ActZero

Elevating Incident Response Readiness

MSE Edition This guide is for midsize enterprises to improve their handling of cybersecurity incidents through preparation, planning and practice - to ultimately reduce the likelihood and impact of cybersecurity breaches.

CONTRIBUTORS:

Adam Mansour
Chief Security Officer

Will Ehgoetz
Manager, Threat Hunting

ActZero

Before the Alarm Sounds

There's no better time to deal with a cybersecurity incident than before it has ever happened. Organizations who are just now recovering from an incident from which they were unprepared learn this the hard way. And even those who have witnessed similar organizations in the news experience a difficult cyber incident should see the impact to their brand, their customers and their bottom line as a wake-up call to think critically about how prepared they truly are.

Most midsize businesses have at the very least a bare bones incident response (IR) plan in place. Organizations like yours likely already understand basic concepts around triage, how to define incidents, and what incident escalation looks like. However, they may struggle with setting up formalized roles, prioritizing incidents, learning from incidents through effective 'post mortems' and regularly practicing their plan to improve it over time. This guide offers insight into what it takes not only to create a better plan, but to continuously update it to meet the changing needs of the business.

A SUSTAINABLE INCIDENT RESPONSE PROGRAM

BUILD CYBER RESILIENCE

Thinking Ahead: Establishing a Sustainable IR Plan and Program

Whether your organization currently has a documented IR plan in place or it still runs on ad hoc procedures, it's important to keep the following IR tenets in mind:

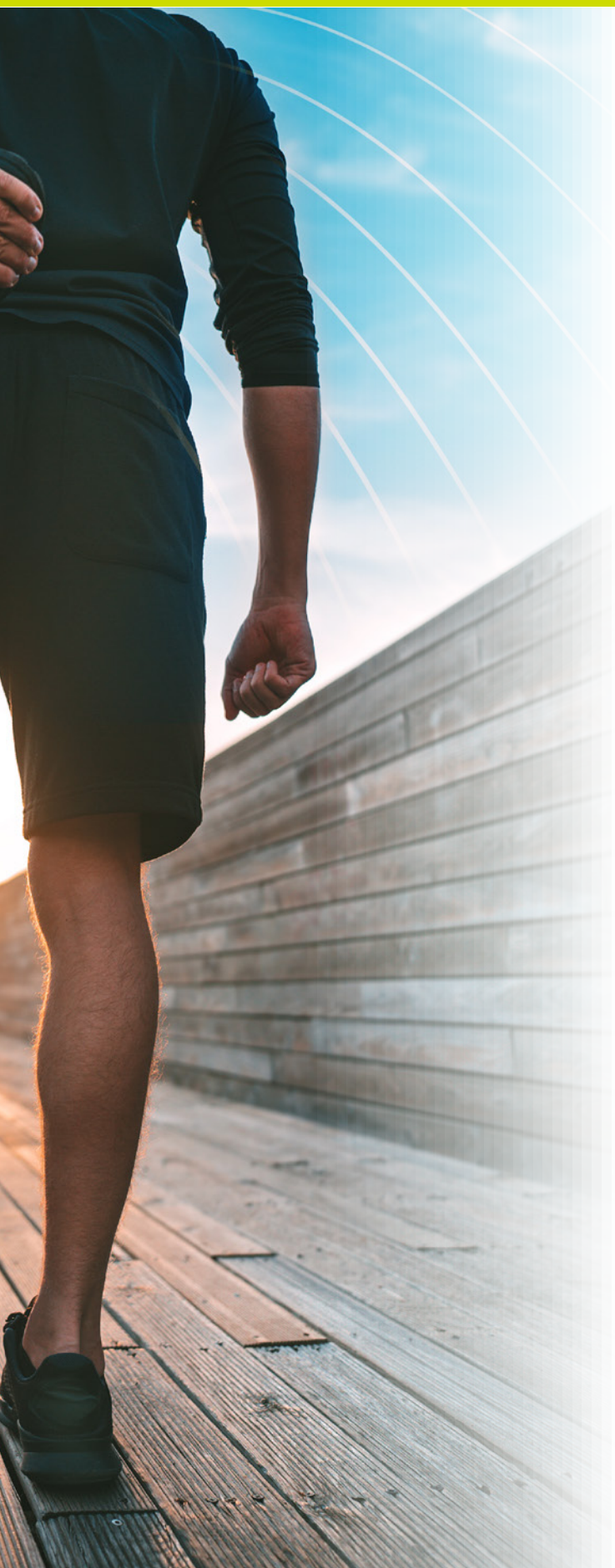
- There is no such thing as a perfect incident response plan
- An imperfect and simple plan is better than none at all
- The goal should be to start small and incrementally improve over time

Maturing midsize organizations should consider preparation for future incidents as an ongoing and cyclical process. The best incident response plans are iterated upon through a three-step cycle: Prepare, Plan, Practice.

1 Prepare

This is where an organization plans to make a plan. To prepare for the improvement of an existing plan (or the development of a new one) organizations must start with some basic but timely self-assessment.

Response planners should probe the current state of their organization by asking questions of themselves—about their team, their technology, processes, and business missions supported. They then should prepare a brief document that lays out what they've discovered by this quick look in the mirror. The document should be shared with IT and business leaders so that everyone can agree on priorities that will drive how the updated IR plan should look.



Self-assessments should help get a level set on the business, the assets at risk, and who's responsible for those assets:

KNOW YOUR BUSINESS:

Identify the key business processes that run the business.

- Include front-of-the house processes that impact production of products, sales processes, and customer communication
- Also include critical back-office processes that keep the lights on, such as financial functions

KNOW YOUR ASSETS:

Map the technical capabilities that power those key business processes

- Mapped assets may include important database servers, and will almost certainly include your network directory infrastructure, such as Active Directory
- Similarly, don't forget important SaaS and cloud components of the asset portfolio, including Microsoft 365 infrastructure
- Comprehensive asset mapping is what mature organizations should strive for, but at very start just try to understand what are the critical components that support processes that keep revenue streaming in
- Identify these critical assets by looking for the most important systems, services, or data that if lost or otherwise interrupted, could lead to extreme business disruption, high costs to recover, or even going out of business
    - These are systems or data that couldn't wait a few days (forget your mean time to recovery – consider worst case scenarios that could threaten business viability if they buck the average) to fix or reinstall, or that are proprietary in nature, such as the proverbial "secret sauce" recipe

KNOW WHO'S RESPONSIBLE:

Identify asset owners and operators for each documented asset

- This should include both the main business stakeholder who depends on that asset, and the IT person in charge of administering it
- Midsize businesses may need to map out who the application/asset owners are for each, as well as the lines of business supported by the asset.
- Also, don't forget to list outside vendors in charge of assets—including SaaS and managed service providers--and important contacts at each
- Start with our template

With that self-knowledge in hand, organizations should list out the most immediate threats to the assets listed and consider those most likely to trigger security incidents. Less mature organizations should keep it simple by identifying the most common scenarios impacting organizations like theirs, such as ransomware, account compromise, data theft, and malware outbreaks. The major threats enumerated here will stand as the main scenarios around which response procedures will be built. Maturing midsize businesses with established SOCs, threat intelligence capabilities, and frequent penetration or red team testing can also layer in global threat trends and threat intelligence, data from internal incidents and events, as well as security validation reports.

Record all the knowledge you've dug up from this discovery process in a clear but simple document. Then use that to get an early sanity check from company leadership that these are, in fact, the priorities that should drive the cybersecurity IR plan. Running this document by line-of-business leaders before starting on the meat of the IR plan will save wheel spinning later on and increase the chances that the team can get solid buy-in from the highest levels of leadership planned responses to critical incidents that might seem extreme to those not informed of the risks. Making choices like these in the heat of an incident takes time that could make all the difference in preventing a minor incident from blowing up into a major one. By front-loading the decisions through early buy-in, those handling incidents on the ground will have the confidence to execute on IR plans immediately.

2 Plan

First ensure that the documented incident response plan includes action steps for the riskiest and most likely scenarios that threaten critical assets. These will typically be critical incidents. Subsequently add in steps that address lower risk scenarios that could still materially impact the business: these are high, medium, and low severity incidents.

For each scenario, be sure to detail the following:

IDENTIFICATION

This will detail how an incident becomes an incident. Identification of incidents most typically comes by way of cybersecurity detection and alerting technology, which triggers many response activities. But it should also include procedures for receiving user complaints or input that can act as a route for incident intake. This could include cases where a user's endpoint is displaying a ransomware ransom note or when a user suspects they may have clicked on a phishing message and they're now experiencing system abnormalities.

If the organization has minimal security detection and alerting capabilities, managed detection and response (MDR) services can help bolster their ability to find incidents earlier and more accurately, especially those leveraging artificial intelligence (AI).

EARLY RESPONSE AND REMEDIATION

Determine a list of what information and logs need to be collected and what needs to be documented after an alert triggers for the particular scenario that's being planned for. For example, if an account compromise is suspected, the planned documentation list might be:

1. The time of detection
2. A brief description of the detection
3. Filenames and paths involved
4. Workstation names of impacted systems
5. Usernames of affected accounts
6. Source IP Addresses of Attackers

Develop a list of immediate steps to isolate and contain the threat before escalating and further investigating the alert. In the case of suspected account compromise, these steps might be:

1. Quarantine the asset: turn it off and unplug/disconnect from the network
2. Require user to reset passwords 3. Enable multi-factor authentication, if it is disabled
3. Investigate system logs associated with account to look for malicious access behavior
4. Determine if sensitive data is present and document the possibility of a breach

ESCALATION PROCEDURES

Decide what the technical triggers will be for unplugging or disabling a potentially compromised system. For example, if ransomware notes are found, that would trigger the endpoint to be removed from the network.

Determine a process and triggers for escalating to further investigation and help from an outside incident response team. Similarly, establish when authorities or regulatory bodies need to be contacted if a breach of personally identifiable information is suspected or confirmed.

Again, establishing these decisions clearly identifying escalation procedures here will help responders avoid pushback or hesitancy from stakeholders mid-incident who inevitably will argue, 'Is it really necessary to shut this system down?'

COMMUNICATIONS PLAN

Decide who needs to be called internally and when they should be called as an incident escalates. This includes internal parties and external service provider contacts such as:

- Asset owners
- Help desk
- Service provider response teams
- Legal
- HR
- Corporate communications
- Privacy Offices

If your plan only includes roles and titles in the communications plan, update it to include names, phone numbers, and email addresses for each contact that needs to be involved at various steps of escalation. These names will change over time, but your plan should be updated frequently enough to keep up with these shifts. Establish a communications and call tree contingency plan for cases when email or phone service has been disabled due to the incident. This means including secondary communications for all staff included in the plan—including cell phone/home phone/emergency contact numbers.

Additionally, make sure you also have a process/cadence by which this call tree is updated.

Finally, consider coming up with an external communication plan for when and how external communication will be made to the following in the event of an incident or breach that impacts customers:

- Legal Departments
- Customers
- Journalists

As a part of this external communications process, identify what conditions would warrant a press release and/or a call to authorities. If organizations are unsure what authorities to call, consider checking out ActZero's Breach Notification Rolodex for help.

CONTAINMENT AND RECOVERY

Document procedures for containment, bringing systems back online, recovering data, and remediating vulnerabilities/active threats so reinfection does not occur. Ideally an external response team can prove an invaluable partner in these clean-up steps.

Getting buy-in on these procedures is crucial. Once the draft of the plan is established, IT and security personnel should have business leaders and the CEO sign off on the plan, especially when it comes to drastic containment measures for critical incidents, such as taking revenue producing systems offline or off the network in certain scenarios.

Doing so will enable IT practitioners to act more quickly mid-incident without having to get someone to sign off on shutting down a key server or online service. This could make all the difference between an isolated infection and a massive incident that puts business viability on the line.

List the response action from your plan.

Be specific. You will practice these procedures, and the person doing them may change.

List the reasons you would respond this way.

The idea is to accept the business impact of the response, given the criteria, before that trigger occurs.

This makes action clear for the responder - if criteria met, initiate response procedure.

List potential disruption of the response action.

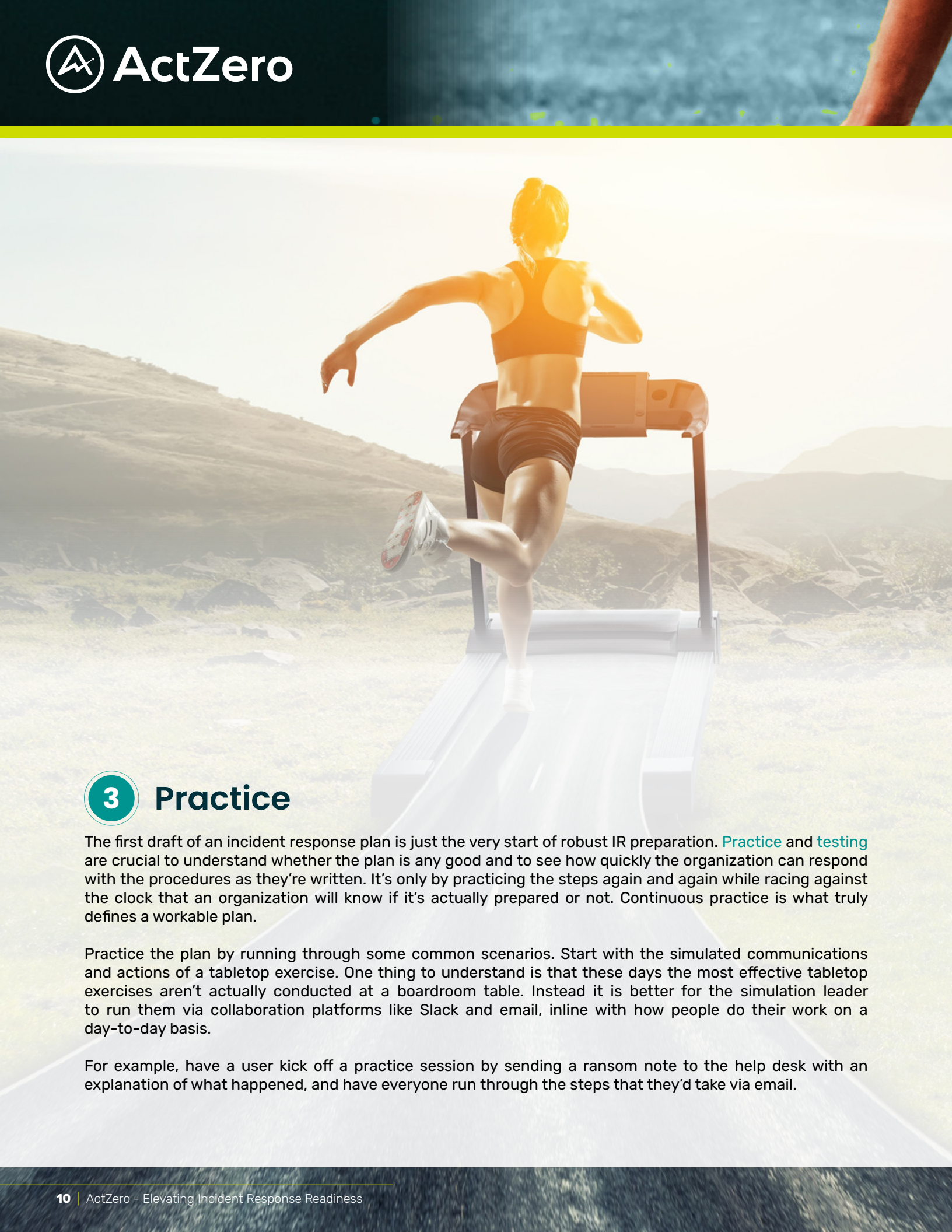
Include systems & teams impacted; how long they will be impacted; and the severity of the impact.

List the person and function responsible. Use the roles you established in your IR plan - as the specific person may change.

List the name / title of the approver. This conveys on whose authority the responder is acting. It helps avoid pushback.

Response Procedure	Trigger / Criteria	Business Impact	Execution	Approved By
Quarantine Workstation	A workstation is infected	Single user down 4 hours Low	Helpdesk	CIO
Password Reset Afflicted Users	A user profile is behaving anomalously	Multiple users down ~1 hour Low	Helpdesk	CIO
Password Reset Across Admins	An administrator profile is behaving anomalously; An administrator profile is no longer accessible by personnel;	All admin profiles down, including for enterprise software. Time & severity vary	IT Manager	CIO
Disconnect Critical Server from Internet (eg, Exchange)	A critical server is infected	Org-wide disruption Time & severity vary	Systems Admin	CEO & CIO CFO if financial systems hit
Disconnect Network Entirely	Multiple endpoints encrypted with ransomware	Org-wide disruption Time & severity vary	Disaster Recovery	CEO & Leadership Team

Click to Download File



3 Practice

The first draft of an incident response plan is just the very start of robust IR preparation. Practice and testing are crucial to understand whether the plan is any good and to see how quickly the organization can respond with the procedures as they're written. It's only by practicing the steps again and again while racing against the clock that an organization will know if it's actually prepared or not. Continuous practice is what truly defines a workable plan.

Practice the plan by running through some common scenarios. Start with the simulated communications and actions of a tabletop exercise. One thing to understand is that these days the most effective tabletop exercises aren't actually conducted at a boardroom table. Instead it is better for the simulation leader to run them via collaboration platforms like Slack and email, inline with how people do their work on a day-to-day basis.

For example, have a user kick off a practice session by sending a ransom note to the help desk with an explanation of what happened, and have everyone run through the steps that they'd take via email.

After running the tabletop exercise, organizations could also consider actually shutting down servers/services (a la Chaos Monkey) in more intensive technical simulations. However, SMBs will likely need the help of external providers with experience running these practice exercises to limit the possibility of incurring unnecessary business risk.

Also consider actual incidents to be the most valuable kind of practice. Don't neglect to run postmortem meetings to learn from incidents themselves by documenting what happened and using those lessons to update the incident response plans.

Practice helps identify gaps in controls and in the IR plan itself to give clues to improving the plan and also building resilience through better targeted cyber investments.

PUTTING IT ALL TOGETHER

Use the following chart to document the preparation, plan and practice stages.

Cybersecurity Scenario Detection and Response Tracker

Scenario	Detection	Alerting	Response	Time
For any incident requiring escalation, execute your Call Tree and engage your team				
I've been hacked and don't know how they got in	None	User Reported	Call ActZero @ 1.855.917.4981	2 Hours
I've been hacked and believe they have accessed sensitive data	RDP Logs	Anti-Virus	For disclosure in your state, check Breach Notification Rolodex	3 Days

Click to Download File

Build Cyber Resilience: Using IR Practice and Threat Modeling to Improve Controls

Threat modeling can stand as an invaluable tool for midsize businesses hoping to improve their cybersecurity and incident response readiness over time. Originally used to model threats in a military context to evaluate defensive preparations, this technique is used today to:

- help identify the threats that are the greatest risk;
- highlight gaps in safeguards, and
- to prioritize the mitigations and controls to protect against the identified threats.

Threat modeling has IT and cybersecurity teams systematically think through scenarios that keep them team up at night and then map those to capabilities that stop them. By using threat modeling to identify gaps in capabilities, maturing midsize organizations can come up with a security roadmap that's easily justifiable to business decision-makers.

The good news is that IR planning, as described above, already gets you part way through the threat modeling process, which first starts with assessing the environment and assessing likely threats and vectors. By putting the plan together and testing it, an organization will be able to analyze where existing controls break down in the face of the most worrying threats to an organization.

While threat modeling frameworks exist to walk organizations through this gap analysis, IT pros don't need to make it complicated. The goal should be to take the basic steps within a threat's typical attack pattern and then map that to existing controls. A threat modeler starts by listing out what the steps in an attack chain look like, and then establishing a visual model of the ideal controls or monitoring that can be used to counter or alert on activity in each of those stages.

Here's an example of the process:

User	User Awareness (Phishing Exercises, Infosec Training), Phish reporting Button
Click Link	Email Content Filtering, IDS/IPS, Email Sandboxing, Sender ID Verification (SPF, DKIM, DMARC)
Malicious Page	URL Reputation, Content Filtering, Anti Virus, NGFW, ActZero MDR
Compromised	Vulnerability Patching Software, Antivirus, ActZero MDR
Installed	Anti Virus, Limit Admin Rights, ActZero MDR
Happens	IDS/IPS, ActZero MDR, DLP

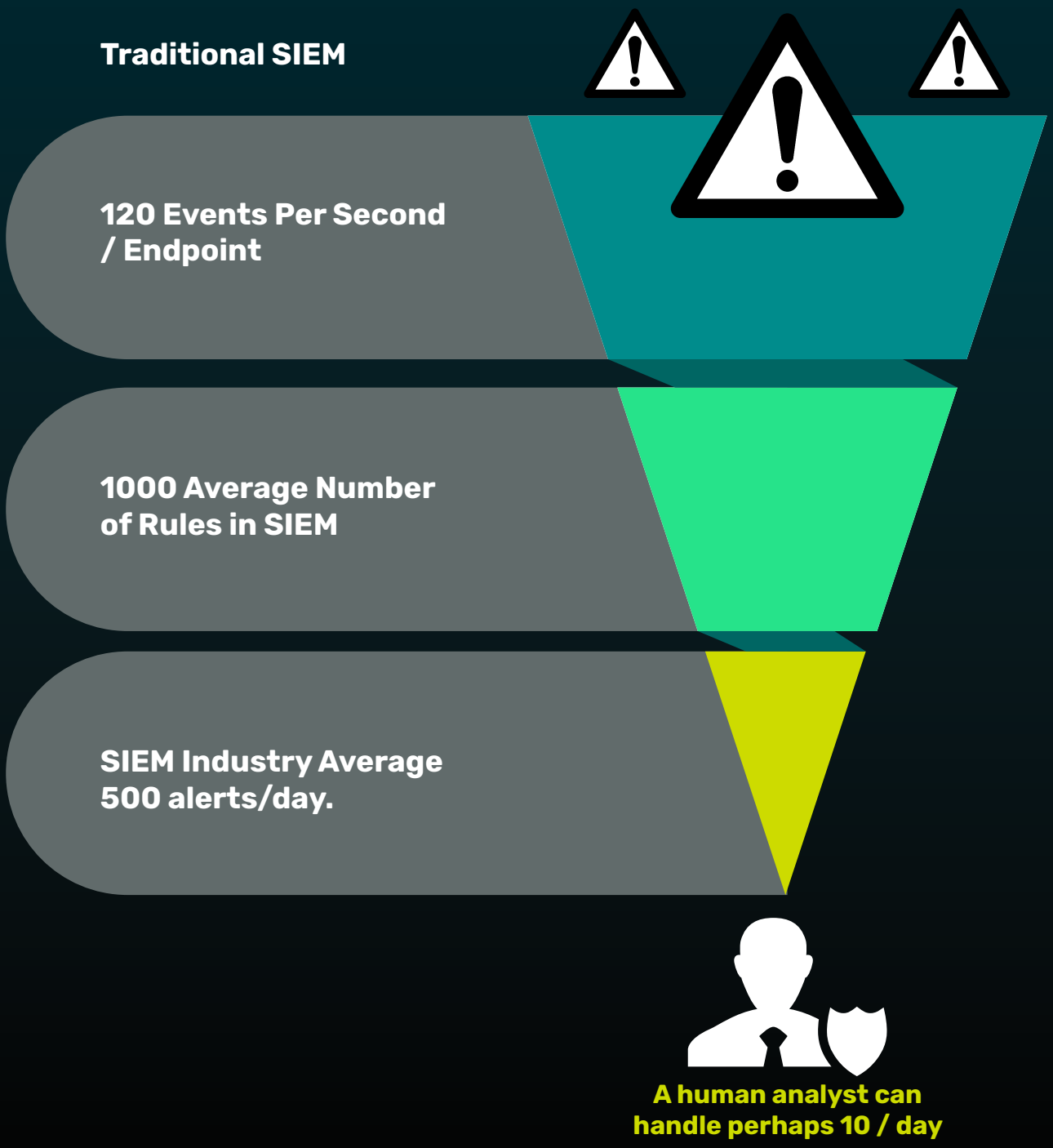
Now look at the diagram to see where your gaps are. Which areas do you not currently have covered? These are the areas you will want to propose new controls, in order to mitigate the risk of such gaps being exploited.

Here at ActZero we use our own maturity model to help customers understand what controls they have addressed or are missing in their environments. This can be a valuable tool for prioritizing which controls to invest in first and plan a sensible roadmap.

From here, implement control improvements and then revise the incident plan accordingly—then test it!

ActZero

Many mid-sized organizations struggle to take their incident response capabilities to the next level because they've tasked and equipped junior security people with tools like SIEM and EDR that are difficult to get maximum value from without a lot of resources and expertise. They labor under the pressure of a growing attack surface, the increasing sophistication of attacks, a massive amount of notifications that don't translate into meaningful responses, and the lack of adequate security resources.



"MDR services provide remotely-delivered modern security operations center capabilities focused on quickly detecting, investigating and actively mitigating incidents[1]"

1. If you find yourself faced with the challenge of alert fatigue, or of disjointed systems that inhibit visibility, an MDR service may be able to augment your capabilities, act as an extension of your team, or improve visibility with portals or dashboards (click here for a rubric to evaluate MDR capabilities).

2. MDRs are specialist firms that can help midsize businesses get over the hump of these obstacles without hiring a rock star team or breaking the budget in the process. MDRs are used to deliver advanced cybersecurity functions.

3. Advanced MDR combines the power of machine learning, AI and robust data science with the expertise of truly elite cyber responders to create the most effective detections that can be layered on top of an organization's existing security infrastructure.

4. On top of all of that, MDR services can also help organizations improve and practice their incident response plans.

[1] 2021 Gartner Market Guide for Managed Detection and Response

Click here to engage ActZero for Advanced Incident Response services.

Or, to see how our Managed Detection and Response service helps stop threats before they become breaches, check out our website or request a demo today.

About ActZero

Through a combination of technology, threat hunting expertise and a deep investment into data science and security engineering ActZero helps midsized organizations remove the complexity of building security operations, while stopping more meaningful threats. Through one unified solution we provide organizations with faster, more effective detection and response, a stronger signal-to-noise ratio, and help to reduce risk and improve your security maturity over time.

ActZero

TORONTO
5045 South Service Road, Suite 300 Burlington, Ontario L7L 5Y7

MENLO PARK
2882 Sand Hill Road, Suite 115 Menlo Park, California 94025

SEATTLE
Hawk Tower, 255 South King Street, Suite 800 Seattle, Washington 98104

ActZero ActZero ActZero.ai