corsica technologies

WHITEPAPER

Incident Response and Containment 101

Introduction

What processes and roles should you establish BEFORE an incident occurs? What does the incident response process look like? Here's everything you need to know.

When a cybersecurity incident occurs, it's all hands on deck.

But the best response process in the world won't help if your organization isn't prepared *before* an incident occurs. In this article, we'll cover everything you need to establish *before* an incident. Then we'll cover the actual process of incident response and containment.

What you need to establish BEFORE an incident

1. SOC (Security Operations Center)

Your SOC is the lifeblood of your cybersecurity operations. Without a SOC and the experienced professionals and technology that accompany it, it's nearly impossible to respond to an incident—let alone contain it. Here's a brief overview of what a SOC gives you.

- **Professional cybersecurity experts.** At the end of the day, cybersecurity will always require skilled professional resources. No SOC is complete without a dedicated team.
- **24/7/365 human monitoring.** It's one thing to leave monitoring systems running 24/7/365. But if there's no one there to respond when the unthinkable happens, then those systems aren't much good. A SOC provides the continuous human monitoring you need.
- **Essential cybersecurity software like MDR and SIEM.** MDR (managed detection and response) is an essential solution that your cybersecurity experts will use to detect and respond to incidents. SIEM (security information and event management) aggregates as much security information as possible in a single user interface while also empowering administrators to respond to events.

Midmarket organizations typically can't handle all this on their own. Existing IT staff can't cover the additional workload of cybersecurity—and they don't often have the experience to do so. Hiring dedicated cybersecurity professionals is difficult due to high salary expectations and frequent churn. For these reasons, midmarket organizations often outsource this function to a cybersecurity managed services provider.

2. Full documentation of your network

When a cybersecurity incident occurs, one of the first things your analysts will do is try to contain the threat. To achieve this, they need full documentation of your network. This includes things like:

- Network topology
- Server rack diagram (for on-premises networks)
- Cloud architecture (for cloud networks)
- IP address map
- Full inventory of network hardware and software
- Wireless network documentation

You should have this documentation in place anyway, but the key here is to keep it up to date. You want to be prepared when an incident occurs.

3. Systems and processes for backup and disaster recovery

No network, device, or cloud system is immune to catastrophe. A cybersecurity incident can result in data loss or corruption, making backup and recovery an essential function to establish *before* an incident occurs.

Due to the expense and skilled labor required, many midmarket organizations outsource this function to an MSSP (managed security services provider). Learn more here: Backup and Disaster Recovery Services

4. Business continuity plan

This might sound similar to backup and disaster recovery, but it's actually quite different. Backup and disaster recovery is about restoring essential business systems and technology infrastructure after a devastating incident.

Business continuity is about keeping a business operational *during* a disaster.

5. Incident response plan

This is the backbone of your incident response readiness. It defines your incident response processes (which we'll cover below) so there are no questions when the unthinkable occurs.

There is no one-size-fits-all approach to this plan. Here are some excellent resources for structuring your plan.

- CISA (U.S. Cybersecurity & Infrastructure Security Agency) Incident Response Plan Basics
- NIST (National Institute of Standards and Technology) Computer Security Incident Handling Guide
- SANS Incident Response Cycle
- HHS Incident Response Plan Whitepaper

Some organizations may not have the bandwidth to create this plan on their own. An MSSP can help craft a plan that fits the unique processes and regulatory requirements governing your organization.

6. Assigned roles for your incident response

While your plan should include role assignments, it's worth calling this out separately. Before an incident ever occurs, you want to have several roles filled, as CISA (the U.S. Cybersecurity & Infrastructure Security Agency) explains.

- **Incident manager.** This is the person who leads the entire response to the incident.
- **Technology manager.** This is the person who can lead the response from a technical perspective.
- **Communications manager.** This is the person responsible for all incident-related communications, whether internal or external.

For midmarket organizations, it may be challenging to assign some or all of these roles in-house. For these organizations, an MSSP (managed security services provider) can assist.

Incident response and containment processes

The exact process you use will depend on your incident response plan. Different plans may use different terminology or combine certain steps together. However, speaking generally, here are the steps involved in incident response and containment.

1. Detection and identification/analysis

Incidents are typically detected by sophisticated software like MDR (managed detection and response), which may use powerful algorithms and even AI to spot anomalous behavior on your network. This allows your cybersecurity analysts to ignore harmless network traffic and focus on activity that looks suspicious.

Once automated systems have detected an incident, your cybersecurity specialists will identify it. This means gathering the specific information they need to contain the threat—such as systems affected, type of attack, IP address of origin, and more. Your specialists will begin a rigorous process of documentation that will aid not only in the incident response, but also in communication with law enforcement and in preparation for any potential legal action.

2. Containment

Once your cybersecurity analysts know what they're dealing with, they'll move fast to contain the threat.

Effective containment will mean different things depending on which systems are compromised. For example, if a workstation has malware installed on it, the first step in containment is to isolate that machine from the network and from all other machines. Cybersecurity specialists can do this remotely using software that still allows them to access the machine after it's been cut off from the network.

If an essential device like a server is compromised, containment gets more complicated. Specialists must take into account the presence (or absence) of redundant server resources, as well as the

potential impact to operations and revenue—both for leaving the server online, and for taking it offline. Experience and understanding of the scenario are essential for making the right decisions here.

3. Investigation

Earlier in the process, your cybersecurity analysts had to prioritize containment over full analysis. This means they only gathered as much information as they needed to contain the threat.

Now that the threat is contained, it's time to get the full story. Your cybersecurity specialists will uncover as much information about the incident as possible. They'll consult SIEM (security information and event management) software, as well as any additional logs required. All along the way, they'll continue to document everything they find to support communication with stakeholders, customers, and law enforcement—as well as providing an evidentiary foundation for responding to any legal action.

4. Eradication

Now it's time for your cybersecurity specialists to destroy the threat. Eradication looks different depending on the type of attack, but here are some actions that typically occur.

- Deletion of any malware installed on a device
- Device reimaging (full wipe and installation of a new operating system), as required
- Closing user accounts compromised in the attack (or resetting their passwords)
- Blocking IP address(es) from which the attack originated

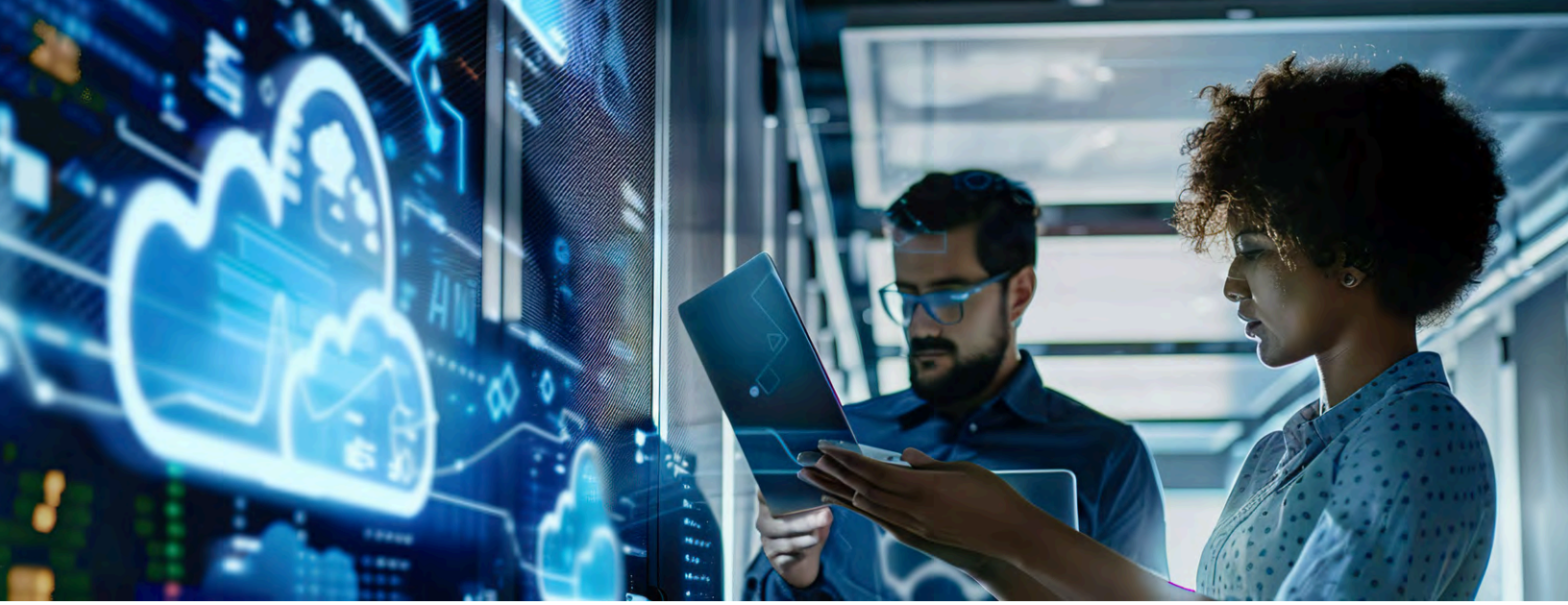
5. Recovery

You can't go back to life as usual after eradicating a threat. The information gathered in the incident response process will offer numerous takeaways for making your environment more secure. The key is to turn that information into real changes to systems, hardware, and processes.

Here are some common changes that companies make during the recovery process.

- Enforcing MFA (multi-factor authentication) on all email accounts
- Catching up on patching (and implementing a plan to stay on top of it from now on)
- Deprecating outdated systems and hardware that don't support modern security controls
- Updating network access policies to make it harder for criminals to get in
- Moving toward a Zero Trust framework

Whatever changes have been implemented, it's a good idea to test them for effectiveness. A network penetration test can determine how effective these changes are.



Getting the incident response plan and service you need

As you can see, it's a fairly significant responsibility to develop and implement an incident response plan—then actually respond when an incident occurs.

Many midmarket companies don't have the resources to achieve this in-house. IT staff have their hands full with day-to-day operations. This leaves no bandwidth for a programmatic approach to incident response, and it makes real-time containment and eradication almost impossible.
This is one reason MSSPs exist. The right partner can advise on the right incident response framework for your organization—and they can create a plan from that framework that's tailored to your unique operations.

The key, though, is to insist on an MSSP who not only notifies you of incidents, but also remediates them.

Unfortunately, most MSSPs don't actually remediate incidents. They only provide notification to their client (and/or to the client's MSP or managed IT service provider). Under this model, incident response and containment gets broken up across multiple vendors and teams. This destroys any synergy across the process. It can lead to essential information getting lost and, at worst, incomplete attempts at containment and eradication.

Choosing an MSSP who offers full or partial cost coverage for their incident response services

Midmarket organizations without cybersecurity experts on staff should look for comprehensive MSSP coverage. Decent MSSPs will handle cybersecurity from top to bottom, including the entire incident response and containment process.

But the best MSSPs go beyond this. They offer cybersecurity service guarantees that cover the cost of their services to remediate an incident (with limitations).

That's what we do here at Corsica Technologies. Our Corsica Service Guarantee empowers us to cover some or all of the cost of services to remediate incidents on our clients' systems. As far as we know, this is the only service guarantee of its kind in the industry. See the link for details and limitations.

Want to learn more? Get in touch with us today. Let's talk about your incident response and containment process—and how we can help.

corsica technologies

Corsica Technologies offers managed IT and cybersecurity services for businesses throughout the United States. We help companies to align technology with their business goals while minimizing the IT risks to their organizations so they can focus on running their business. One of the nation's leading managed service providers, Corsica Technologies is full service—offering everything from help desk IT support to advanced cybersecurity risk management and compliance.

Ready to learn more about cybersecurity managed services?

Schedule a free consultation with our specialists to learn how technology can enable and transform your business.

corsicatech.com (855) 411-3387

Mid-Atlantic
508 Rhett Street
Greenville, SC 29601

Midwest
9921 Dupont Circle Dr West
Ft. Wayne, IN 46825

Southeast
1721 Goodrich Street
Augusta, GA 30904