR plan, or elsewhere, specific roles and responsibilities.

**Incident response skills**

The IR team should include the following:

- Technical team: IT and security team members.
- Executive sponsor: A senior executive charged with overseeing information security.
- Incident response coordinator: The person responsible for ongoing management of the team and incidents.
- Media relations coordinator: Your PR representative in charge of interfacing with the news media and related outlets once a breach occurs.
- Forensic analyst: A forensics expert internal to the company or an outside adviser.
- Outside consultant: A third-party information security or incident response expert.
- Legal counsel: Your corporate attorney or outside law firm that would represent your organization as needed for incidents and breaches.

Incident response requires a number of skills. At the heart of an IR team is the core group of technical staff and [incident responders](#) who defend an organization against cyberthreats. These members are skilled at security and can execute on tasks such as

---

### In this e-guide

---

Ultimate guide to cybersecurity incident response	p. 2
What is incident response	p. 3
Why do you need it?	p. 3
Building an IR team	p. 6
IR methodology	p. 11
Creating an incident response plan	p. 11
How, when and why to use IR tools	p. 16
A role for SOAR	p. 19
Incident response problem-solving	p. 21
Prevention is key	p. 23
Further reading	p. 25

monitoring the network for vulnerabilities and breaches and taking the appropriate measures where necessary.

As for incident responders, these team members use data to spot and assess the scope or urgency of incidents and perform other ongoing IR duties. They may also report on trends, educate the organization's users and liaise with law enforcement. There are [specific questions that can help organizations](#) better hire these team members.

But technical skills are not all that's required for successful incident response. As noted above, a solid IR team will need cross-functional members who can execute on nontechnical tasks, such as talking with the media and responding to legal issues. The actual titles for each of these roles can vary from organization to organization depending on your existing staff structure, staff expertise and your specific business needs. The important thing is that you have the right people on board.

In terms of team building, rather than pulling people into your IR team who may not want to be there, seek out those in the organization who are interested in the topic and are eager to add value to this critical aspect of security. Each IT and security team member has his or her own interests, and incident response may not be one of them. Moreover, it's critical to have both technical and nontechnical people on your IR team. The technical people will know the network environment and can help dig into the details in system logs, network packet captures, vulnerability scanner reports and the like. Nontechnical people can help lead the oversight and team communications required to keep everyone in the know, ask the not-so-obvious questions, and help in

---

## In this e-guide

---

- [Ultimate guide to cybersecurity incident response](#) p. 2
- [What is incident response](#) p. 3
- [Why do you need it?](#) p. 3
- [Building an IR team](#) p. 6
- [IR methodology](#) p. 11
- [Creating an incident response plan](#) p. 11
- [How, when and why to use IR tools](#) p. 16
- [A role for SOAR](#) p. 19
- [Incident response problem-solving](#) p. 21
- [Prevention is key](#) p. 23
- [Further reading](#) p. 25

the decision-making process so that business interests are properly represented. You might consider linking to an [overall business communication plan](#) that may exist.

---

## IR methodology

An incident response plan is a go-to document for when the going gets rough with security issues. It outlines the *who, what, when, why* and *how* of addressing security events, incidents, and, once confirmed, breaches. It's important because the last thing you need to be doing under duress is figuring out how to respond to these challenges. In fact, when you don't have a documented plan, you'll be reacting. And when you react, you lose your ability to reason. You're flying by the seat of your pants. You can't think clearly, and you're quite likely not going to make good decisions. By having a documented IR plan, you can respond with clarity and direction and avoid letting emotions drive your response efforts.

---

## Creating an incident response plan

An incident response plan should be developed by the team or IR coordinator in advance and should contain the components detailed in the chart below.

**In this e-guide**

- [Ultimate guide to cybersecurity incident response](#) p. 2
- [What is incident response](#) p. 3
- [Why do you need it?](#) p. 3
- [Building an IR team](#) p. 6
- [IR methodology](#) p. 11
- [Creating an incident response plan](#) p. 11
- [How, when and why to use IR tools](#) p. 16
- [A role for SOAR](#) p. 19
- [Incident response problem-solving](#) p. 21
- [Prevention is key](#) p. 23
- [Further reading](#) p. 25

Incident plan element	Purpose and scope
<b>Overview</b>	Introduces the plan; details high-level goals, the scope of what's covered and assumptions that have been considered.
<b>Outline of roles and responsibilities</b>	Lists and discusses the duties and expectations of each of the team members.
<b>Detailed list of incidents requiring action</b>	Outlines the specific threats, exploits and situations that require formal incident response actions. The possibilities are endless, but could include denial-of-service attacks, malware infections, email phishing and lost or stolen laptops. <b>Note:</b> This is arguably the most important part of the incident response plan.
<b>Detection, investigation and containment procedures</b>	The beginning of the actual incident response procedures that you plan to use; this includes directives on tasks such as analyzing the situations, notifying team members, getting outside parties involved, securing the network, confirming the incident, gathering evidence and reporting on findings.

**In this e-guide**

- [Ultimate guide to cybersecurity incident response](#) p. 2
- [What is incident response](#) p. 3
- [Why do you need it?](#) p. 3
- [Building an IR team](#) p. 6
- [IR methodology](#) p. 11
- [Creating an incident response plan](#) p. 11
- [How, when and why to use IR tools](#) p. 16
- [A role for SOAR](#) p. 19
- [Incident response problem-solving](#) p. 21
- [Prevention is key](#) p. 23
- [Further reading](#) p. 25

<b>Incident plan element</b>	Purpose and scope
<b>Eradication steps</b>	Provides the general steps for cleaning up the incident and may include network traffic and system log analysis, forensics review and subsequent vulnerability testing to confirm resolution.
<b>The recovery phase</b>	Details tasks in the recovery phase, such as reinstalling or reimaging hosts, resetting passwords, and adjusting firewall rules and related network configurations.
<b>Breach notification</b>	Outlines the <i>how</i> and <i>when</i> to alert those impacted by a confirmed breach as required by contracts or law.
<b>Follow-up tasks</b>	Discusses additional reports, enhanced documentation and lessons learned that might come out of this phase.
<b>Call list (in the appendix)</b>	Provides contact information for incident response team members and involved outside vendors, such as internet service providers and cloud service providers.



**In this e-guide**

- ▶ [Ultimate guide to cybersecurity incident response](#) p. 2
- ▶ [What is incident response](#) p. 3
- ▶ [Why do you need it?](#) p. 3
- ▶ [Building an IR team](#) p. 6
- ▶ [IR methodology](#) p. 11
- ▶ [Creating an incident response plan](#) p. 11
- ▶ [How, when and why to use IR tools](#) p. 16
- ▶ [A role for SOAR](#) p. 19
- ▶ [Incident response problem-solving](#) p. 21
- ▶ [Prevention is key](#) p. 23
- ▶ [Further reading](#) p. 25

Incident plan element	Purpose and scope
<b>Testing scenarios (appendix)</b>	Outlines specific testing scenarios that have been or will be carried out.
<b>Revision history (appendix)</b>	Outlines details on plan updates and improvements, including who did it and when it was done.

Everyone's plan will look a little different depending on specific needs. However, the essentials covered by this template are standard and should be included in every organizations' plan. There are [IR best practices](#) and other resources available from organizations that you might consider integrating into your plan.

[NIST](#), [US-CERT](#), [ISACA](#) and [ISO/IEC](#) all provide [frameworks that organizations can use](#) as guidance. For example, the NIST "Computer Security Incident Handling Guide" includes an incident response framework in the form of an IR lifecycle -- preparation; detection and analysis; containment, eradication and recovery; and post-incident activity.

Additional frameworks are available from the SANS Institute, the Institute of Electrical and Electronics Engineers, the Internet Engineering Task Force and the European Union Agency for Network and Information Security.

---

### In this e-guide

---

- [Ultimate guide to cybersecurity incident response](#) p. 2
- [What is incident response](#) p. 3
- [Why do you need it?](#) p. 3
- [Building an IR team](#) p. 6
- [IR methodology](#) p. 11
- [Creating an incident response plan](#) p. 11
- [How, when and why to use IR tools](#) p. 16
- [A role for SOAR](#) p. 19
- [Incident response problem-solving](#) p. 21
- [Prevention is key](#) p. 23
- [Further reading](#) p. 25

An incident response plan should not be combined with documents on other organizational security plans and procedures, such as such as an overview of security policies or disaster recovery and business continuity plans. Instead, it works best as a stand-alone document that all your incident response team members know about and have easy access to -- both on the network and in hard-copy form. In addition to consulting frameworks from the organizations mentioned above, it can help to start with an [IR plan template](#) to guide you in the right direction.

[Creating an incident response plan](#) requires the expertise and input of all your incident response team members. A good way to go about establishing a plan -- or, even, fleshing out your existing one -- is to divvy up the various parts to the necessary team members. Once everyone has fleshed out their section, the incident response team can pull it all together into a single document and start working on editing and forming the final version. Keep in mind that your incident response plan is not unlike any given security policy; it's a work in progress. So, you want to make sure that it's reviewed periodically and adjusted appropriately as changes to your network, security and business come about.

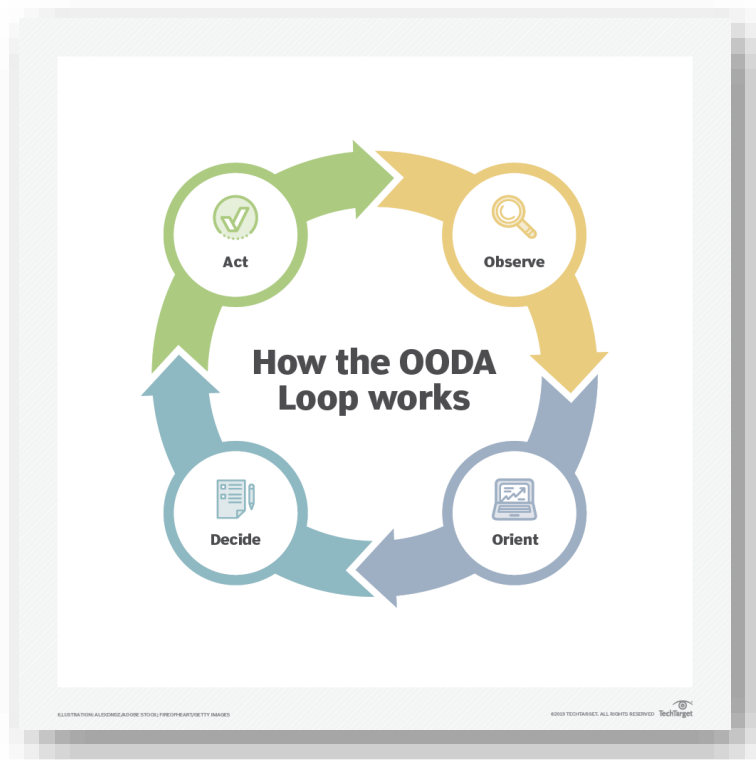
To put a fine point on it: Your IR plan needs to be kept current, or it cannot keep your organization safe.

In this e-guide

- Ultimate guide to cybersecurity incident response p. 2
- What is incident response p. 3
- Why do you need it? p. 3
- Building an IR team p. 6
- IR methodology p. 11
- Creating an incident response plan p. 11
- How, when and why to use IR tools p. 16
- A role for SOAR p. 19
- Incident response problem-solving p. 21
- Prevention is key p. 23
- Further reading p. 25

## How, when and why to use IR tools

If information security is considered a strategic function of the business (and it often is), then incident response would be a tactical component of the security program. A military concept associated with the decisions and actions needed for effective incident response -- dubbed the **OODA loop** -- is a cycle where you *observe*, *orient*, *decide* and *act*. The essence of the OODA loop is to use situational awareness and information to see impactful events, such as security incidents, unfold so you can quickly respond and gain an advantage toward thwarting the threat. This enables you to minimize the impact of threats on your business.



**In this e-guide**

- [Ultimate guide to cybersecurity incident response](#) p. 2
- [What is incident response](#) p. 3
- [Why do you need it?](#) p. 3
- [Building an IR team](#) p. 6
- [IR methodology](#) p. 11
- [Creating an incident response plan](#) p. 11
- [How, when and why to use IR tools](#) p. 16
- [A role for SOAR](#) p. 19
- [Incident response problem-solving](#) p. 21
- [Prevention is key](#) p. 23
- [Further reading](#) p. 25

The OODA loop can be utilized as an overall approach to incident response and can also help define which security tools you use in the process. Whether from the functions of prevention, detection or response, there are [numerous incident response tools](#) that can be used in this regard. For example, the visibility provided by packet analysis, system resource examination and file integrity monitoring are technologies you can use to fulfill the *observe* component of the OODA loop. Technologies that use real-time threat indicators and threat intelligence can provide context on attacks and be used to fulfill the *orient* component of the OODA loop. The *decide* component could be fulfilled by tools that provide forensic details, including replays of what happened in order to shed light on context and technical information. This can help you make more informed decisions on what to do -- or what not to do -- during the incident response process. Finally, the *act* component of the OODA loop can be fulfilled by activities such as blocking, redirecting or quarantining threats in order to minimize their effects on your network and information assets.

While cybersecurity incident response is a *process*, technology can automate certain functions to help minimize the time involved and eliminate errors. [IR-focused technology vendors](#) provide tools for functions such as the following:

- net flow and traffic analysis;
- vulnerability management;
- security incident and event management;
- [endpoint detection and response](#);
- firewall, intrusion prevention and denial-of-service mitigation; and
- forensic analysis.

**In this e-guide**

- [Ultimate guide to cybersecurity incident response](#) p. 2
- [What is incident response](#) p. 3
- [Why do you need it?](#) p. 3
- [Building an IR team](#) p. 6
- [IR methodology](#) p. 11
- [Creating an incident response plan](#) p. 11
- [How, when and why to use IR tools](#) p. 16
- [A role for SOAR](#) p. 19
- [Incident response problem-solving](#) p. 21
- [Prevention is key](#) p. 23
- [Further reading](#) p. 25

Most technology products in this space are commercial, so you'll need the budget -- sometimes a big one -- for both capital and operating expenditures associated with these tools. As an alternative, there are open source software offerings for most of these areas. You'll have to decide whether open source can meet your specific business requirements and what level of effort will be involved in doing so. You must also consider whether the open source software will be around over the long haul after you've invested so much in establishing your incident response efforts.

You can't simply depend on IR tools to run your entire incident response program.

Of course, as with any new technical control you put in place, you'll need to make sure you have the staff and expertise. Having the necessary resources is critical not only in terms of initial design and implementation, but also with day-to-day administration, troubleshooting and so on.

One final point: Does it make sense to fully integrate the OODA loop with your incident response efforts? It depends. You might at least consider it as a guideline for your approach to incident response and customize your methodology according to your needs. Similarly, you can't simply depend on IR tools to run your entire incident response program. The reality is, the success of the IR function depends on many factors, such as business culture, security buy-in, network design, budget and people. As with your incident response plan document, your IR methodology and tools are going to be unique based on your specific business requirements. If you follow the core OODA steps and [use incident response tools where appropriate](#), that will put you at an advantage -- ahead of the curve -- and that's where you need to be.

---

## In this e-guide

---

Ultimate guide to cybersecurity incident response	p. 2
What is incident response	p. 3
Why do you need it?	p. 3
Building an IR team	p. 6
IR methodology	p. 11
Creating an incident response plan	p. 11
How, when and why to use IR tools	p. 16
A role for SOAR	p. 19
Incident response problem-solving	p. 21
Prevention is key	p. 23
Further reading	p. 25

---

## A role for SOAR

Security orchestration, automation and response (**SOAR**) is a stack of compatible software that enables cybersecurity professionals to collect data about security threats and automatically respond to them. **SOAR performs the following three main functions:**

- connects and coordinates heterogeneous tool sets and defines incident analysis parameters and processes;
- automatically triggers specific workflows, tasks and triages based on those parameters; and
- accelerates general and targeted responses by enabling a single view for analysts to access, query and share threat intelligence.

SOAR and SIEM may seem to play similar roles in the SOC, but **they serve different purposes**. SIEMs take in log and event data from traditional infrastructure component sources, while SOAR platforms extend that capability, pulling information from a variety of sources, including endpoint security software and third-party sources. SOAR platforms are also more sophisticated in their ability to orchestrate and automate alert responses.

**SOAR has an array of use cases**, including the following:

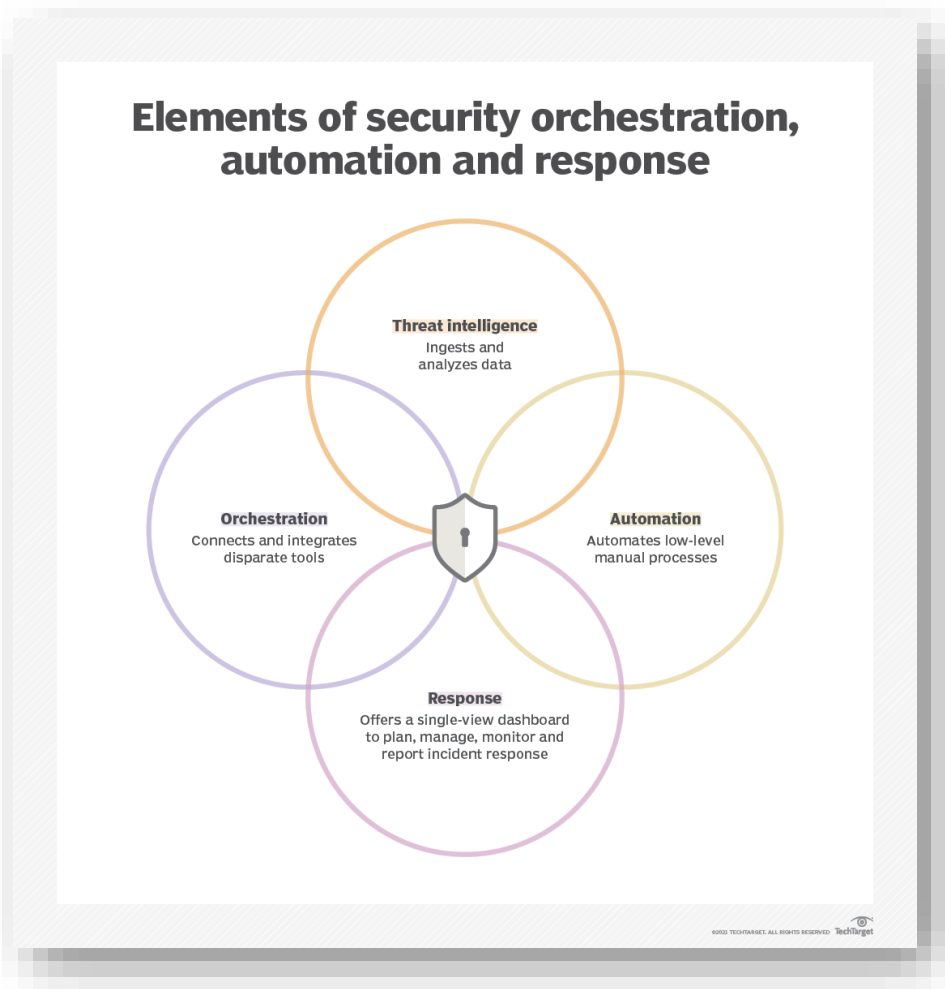
- threat intelligence coordination;
- case management;
- vulnerability management;



**In this e-guide**

- Ultimate guide to cybersecurity incident response p. 2
- What is incident response p. 3
- Why do you need it? p. 3
- Building an IR team p. 6
- IR methodology p. 11
- Creating an incident response plan p. 11
- How, when and why to use IR tools p. 16
- A role for SOAR p. 19
- Incident response problem-solving p. 21
- Prevention is key p. 23
- Further reading p. 25

- automated enrichment for remediation;
- threat hunting; and
- incident response.



---

## In this e-guide

---

Ultimate guide to cybersecurity incident response	p. 2
What is incident response	p. 3
Why do you need it?	p. 3
Building an IR team	p. 6
IR methodology	p. 11
Creating an incident response plan	p. 11
How, when and why to use IR tools	p. 16
A role for SOAR	p. 19
Incident response problem-solving	p. 21
Prevention is key	p. 23
Further reading	p. 25

---

## Incident response problem-solving

Problem-solving is a key part of incident response. Even though the OODA loop is about decision-making, it's important to not get caught up in the process of it or any other IR methodology. It's easy to get sidetracked and lose sight of what's important, and that's *prioritization*. Looking at this from the perspective of incidents requiring actions discussed above, you must be able to prioritize what to focus your efforts on and know which ones you can ignore. You go about doing this by considering which security events are urgent, which are important and how you'll need to respond to the various scenarios. The best way to do this is to view security events, incidents and confirmed breaches in terms of the following:

1. What's urgent but not important?
2. What's important but not urgent?
3. What's both urgent and important?

An example of an *urgent but not important* issue would be a malware infection on a branch office sales workstation that only connects to the office network or internet via guest Wi-Fi. An example of an *important but not urgent* issue is a new, recently imaged laptop that is lost but that doesn't yet contain any business-related information.

Examples of an *urgent and important* situation is a distributed denial-of-service attack against an e-commerce website, a malware infection affecting production servers and phishing attempts against executives that have led to the compromise of network credentials. Urgent and important scenarios are those where something bad is

**In this e-guide**

- [Ultimate guide to cybersecurity incident response](#) p. 2
- [What is incident response](#) p. 3
- [Why do you need it?](#) p. 3
- [Building an IR team](#) p. 6
- [IR methodology](#) p. 11
- [Creating an incident response plan](#) p. 11
- [How, when and why to use IR tools](#) p. 16
- [A role for SOAR](#) p. 19
- [Incident response problem-solving](#) p. 21
- [Prevention is key](#) p. 23
- [Further reading](#) p. 25

happening to a critical business resource or asset and you know that something must be done quickly.

The average small business, midmarket corporation or large enterprise has countless vulnerabilities that have yet to be acknowledged.

You'll find that [many security issues you're forced to address](#) fall into the first two categories above. Although they may need to be addressed in some way, they'll likely only serve as a distraction. This is why you must be good at filtering out the noise and focusing on the things that really matter for your particular environment. The third category -- both urgent and important -- is where you'll find most of your incident response resources should be dedicated. What's important is that you take the bigger picture into account and [address the security events that are most impactful](#) towards your critical network resources and information assets.

In today's technology-centric world where decisions are often made for us, it's becoming more of a struggle to find IT and security staff who can truly solve problems, especially when under the pressure of a security event. As it relates to incident response in your security program as a whole, ensure that problem-solving involves the proper areas, which include defining the problem, determining all possible solutions, deciding on the best solution and then taking purposeful action.

**In this e-guide**

- ▶ [Ultimate guide to cybersecurity incident response](#) p. 2
- ▶ [What is incident response](#) p. 3
- ▶ [Why do you need it?](#) p. 3
- ▶ [Building an IR team](#) p. 6
- ▶ [IR methodology](#) p. 11
- ▶ [Creating an incident response plan](#) p. 11
- ▶ [How, when and why to use IR tools](#) p. 16
- ▶ [A role for SOAR](#) p. 19
- ▶ [Incident response problem-solving](#) p. 21
- ▶ [Prevention is key](#) p. 23
- ▶ [Further reading](#) p. 25

## Prevention is key

**Prevention is critical to incident response.** You create a great IR program so you are ready to mitigate cyberattacks and deal with security mishaps and exploits. However, your first line of defense is to keep your network safe and your users empowered and security-aware. The security incidents that can create the most damage are those that exploit the gullibility of your network users, malware, and misconfigured computer systems and software that can be exploited for further enumeration and penetration. The average small business, midmarket corporation or large enterprise has countless vulnerabilities that have yet to be acknowledged, much less addressed. Knowing what we know today and having such advanced tools at our disposal, there's simply no reason to offer low-hanging fruit to hackers. Weak passwords, missing patches and unsecured information can easily lead to an incident or confirmed breach. Unfortunately, that's typically how incidents and breaches occur, so it's up to the incident response team or the security committee to determine where the gaps and opportunities lie and then vow to not let them lead to the downfall of your business.

Rather than implementing more paperwork and technical controls policies, processes and technologies -- many of which can serve as mere bureaucracy or a false sense of security -- what's often needed most is *discipline*. The discipline to acknowledge security threats and vulnerabilities. The discipline to acknowledge weaknesses in your information security program, including incident response. The discipline to take reasonable steps to prevent *most* incident scenarios. And the discipline to have the

**In this e-guide**

- Ultimate guide to cybersecurity incident response p. 2
- What is incident response p. 3
- Why do you need it? p. 3
- Building an IR team p. 6
- IR methodology p. 11
- Creating an incident response plan p. 11
- How, when and why to use IR tools p. 16
- A role for SOAR p. 19
- Incident response problem-solving p. 21
- Prevention is key p. 23
- Further reading p. 25

proper visibility and control in place to [minimize the impact of the exploits](#) that do get through.

Incident response is not just an IT and security issue that's overseen and executed by technical professionals. Instead, it's a core business function that's arguably as important as anything on the legal, financial or operations side of the business. Business leaders must understand that information security is a critical underpinning of the enterprise that must be supported at the highest of levels. Unless and until critical aspects of security are mastered, including incident response, it's a matter of time before the going gets rough, the questioning begins and intrusive investigations ensue. It's unreasonable to expect a perfect security program. Still, it's better to get started on improving your incident response efforts now before you're forced to.

**Further reading**

**In this e-guide**

- Ultimate guide to cybersecurity incident response p. 2
- What is incident response p. 3
- Why do you need it? p. 3
- Building an IR team p. 6
- IR methodology p. 11
- Creating an incident response plan p. 11
- How, when and why to use IR tools p. 16
- A role for SOAR p. 19
- Incident response problem-solving p. 21
- Prevention is key p. 23
- Further reading p. 25

**About SearchSecurity**

IT security pros turn to SearchSecurity.com for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security certification training resources, security standard compliance, webcasts, white papers, podcasts, Security Schools, a selection of highly focused security newsletters and more -- all at no cost.

**For further reading visit us at**

[www.SearchSecurity.com](http://www.SearchSecurity.com)

Images; Fotolia

©2021 TechTarget. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher.