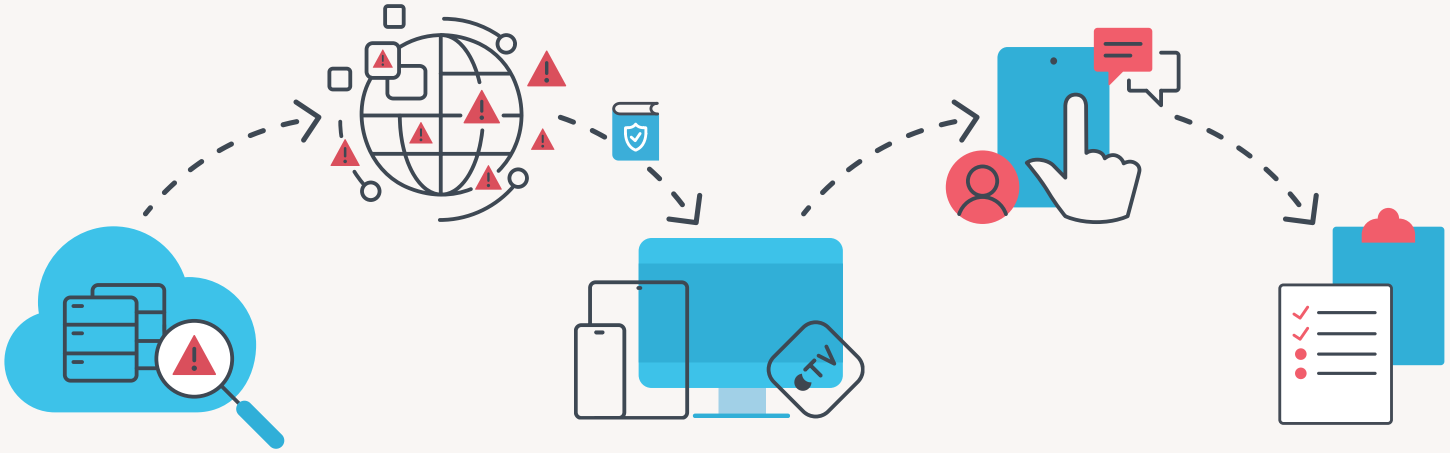
Advanced Guide to Incident Response and Remediation

> “Computer security incident response has become an important component of information technology (IT) programs. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources.”

The excerpt above from the National Institute of Standards and Technology (NIST) perfectly underscores the importance of having an effective plan when responding to security incidents. The faster the response, the more managed the risk may be to contain by minimizing the potential scope of exposure. The second half of this equation — the remediation process — will vary greatly depending on the tools available to IT. By aligning with the proper recovery tools, remediation time for compromised systems can be significantly reduced.



By identifying the assets and resources in the enterprise and performing a thorough assessment of possible and potential risks, organizations will be armed with the information required to develop robust response plans for incident handling. Additionally, this information will provide insight into what tools are necessary to manage, monitor and patch endpoints as well as remediate them expeditiously to minimize all forms of loss.

In this guide, we address:

- How to develop effective, robust playbooks to handle incident response for varied threats
- Why equipping IT with the right tools is paramount to successfully assessing, responding to and recovering from security threats
- A purpose-built security solution is the best way to secure your Apple fleet

“An ounce of prevention…

Is worth a pound of cure.” Quoted by Benjamin Franklin, the saying is just as true today as it was when he initially said it. And it could not be more fitting for IT protecting against cybersecurity threats and attacks.

Having the proper policies, people and tools in place are tantamount to successfully mitigating incidents and remediating any affected devices in a timely, efficient manner, cuts down the potential of the threat to system processes and business continuity in meaningful ways.

Knowing is half the battle

This helps your reputation as a company — especially among prospective hires, who search review sites to gain information on how a company operates and view comments from former employees.

Perhaps not half, but a significant part of the equation. After all, how can something possibly be protected if no one knows anything about it? Hence the case for inventory management and ensuring that it is kept up to date is imperative to protect all assets.

> It is a good practice in general for organizations to keep tabs on the equipment and peripherals they own, as well as where they are located and to whom they may be assigned — an essential piece of information for both company-owned or BYOD devices.

With inventory data in hand, this information becomes an invaluable tool, helping to shape the decisions being made regarding the types of security that devices will require, including what services will need to be procured to ensure they are fully protected to the extent of their capabilities. Not all assets perform the same functions, so why would a generic solution be the right fit for such dynamic technologies? The answer is that often, as in the case of Apple products, for example, generic solutions are not the best fit since they do not offer the types of comprehensive coverage and insight that purpose-built products, like Jamf Protect, offer.

But more on procurement of tools later in this guide. For now, let’s focus on identifying and inventorying equipment, and their respective uses, to provide an accurate picture of what equipment the organization owns and what it is used for. Be sure to include any valuable services these devices may provide, such as identifying public-facing servers that provide web content, mobile devices used in telehealth that store medical records or private patient data and so on. This information will come in very handy during the next phase in continuing to prepare.

If this, then that

Armed with a full inventory, the next phase is Risk Assessment, or determining what threats the devices are susceptible to, the probability that the threat will be exploited and what the potential fallout could be – and how all of that ties back to and affects the organization's business continuity plan.

Assessing risk factors is not for the faint of heart. It requires a lot of information to provide an accurate landscape of the devices in the organization. Additionally, in-depth knowledge of technical, security, financial, administrative and perhaps even legal may be necessary to properly determine the correct valuation of devices and the services they render. This is to say that assessing risk properly does not happen in a vacuum, but rather involves many stakeholders to account for all possible evaluations of a product or service before a final determination can be reached. Ultimately, the extent of the involvement of multiple departments will rely on the company's culture and governance, with even a basic level of risk assessment better than none at all.

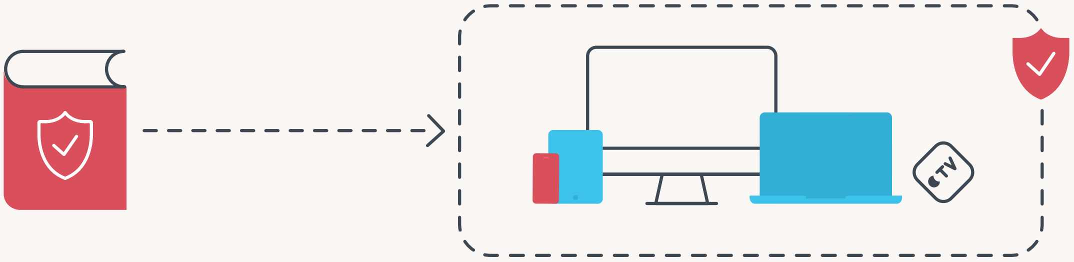
Let's utilize the web server mentioned in the previous section as an example. Web servers are inherently public-facing, which means they are directly accessible from a public network like the Internet. This makes it a higher value target compared to other devices that are otherwise accessible behind a firewall – not in front of it. If this web server acts as the front-end to a web application that stores user information on a database-driven back-end, then the risk value has just gone up because it is both linked to a back-end system (database) and it acts as the gateway to accessing personally identifiable information (PII) or private user data. If this web server processes survey data for customer service reports to gauge interest in new product offerings, you probably would not want this information leaking due to a data breach. However, if your company gathers this information as its sole revenue stream, a data breach could be significant enough of an event to severely affect the organization's future. Hence, the latter scenario would garner a much higher risk evaluation than the former, since one could effectively prevent the organization from continuing to operate for a period of time versus ceasing business operations altogether.

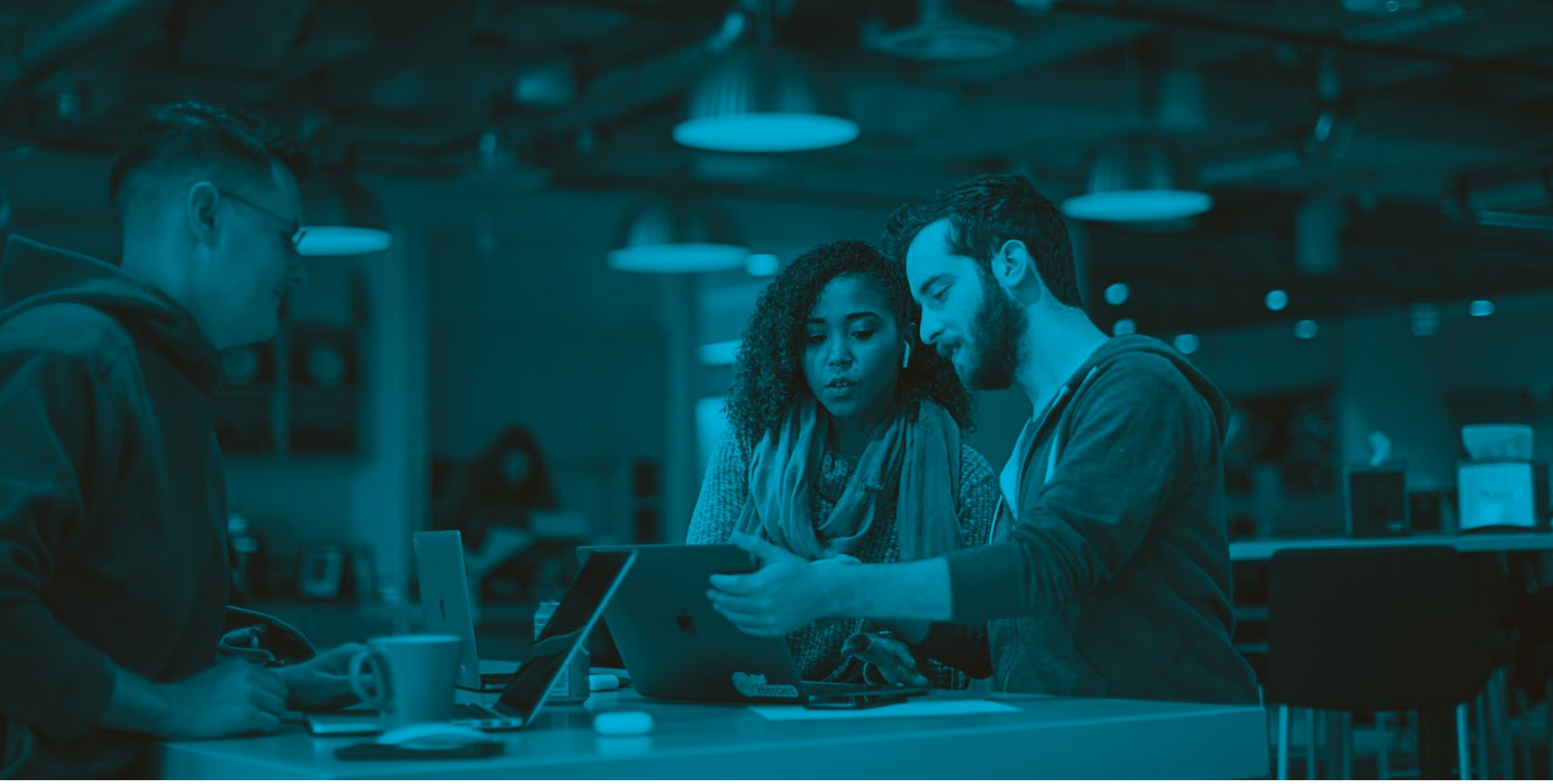
This is the way

Knowing what the organization has and how to respond to incidents are two related, but separate things. The tool that determines how the organization will classify and handle incidents based on the data obtained thus far should be crafted as part of company policies. These serve as guidelines for how to navigate any number of possible incidents as they arise.

Given that when computer security incidents occur, speed of response is of the utmost importance, having a clear set and defined "rulebook" for how to handle a situation will greatly alleviate any uncertainty, allowing Computer Security Incident Response Teams (CSIRTs) to spring into action immediately — regardless of the size of the team or if working with external partners — with a clear and concise plan of action to make short work of any threats detected. While policies can vary by organization, NIST describes several key elements that are crucial to developing organizational policies governing incident response:

- Statement of commitment to management
- Purpose of the policy and its objectives
- Policy scope
- Definitions of security incidents and terms relative to the organization
- Organizational structure, which includes the following:
    - Defined roles and responsibilities of stakeholders
    - Stakeholder authority levels
    - Information sharing requirements
    - Workflow for handoff and escalation points
- Risk assessment and incident severity levels
- Performance or baseline metrics
- Reporting procedures and contact tree





This is how we do it

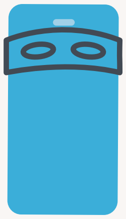
There are elements to the policy that governs how incidents are to be responded to. Then there are elements to the incident response plan itself, which details the stakeholders and the respective steps they must take when responding to an incident. Remember, everyone has a role to play – regardless of whether it is hands-on or calling the shots behind the scenes – it is most certainly a team effort and the plan itself serves as the roadmap with a focused and coordinated approach to responding to incidents based on the unique requirements of the organization, while leveraging its capabilities and partnerships to maximum effectiveness.

Similar to the policies above, the plan itself can and will vary greatly based on the organization's mission, size, structure (including senior management support) and functions. Key elements to consider when developing a successful plan include:

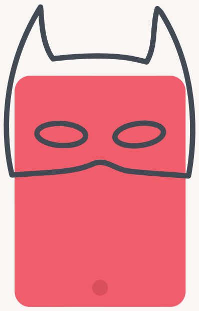
- Mission statement
- Strategies and/or goals
- Organizational approach
- Approved communication processes
- Metrics measuring effectiveness
- Process for optimizing capabilities
- Integration into the organization's processes

Avengers assemble

By now, the organization should have a team in place or at least an idea of who can be a good fit and at what capacity they contribute to the incident response model. For example, members of the IT and Information Security departments are ideal choices for response team membership. Additionally, individuals with project manager strengths can be essential to the remediation process by organizing and scheduling any processes required to complete remediation in a timely manner. Ultimately, this too will vary, with larger organizations usually having an internal team dedicated to handling these types of security concerns. Smaller organizations or those with limited capabilities are urged to form partnerships with providers to outsource incident response in part or in whole.



Even larger, dedicated teams will often form partnerships with vendors and other third-parties, such as law enforcement and the United States Computer Emergency Readiness Team (US-CERT) in the U.S., which is responsible for, among other things, coordinating incident response teams and activities. Other vendor partnerships may provide similar services and companies are urged to become familiar with the governmental organization that oversees incident response in their respective country for additional support, if necessary. Especially when they're missing expertise or for more severe incidents.



Developing response teams can require a great many questions to be answered prior to creating the team that best suits the organization's needs. The following questions will help in the development of these teams and/or in creating partnerships to fill skills or requirement gaps:

- Will the team perform best as a single, centralized model or distributed model across multiple locales?
- Who will handle coordination among all internal and external teams, including 3rd-party entities, like US-CERT?
- How will industry regulation, if any, affect the type(s) of incident response support the organization is able to develop or partner with?
- Is there adequate internal staff to manage incidents in a timely manner, or will partial/full outsourcing be required to fill the needs gap?
- What are the availability requirements of the incident response team? Considerations for 24/7/365 availability or full-time vs part-time support?
- What, if any, budget considerations are required to properly fund the team, including salaries, paid time off (PTO), addressing skills gaps and continuing education?
- For smaller organizations, what are the options that exist to keep assets protected when dedicated teams are not feasible? Including what planning is required to ensure that quick response is available, when necessary.

If you only have a hammer, everything looks like a nail

"The law of the instrument is a cognitive bias that involves an over-reliance on a familiar tool." This idiom illustrates how relying on one tool may lead to seeing only part of the picture when it comes to the security posture of the devices owned by your organization. An obstructed view is a problem because potentially important information is not visible and since decisions should be made on visible data only, this could lead to poor decision making.

How does this relate to incident response, you ask? The connection between being alerted to a potential threat and dispatching the CSIRT to remediate it is fairly evident. However, there are two important factors to consider: before the alert is raised and during the remediation phase itself. These are the two key phases where the correct tools can – and will – make all the difference between resolving the issue quickly or not.

Before the alert is received, it must be triggered. The tools an organization ideally uses will provide alerting capabilities based on actively monitoring the endpoint using tried and true signature-based methods to stop known malware. Augmenting this detection type, a strong, capable method based on heuristics, or analytics, will detect potential malware, other attackers or potentially rogue employees based on behavioral patterns. This is especially useful for alerting teams to possible threats for currently unknown malware or those that may be variants that are different enough to not have a definition just yet. The latter system allows IT to investigate indicators when an infection has been detected. During the investigative phase, team members need to validate the accuracy of detections to determine if they are false-positives or true-positives. The former is known to occur and by verifying them first, time and organizational resources can be saved; conversely, if detections are verified to be true-positives, the appropriate resources can be dispatched before detections can possibly grow to affect more endpoints or worse, lead to a full-scale data breach.

However, the monitoring and investigative phases make up a part of the incident response portion of the process. What about remediation? After all, your team has been alerted to an issue, they have actively determined that it is a true positive. But now what happens?

This is where the remediation portion of the process takes over and will rely on an entirely different set of tools to correct the problems found, returning the affected devices to their normalized, operational state. If you have not figured out by now, incident response and remediation processes will largely depend on the organization, their budget, partnerships and so forth. There is no "one size fits all" to determine the processes that work for each instance, only a set of best practices and guidance's that allow organizations the best opportunity to develop the plans, policies, people and tools that will offer them the greatest chance of success in responding to and remediating threats within the unique parameters of their organization's needs.

With this in mind, endpoint management tools should offer – at a minimum – the highest level of support for the devices to which they manage. This is to say that, in an Apple-centric environment, an endpoint management system that does not fully support Apple products because they may be several versions behind in supporting Apple's latest in security and device management frameworks could place IT, CISRT, stakeholders and the organization overall in a position where they may not be able to respond to threats as quickly as they would like to.

Furthermore, a lack of comprehensive support may not adequately address the holistic needs of the organization's information technology and information security policies, further putting a strain on stakeholders when incidents occur or simply when planning for change management projects, such as updating macOS as part of a recommended patch management strategy.

Arguably, the only feeling worse than having the tools to do something but lacking the knowledge to do it is having the capability to execute a task, but not having the proper tools with which to perform them with. It's frustrating for all stakeholders for a variety of reasons and adds undue stress on IT and security teams, especially when considering that time is of the essence when responding to and remediating detections, as resident Jamf expert, Bill Smith alludes to. Simply put, the wrong tools – whether they are designed for another OS or merely not up to the task of reporting and remediating as quickly and efficiently as the organization would like (or need) – may lead to potentially costly circumstances.

From delays in detection to reporting too much/little information to not providing IT and CSIRT teams the appropriate tools to resolve detections through remediated efforts, the right tool for the job can – and will – ensure that each technical process occurs smoothly. That kind of seamless integration that works in the background to keep devices protected, but can effortlessly pivot to isolating the root cause and remediating it is only possible through a combination of all the processes mentioned above working in harmony alongside purpose-built technologies, such as Jamf Protect and Jamf Pro, to keep your Mac secured from security threats and performing optimally through patch management, policy enforcement and same day support for the latest Apple features and updates.

Pass on what you have learned

This is to say, document your findings. All of them. Through documentation, stakeholders are given the opportunity to not only be informed as to the causes and resolutions of issues, but also allows for them to work together in developing new, possibly better solutions to address shortcomings to existing processes to further optimize the incident response and remediation workflows, policies and so on.

Documentation does not solely serve the purpose of recording what happened and what was done to correct it, then file it away and move on to the next fire to put out. While that is an important part of the process, there is much more information that can be gleaned from documenting findings and reviewing them regularly. This information has the ability to cause ripple effects throughout the entire incident response and remediation process, building toward greater efficacy of processes and cutting out what is unnecessary or simply detracts from or does not add value to the overall process.

Consider the culmination of the processes as cyclical in nature instead of linear. In the latter, once the final workflow is implemented, the process is complete. You move on to the next task and restart from the beginning. However, by viewing this in the context of the former, when the last workflow has been completed, it comes back full circle by bringing those findings back to the stakeholders for review. Providing an iterative step with feedback whereby the actions and reactions of each step can be analyzed and compared to established baselines, evolving capabilities & best practices, and changes in technology and processes for starters, to determine what – if any – changes can be made to significantly reduce risk, minimize the negative impacts on users, shave precious time from processes to make them more efficient and/or determine what training, software or hardware changes may provide an overall benefit to the organization's incident response and remediation policy.

The end goal to these processional changes being a better, leaner set of workflows that optimize security detection, response and remediation efforts while limiting risk, mitigating threats effectively and quickly. The aim is ultimately to align response and remediation plans with IT's mission to address the unique needs of the organization and its users, while keeping downtime as low as possible.

Learn how Jamf can partner with your organization in crafting a unique, incident response and remediation plan to holistically secure your Mac endpoints using purpose-built software and customized workflows that integrate seamlessly with Apple's architecture while providing your organization the tools necessary for successfully managing its Mac infrastructure.

Get Started with **Free Trial Today.**

Or contact your preferred reseller of Apple hardware to get started.