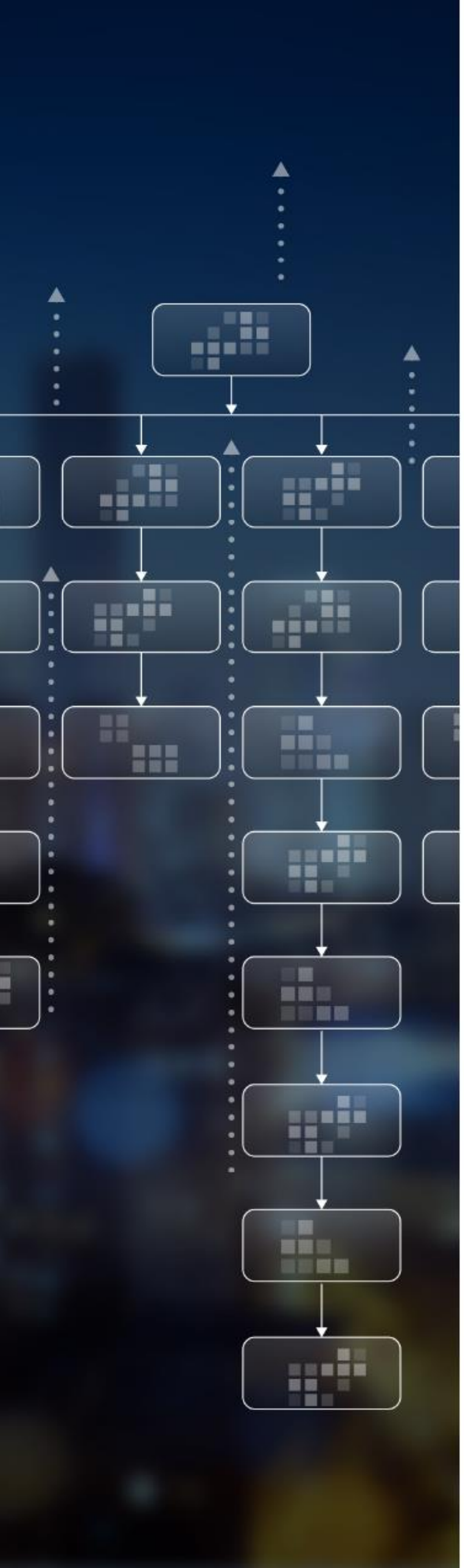


What is incident response? Plans, teams and tools

April 2023

In this guide:

Incident response is an organized, strategic approach to detecting and managing cyberattacks in ways that limit damage, recovery time and costs. This guide shows how to establish an incident response strategy. It then outlines steps needed to craft a plan and put in place the team and tools required to minimize the fallout when a cyberattack hits your organization.

In this guide:

What is incident response? Plans, teams and tools

ALISSA IREI, SENIOR SITE EDITOR

Strictly speaking, incident response is a subset of incident management. *Incident management* is an umbrella term for an enterprise's broad handling of cyber attacks, involving diverse stakeholders from the executive, legal, HR, communications and IT teams. Incident response is the part of incident management that handles technical cybersecurity tasks and considerations.

Many experts use the terms *incident response* and *incident management* interchangeably, however, because both incident management and incident response strategies work to ensure business continuity in the face of a security crisis, such as a data breach.

WHY IS INCIDENT RESPONSE IMPORTANT?

Today, Benjamin Franklin might say the only certainties are death, taxes and cyber attacks. Research suggests critical security incidents are all but inevitable, thanks to both criminal ingenuity on the attacker's side and human error on the user's side. A reactive, disorganized response to an attack gives bad actors the upper hand and puts the business at greater risk.

At worst, the financial, operational and reputational damage from a major security incident could force an organization to go out of business.

On the other hand, a cohesive, well-vetted incident response strategy that follows incident response best practices limits fallout and positions the business to recover as quickly as possible.

TYPES OF SECURITY INCIDENTS

In developing incident response strategies, it's important to first understand how security vulnerabilities, threats and incidents relate.

A *vulnerability* is a weakness in the IT or business environment. A *threat* is an entity -- whether a malicious hacker or a company insider -- that aims to exploit a vulnerability in an attack. To qualify as an *incident*, an attack must succeed in accessing enterprise resources or in otherwise putting them at risk. Finally, a *data breach* is an incident in which attackers successfully compromise sensitive information, such as personally identifiable information or intellectual property.

When it comes to cybersecurity, an ounce of prevention is worth a pound of cure. Experts say organizations should fix known vulnerabilities and proactively develop response strategies for dealing with common security incidents. These include the following:

- Unauthorized attempts to access systems or data.
- Privilege escalation attacks.
- Insider threats.
- Phishing attacks.
- Malware attacks.
- Denial-of-service (DoS) attacks.
- Man-in-the-middle attacks.
- Password attacks.
- Web application attacks.
- Advanced persistent threats.

But since all security events are not equally serious -- and enterprises simply do not have the resources to aggressively address each and every one -- incident response requires prioritization. Weigh an incident's urgency and importance to determine if it warrants a full-fledged response. For example, an active ransomware attack is both urgent (i.e., time-sensitive) and important (i.e., it puts critical IT assets and business continuity at risk). Such an attack logically warrants a major, expedited response.

Learn more about the top cybersecurity threats enterprises face today.

WHAT IS AN INCIDENT RESPONSE PLAN?

An incident response plan is an organization's go-to set of documentation that details the following:

- **What.** Which threats, exploits and situations qualify as actionable security incidents, and what to do when they occur.
- **Who.** In the event of a security incident, who is responsible for which tasks and how others can contact them.
- **When.** Under what circumstances team members should perform certain tasks.
- **How.** Specifically how team members should complete those tasks.

An incident response plan acts as a detailed, authoritative map, guiding responders from initial detection, assessment and triage of an incident to its containment and resolution.

HOW TO CREATE AN INCIDENT RESPONSE PLAN

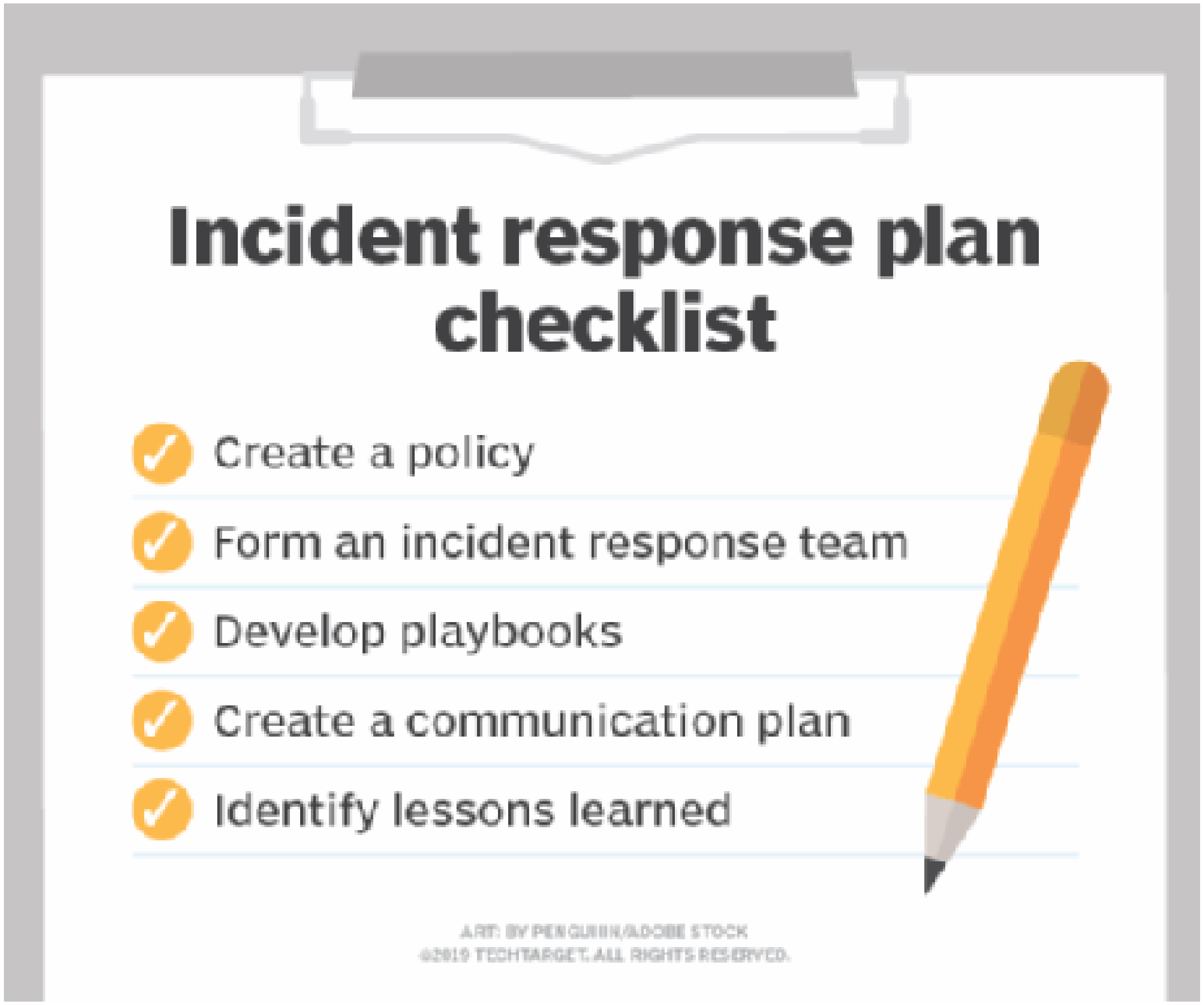
Successful incident response requires proactively drafting, vetting and testing plans *before* crisis strikes. Best practices include the following:

1. **Establish a policy.** An incident remediation and response policy should be an evergreen document describing general, high-level incident-handling priorities. A good

policy empowers incident responders and guides them in making sound decisions when the proverbial excrement hits the fan.

2. **Build an incident response team.** An incident response plan is only as strong as the people involved. Establish who will handle which tasks, and ensure everyone has adequate training to fulfill their roles and responsibilities.
3. **Create playbooks.** Playbooks are the lifeblood of incident response. While an incident response policy offers a high-level view, playbooks get into the weeds, outlining standardized, step-by-step actions responders should take in specific scenarios. Playbook benefits include greater consistency, efficiency and effectiveness -- in both incident response and incident responder training. Learn how to create playbooks.
4. **Create a communication plan.** An incident response plan can't succeed without a solid communication plan among diverse stakeholders. These may include the incident response, executive, communications, legal and HR teams, as well as customers, third-party partners, law enforcement and the general public.

In this guide:



Incident response plan checklist

- ✓ Create a policy
- ✓ Form an incident response team
- ✓ Develop playbooks
- ✓ Create a communication plan
- ✓ Identify lessons learned

ART: BY PENGUIIN/ADOBE STOCK
©2019 TECHTARGET. ALL RIGHTS RESERVED.

In general, an incident response plan should include the following components:

- A plan overview.
- A list of roles and responsibilities.
- A list of incidents requiring action.
- The current state of network infrastructure and security controls.
- Detection, investigation and containment procedures.
- Eradication procedures.
- Recovery procedures.
- The breach notification process.
- A list of post-incident follow-up tasks.
- A contact list.
- Incident response plan testing.
- Ongoing revisions.

HOW TO MANAGE AN INCIDENT RESPONSE PLAN

The worst time to find out if an incident response plan has holes is during a real security crisis, which makes ongoing testing critical. Experts advise organizations to hold regular simulations featuring diverse attack vectors, such as ransomware, malicious insiders and brute-force attacks.

Many enterprises conduct incident response tabletop exercises to vet their plans. A discussion-based tabletop exercise involves talking through the specifics of an attack and the team's response. An operational tabletop exercise includes hands-on tasks, with enactment of relevant processes to see how they unfold. Templates such as this one can help plan effective simulations.

After both simulated and real security incidents, response teams should study what happened and review lessons learned. Note any security gaps that emerged, recommend appropriate additional controls, brainstorm ways to improve processes and update the incident response plan accordingly.

Remember, an incident response plan is not a set-it-and-forget-it proposition. It should continually evolve to reflect changes in the threat landscape, IT infrastructure and business environment. Experts recommend formal, comprehensive reassessments and revisions annually, at the very least.

INCIDENT RESPONSE FRAMEWORKS: PHASES OF INCIDENT RESPONSE

Rather than trying to recreate the wheel, an organization looking to build an incident response plan can refer to established incident response frameworks for high-level guidance and direction.

Well-known frameworks from NIST, SANS Institute, ISO and ISACA all differ slightly in their approaches, yet they each describe similar phases of incident response:

1. **Preparation/planning.** Build an incident response team and create policies, processes and playbooks; deploy tools and services to support incident response.
2. **Detection/identification.** Use IT monitoring to detect, evaluate, validate and triage security incidents.
3. **Containment.** Take steps to stop an incident from worsening and regain control of IT resources.
4. **Eradication.** Eliminate threat activity, including malware and malicious user accounts; identify any vulnerabilities the attackers exploited.
5. **Recovery.** Restore normal operations and mitigate relevant vulnerabilities.
6. **Lessons learned.** Review the incident to establish what happened, when it happened and how it happened. Flag security controls, policies and procedures that functioned sub-optimally and identify ways to improve them. Update the incident response plan accordingly.

WHO IS RESPONSIBLE FOR INCIDENT RESPONSE?

Behind every great incident response program is a coordinated, efficient and effective incident response team. After all, without the right people to support them and put them into practice, security policies, processes and tools mean very little. This cross-functional group consists of people from diverse parts of the organization who are responsible for completing the steps and processes involved in incident response.

TYPES OF INCIDENT RESPONSE TEAMS

The three most common types of incident response teams are as follows:

- Computer security incident response team (CSIRT).
- Computer incident response team (CIRT).
- Computer emergency response team (CERT).

These acronyms are often used interchangeably in the field, and the teams generally have the same goals and responsibilities. One important note is that the name *CERT* is a registered trademark of Carnegie Mellon University, so companies must apply for authorization to use it.

Another term commonly heard during an incident response team conversation is *security operations center* (SOC). A SOC encompasses the people, tools and processes that manage an organization's security program. While SOC teams may be responsible for incident response, it is not their sole task within an organization. SOC teams' other duties can include conducting asset discovery and management, keeping activity logs and ensuring regulatory compliance, among others.

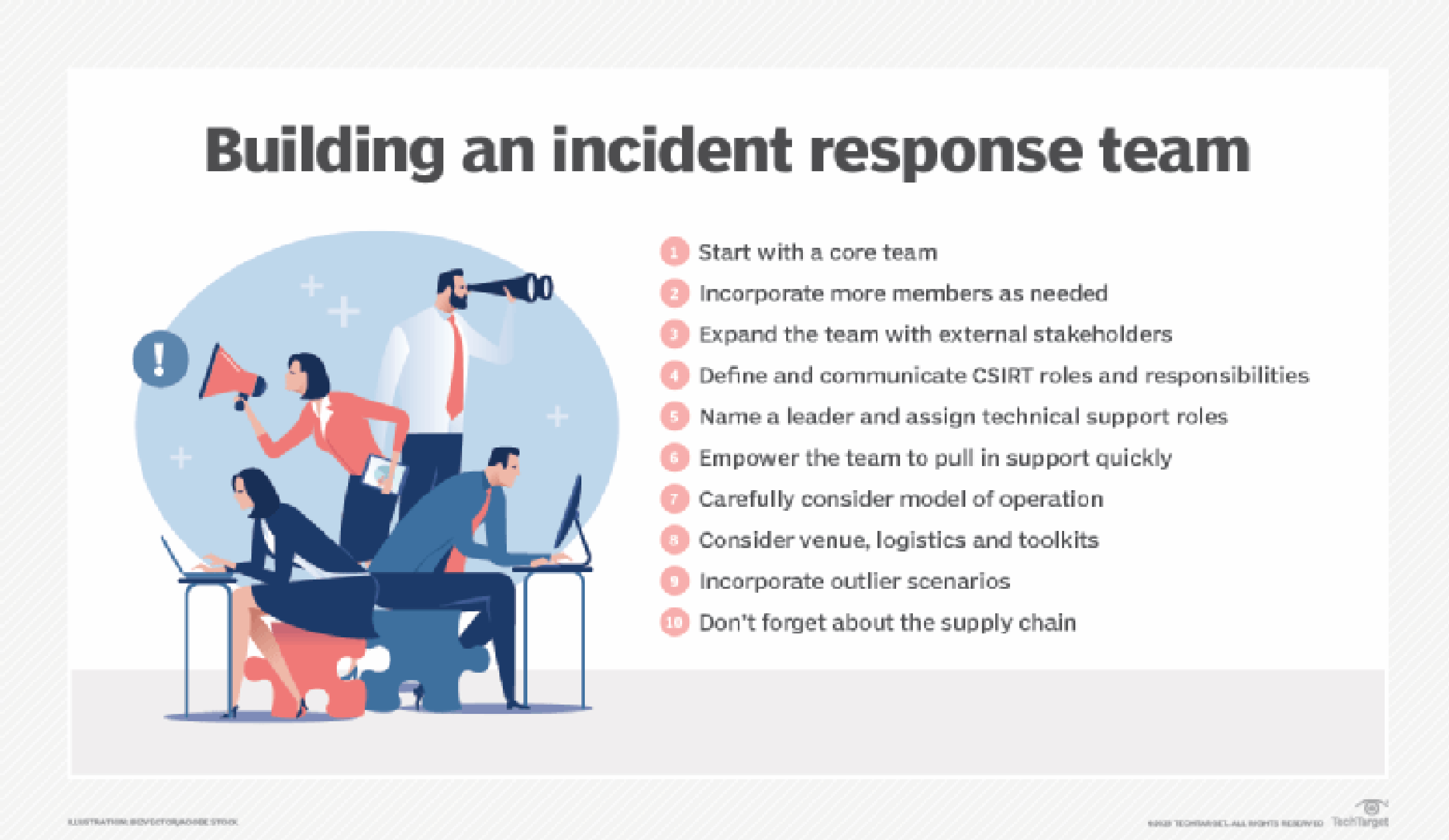
Learn more about CSIRTs, CIRTs, CERTs and SOCs.

Incident response team members

The size of an incident response team and the members included will vary based on the individual organization's needs. Some members may even fill multiple roles and responsibilities.

In general, an incident response team consists of the following members:

- **Technical team.** This is the core incident response team of IT and security members who have technical expertise across company systems. It often includes an incident response manager, incident response coordinator, team lead, security analysts, incident responders, threat researchers and forensics analysts.
- **Executive sponsor.** This is an executive or board member, often the CSO or CISO.
- **Communications team.** This includes PR representatives and others who manage internal and external communications.
- **External stakeholders.** Members include other employees or departments within the organization, such as IT, legal or general counsel, HR, PR, business continuity and disaster recovery, physical security and facilities teams.
- **Third parties.** These external members might include security or incident response consultants, external legal representation, MSPs, managed security service providers, cloud service providers (CSPs), vendors and partners.



Building an incident response team

1. Start with a core team
2. Incorporate more members as needed
3. Expand the team with external stakeholders
4. Define and communicate CSIRT roles and responsibilities
5. Name a leader and assign technical support roles
6. Empower the team to pull in support quickly
7. Carefully consider model of operation
8. Consider venue, logistics and toolkits
9. Incorporate outlier scenarios
10. Don't forget about the supply chain

ILLUSTRATION: [illegible]/ADOBE STOCK

[illegible] TECHTARGET. ALL RIGHTS RESERVED TechTarget

What does an incident response team do?

The chief goals of an incident response team are to detect and respond to security events and minimize their business impact. As such, team responsibilities largely align with the phases outlined in an incident response framework and plan. Team tasks include the following:

- Prepare for and prevent security incidents.
- Create the incident response plan.
- Test, update and manage the incident response plan before use.
- Perform incident response tabletop exercises.
- Develop metrics to analyze program initiatives.
- Identify security events.
- Contain security events, quarantine threats and isolate systems.
- Eradicate threats, discover root causes and remove affected systems from production environments.
- Recover from threats and get affected systems back online.
- Conduct follow-up activities, including documentation, incident analysis and identifying how to prevent similar events and improve future response efforts.
- Review and update the incident response plan regularly.

INTERESTED IN BECOMING AN INCIDENT RESPONDER?

Incident response requires professionals with security skills who can execute on tasks such as monitoring for vulnerabilities and taking appropriate measures when necessary. They must be able to analyze data to spot and assess the scope and urgency of incidents, as well as perform other duties. They may also report on trends, educate internal users and work with law enforcement.

The incident responder role can be an exciting, albeit challenging, career. Incident responder jobs are in demand and can command sizeable salaries. The tradeoff, however, is that many incident responders work long hours under constant stress.

Learn more about the incident responder career path.

Headed to an interview? Check out these sample interview questions.

INCIDENT RESPONSE IN THE CLOUD

As enterprise cloud use proliferates, the importance of including the cloud in incident response processes increases. The goals of cloud incident response are the same as in traditional incident response but with some caveats.

Consider the shared responsibility model, for example. With on-premises applications, platforms and infrastructure, an organization's IT and security teams are generally in charge of all management and security tasks. With SaaS, PaaS and IaaS, on the other hand, some or all responsibility shifts to CSPs. This can make incident detection and investigation more difficult or even impossible, depending on the deployment.

Cloud incident response may also require new tools and skill sets, as well as a deeper knowledge of cloud security incidents and threats. Traditional tools may not work properly -- or at all -- in cloud environments. New tools and procedures not only add to what incident response teams must learn and manage but may also require extra budget.

Learn more about cloud incident response, including the Cloud Security Alliance's framework and best practices for including cloud in incident response programs.

INCIDENT RESPONSE TOOLS AND TECHNOLOGIES

As Benjamin Franklin once said, "The best investment is in the tools of one's own trade." In the case of incident response, this involves many tools, typically categorized by their prevention, detection or response functionalities.

No silver-bullet, one-size-fits-all incident response tool exists. Rather, a mix of tools and technologies are required to help incident response teams prevent, detect, analyze, contain, eradicate and recover from incidents. Most organizations already have a variety of incident response tools and processes in deployment. Typically categorized by their detection, prevention and response functionalities, these include the following:

- Antimalware.
- Backup and recovery tools.
- Cloud access security broker.
- Data classification tools.
- Data loss prevention.
- DoS mitigation.
- Employee security awareness training.
- Endpoint detection and response.
- Firewalls.
- Forensics analysis.
- Intrusion prevention and detection systems.
- Security information and event management (SIEM).
- Security orchestration, automation and response (SOAR).
- Vulnerability management.

Managing all these tools can be a lot for a security team to handle. Many organizations are turning to automation in incident response to reduce alert fatigue, perform alert triage, automatically investigate and respond to threats, automate ticketing and alerting, conserve human efforts for more high-value activities, respond and resolve issues faster, automate case management and reporting, and save money.

Contemplating whether to handle incident response in-house versus outsourcing some or all incident response duties? In-house incident response requires the proper staff, tools and budget. It's also important to consider the nature and complexity of the threats the organization faces. In some scenarios, in-house incident response may be the best bet. Organizations facing more serious threats -- or those that have multiple locations, each facing unique threats -- may be better suited to outsourcing their incident response needs, however.

Service providers often offer incident response services, such as the following, on retainer or on an emergency basis:

- Managing threat detection and response.
- Providing threat prevention services.
- Conducting penetration tests and threat hunting.
- Assisting with media and PR management.

- Conducting root cause analysis.
- Conducting crisis management.
- Maintaining regulatory compliance.

Get help deciding between deploying incident response in house or employing a service provider, and read up on the leading incident response software, vendors and service providers.

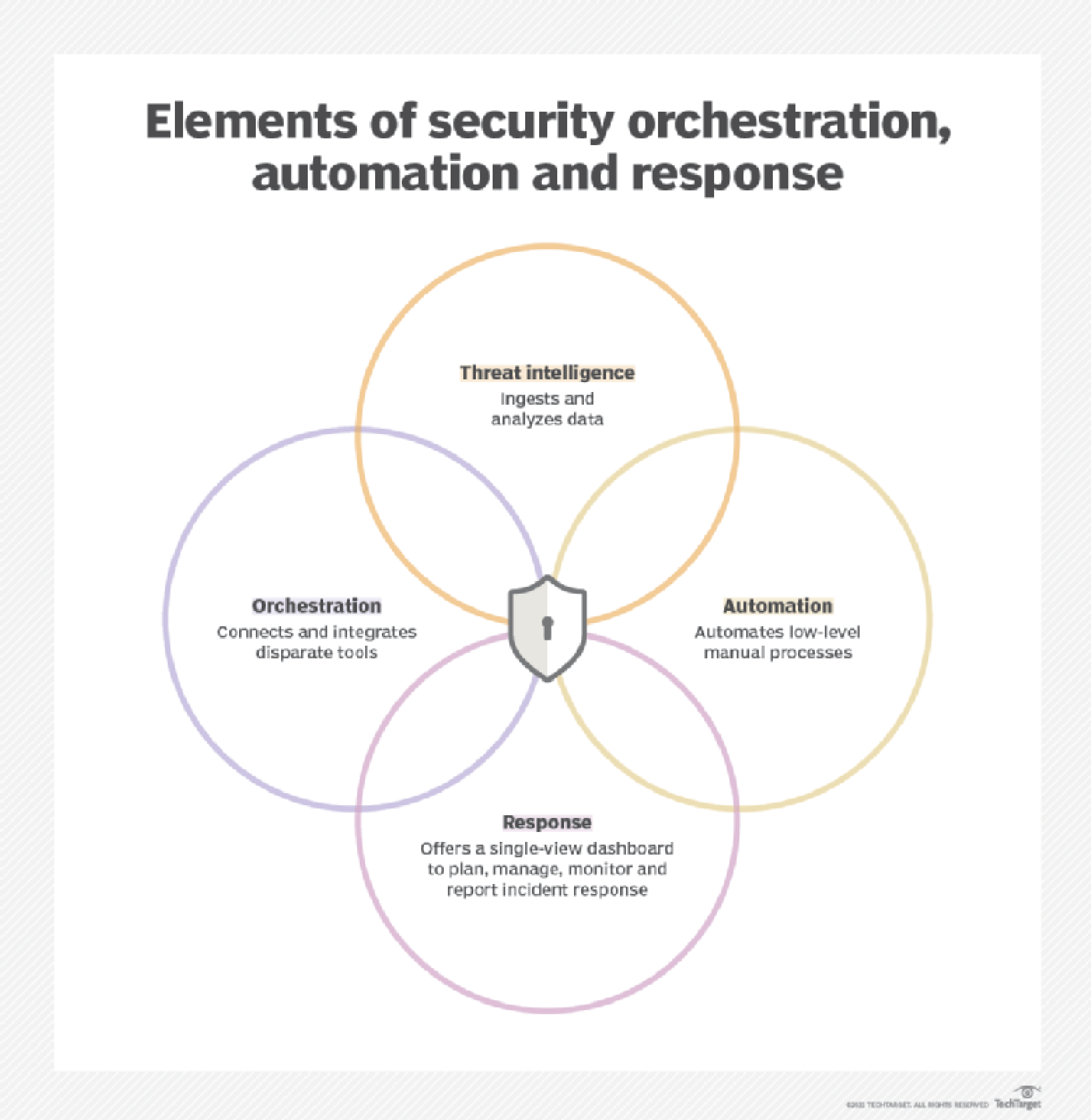
INCIDENT RESPONSE AND SOAR

SOAR is one of the newest tools to join the incident response arsenal. As such, confusion surrounds what it is and what it does. Its capabilities sound similar to those of SIEM, adding to the confusion.

Security orchestration, automation and response is a collection of technologies that, when combined, help security teams aggregate, analyze, detect and respond to security events with little or no human input. The main functions of each component of SOAR are outlined below:

- **Security orchestration.** This function connects and integrates internal and external tools through built-in or custom integrations and APIs. It collects and consolidates data collected by various tools to initiate response functions, based on defined incident analysis parameters and processes.

- **Security automation.** This function uses the data collected during security orchestration to trigger workflows and tasks based on defined thresholds and actions laid out in incident response playbooks. SOAR platforms can automatically remediate lower-risk vulnerabilities and complete low-level tasks historically performed by human analysts, such as vulnerability scanning. High-risk threats also can automatically escalate to security analysts for further investigation.
- **Security response.** Delivered via a single view, this function enables security, network and systems analysts to access and share threat intelligence, collaborate and conduct post-incident response activities.



Elements of security orchestration, automation and response

Threat intelligence
Ingests and analyzes data
Orchestration
Connects and integrates disparate tools
Automation
Automates low-level manual processes
Response
Offers a single-view dashboard to plan, manage, monitor and report incident response
©2023 TECHTARGET. ALL RIGHTS RESERVED
TechTarget

SIEM systems' operations are similar to SOAR platforms, but they lack a key feature: automated response. SIEMs simply alert teams about potential incidents; they do not trigger automated actions. SIEMs and SOARs have similar mean time to detect, but SOARs excel with mean time to respond, thanks to their automated capabilities.

SOAR platforms augment human analysts with the following capabilities:

- Threat intelligence coordination.
- Case management.
- Vulnerability management.
- Automated enrichment for remediation.
- Threat hunting.
- Incident response automation.

In these use cases, SOAR platforms can help improve productivity; automate repetitive, tedious and low-importance tasks; use existing security tools better and more contextually; and improve third-party tool integration, among other benefits. SOAR platforms aren't without challenges, however. Namely, SOARs may not be able to integrate with all security tools easily or at all, do not address security culture within an organization and may fail to live up to inflated user expectations.

Learn more about the benefits and challenges of SOAR systems.

Incident response is a cornerstone of any enterprise cybersecurity program; its importance cannot be overstated. Quickly responding to security incidents effectively and efficiently helps minimize damage, improve recovery time, restore business operations and avoid high costs.

But as Benjamin Franklin would attest, "Look before or you'll find yourself behind." In other words, prevention is key. A well-thought-out incident response plan and top-notch incident response team will prepare organizations for when the inevitable happens. But the first line of defense should always be keeping networks and data safe, as well as ensuring users are empowered and security-aware.

CONTINUED READING

10 types of security incidents and how to handle them

Top 10 types of information security threats for IT teams

SOAR vs. SIEM: What's the difference?