

10 Tips to Help You Minimize the Duration and Impact of a Security Breach

Incident Management and Response



Introduction

The SecureWorks Incident Management and Response team helps organizations of all sizes and across all industries prepare for, respond to and recover from even the most complex and large-scale security incidents.

Based on direct experience working with customers during security incidents over the past year, and incorporating threat intelligence on the latest tactics, techniques and procedures (TTP) that threat actors employ, the incident response team developed the following recommendations to help IT and IT security organizations minimize the duration and impact of a security breach.

What's it Going to Take to Change?

To help you prioritize changes to enhance the security of your environment, and to reduce the duration and impact of a security breach, we've added the following classifications to help you understand the level of complexity involved to implement the various recommendations:



Low Complexity

Can be implemented by management controls or IT staff



Medium Complexity

Can be implemented by IT staff with support of security professionals



High Complexity

Requires security professionals and possible outside consulting services

A layered incident response model, whereby internal resources are complemented by third-party expertise, can mobilize the optimal mix of skillsets and capabilities needed during a security breach.

Who Should Read This White Paper


- » CISO/CSOs
- » CIOs
- » CFOs
- » Directors of Security
- » Security Researchers
- » Security Architects


The Top 10 Tips


1. Have a Computer Security Incident Response Plan in Place Before You Need it

Problem: Many organizations don't have a basic Computer Security Incident Response Plan (CSIRP) in place. If a plan is in place, it is not regularly tested and revised.

Recommendation: For any organization that is serious about effectively responding to a security breach, we recommend IT and IT security professionals develop and test a Computer Security Incident Response Plan based on best practices.

 **Establish a Computer Security Incident Response Plan:** Establish a CSIRP that is compliant with the organization's applicable mandates (i.e., PCI/PFI, NIST, HIPAA) and addresses the specific requirements of the overall organization.

 **Test Your Incident Response Team:** Routinely test the CSIRP to assess procedures, identify gaps in execution and evaluate your team's proficiency in responding to a security breach. Testing should include multiple breach scenarios that address both commodity and targeted attacks.

 **Address Distributed Denial of Service (DDoS) Attacks in Your Plan:** If your critical business operations rely on your connectivity with customers from the Internet, ensure DDoS is addressed in your plan. Make sure recovery planning is rehearsed and stress tested, and can be implemented in close coordination between IT and IT security staff. Consider subscribing to a DDoS protection service, if necessary.

Why it's so Important: The CSIRP is the master document to help organizations plan for the contingency of a security breach. The document defines the roles, responsibilities and procedures of the incident response function within the organization. In essence, the document formalizes the incident response function within the organization and within the security stack.

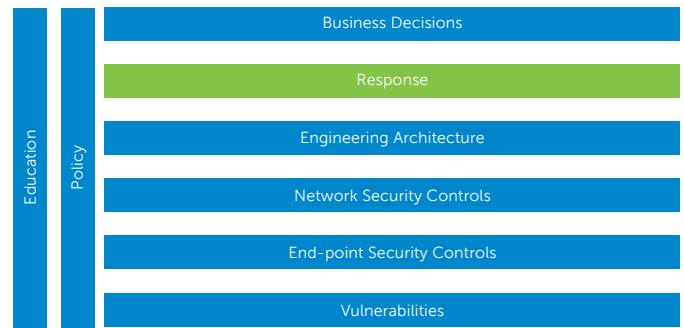


Figure 1 shows incident response (IR)


A good plan will detail roles, responsibilities, stakeholders, and response policies and procedures. A good plan will also provide actions to take during certain types of incidents, including incidents involving advanced or targeted threats (including Advanced Persistent Threats). Integral to implementing a good plan is testing the plan through various exercises and real-world testing scenarios. The only way to effectively tune the capabilities of your plan and your IR team overall is to conduct periodic testing of your capabilities and planning.

DDoS is an important area to consider in your CSIRP as well. The SecureWorks Incident Management and Response team has serviced customers who have been victims of a DDoS attack, as well as customers whose infrastructure was used by threat actors to conduct DDoS attacks. The DDoS attacks have had two different objectives. The first objective was to have an operational impact on the victim by making their network unavailable to customers. The second objective was to cover criminal activity by executing a DDoS attack just after completing an illegal wire transfer of funds from a user account.

2. Assess Current Incident Response Competencies, Identify Gaps and Take Proactive Steps to Enhance Capabilities

Problem: Organizations are overestimating their capacity to resolve security breaches quickly and effectively and, as a result, are making mistakes and prolonging resolution of an incident.

Recommendation: We recommend organizations perform a thorough assessment of their current incident response function and CSIRP, identify gaps and explore ways to enhance the IT and IT security's ability to respond effectively during a security breach.

 **Assess current capabilities and address gaps:** Organizations should assess and contrast their incident response needs (in terms of people, skillsets and tools required) with their existing competencies to identify gaps. This includes assessment of types of security breaches that can be handled by internal resources versus those requiring additional expertise. Organizations can address gaps in their capabilities either by hiring additional resources, or (if that isn't feasible or practical) retain services with a third-party provider that specializes in incident response.

Why it's so Important: Performing a proactive assessment of your incident response capabilities is critical to developing an incident response function that can handle all types of crises effectively and quickly.


A layered incident response model, whereby internal resources are complemented by third-party expertise, can mobilize the optimal mix of skillsets and capabilities needed during a security breach. This increases the organization's capacity to deal with a wide range of security breaches caused by commodity threats and targeted threats to include Advanced Persistent Threats (APT).


The SecureWorks Incident Management and Response team is regularly called into situations where IT and IT security resources unsuccessfully attempted to resolve an incident internally. This delays resolution of the incident, often due to the inadvertent destruction of evidence. In addition, the researching of vendor solutions and subsequent contract negotiations can add delays to any effective response, increasing the breach's overall impact.


3. Get Full Management and Executive Leadership Buy-in on the Incident Response Plan


Problem: At times, organizations lack executive sign-off on their incident response plans, which can create indecision and disagreement and, ultimately, delay resolution of a security breach.

Recommendation: We recommend IT and IT security leadership work with executive leaders and senior management as part of the overall process to prepare for and resolve a security breach.

 **Obtain leadership buy-in:** Get executive leadership sign-off on your plan

 **Articulate roles and responsibilities:** Address delegation of roles and responsibilities across all stakeholders in your plan.

 **Ask leadership to participate in practice and testing:** Have leadership participate in testing and tabletop exercises so they understand their roles and what to expect.

 **Have a communications plan:** Address communications to leadership and other critical persons in your plan.

- Internal: IT, senior leadership, Public Relations, legal, business units
- External: Customers, partners, regulators, law enforcement


Why it's so Important: The implications of a security breach are multifaceted and will span a number of managers and senior leaders across the organization. As a result, the organization's overall ability to resolve a security breach effectively and quickly will be contingent on all parties accepting their roles, and what's expected of them during a security incident.


4. Proactively Assess User Privileges and Accounts


Problem: Many organizations are not adhering to robust user and administrator privilege practices. As a result, attackers are able to gain undetected and unfettered access using actual employee privileges. Additionally, disgruntled former employees represent a significant risk for organizations.

Recommendation: We recommend organizations grant the lowest system access privileges permissible while still ensuring employees can do their jobs.


 **Implement Security Awareness Training:** Implement aggressive user training and certification to raise the level of awareness on types of threats. Tie user access and privileges to performance and compliance with training programs (i.e., restrict Internet access for non-compliance users).


 **Maintain strict access controls:** Restrict administrator access to regular users on local systems; segregate administrator and service accounts. Each function should have separate credentials for various elements of the environment, e.g., border routers, exchange server, domain controller/AD; backup service. When the administrator wants to perform normal user functions, they need to log in as user. Ensure that employees with domain-level administrator access are limited in number, are properly trained, and that they execute these duties in a secure, monitored and audited manner.

 **Tie access levels to job function:** Ensure access control is tiered and mapped to a data classification program where users only have access to data they need to do their jobs. Attributes tied to data access should be determined as part of the Human Resources onboarding process.

 **Establish a process to delete terminated employee privileges:** Coordinate with Human Resources to get advance notice of pending terminations of employees. Managers of employees with

elevated privileges should be cognizant of the risk their employees pose to the organization, and take appropriate action to restrict access when warranted by an employee's poor performance or misconduct.

 **Use two-factor authentication:** Implement two-factor authentication, especially for remote access through a VPN.

 **Use an alternate token:** Implement an alternate token for administrator access.

Why it's so Important: Though it may seem mundane, implementing strict controls and close monitoring of account privileges can help identify unusual activity and actions that may indicate a threat operating within your environment.

The SecureWorks Incident Management and Response team has seen numerous incidents where the actor was able to obtain and expand privileges, and roam freely within the network environment. However, if effective controls and monitoring had been in place, these organizations would have detected malicious activity much sooner, significantly reducing the duration and impact of the overall incident.

Organizations must also be diligent regarding terminated employees. Former employees who still have working login credentials pose a serious risk. Information Security's 2015 "Insider Threat Spotlight," report states 62 percent of security professionals say insider threats have become more frequent in the last 12 months. But only 34 percent expect additional budget to address the problem.

5. Collect and Analyze Log Data

Problem: Many organizations do not sufficiently collect, analyze and retain log information.

Recommendation: We recommend that logging collection, analysis and retention be conducted with the greatest breadth and depth possible.



Implement a log management solution:

Implement a log management solution to centralize, analyze, and report on patterns, anomalies and overall log traffic flows. The four most critical logs to help resolve an incident are firewall logs, DNS server logs, domain controller logs and Virtual Private Network (VPN) appliance logs. As such, organizations must pay special attention to retaining these logs. Collect log data for anomalies as frequently as possible. A good rule of thumb is to collect and retain logs for 3 to 6 months.



Perform log analysis: Optimize event logging to ensure you are capturing all relevant security events that could be elevated to security incidents. Ensure analytics are conducted on these event logs based on a reputable set of threat indicators to look for threat activity that may be avoiding your signature-based defense appliances. A good rule of thumb is to analyze logs at least weekly.

Why it's so Important: Regular analysis of log data will ensure that your team has the opportunity to detect a breach at the earliest possible moment and before an actor can do irreparable harm. Should a breach occur, having raw log data available for analysis will help incident responders piece together when and how the breach occurred and will help them capture digital traces of the actor's progression in your network.

6. Control Traffic Flows

Problem: Many organizations are putting critical infrastructure on addressable IP space.

Recommendation: We recommend IT and IT security professionals review their current network architecture and communications traffic flows to ensure systems are appropriately segregated from the Internet, and web traffic is routed in a secure manner.



Restrict server access to the Internet: Restrict most servers from directly accessing the Internet. There is no reason a domain controller should have a direct connection to the Internet. Only

applications with a true web-facing need should access the Internet. Additionally, servers requiring direct Internet access should only use essential ports and protocols.



Route all web traffic through proxy servers located in a DMZ

Why it's so Important: The ability to constrain a potential adversary in the available pathways into and out of an organization is a key aspect to increasing the means to detection. A small "attack surface" works to the advantage of the organization. Reducing communication paths to the Internet causes choke points that an attacker must go through. And with these "choke points" adequately instrumented, an organization improves its overall defensive security posture.

7. Conduct Network Monitoring

Problem: Many organizations don't have network monitoring in place, limiting visibility to activity occurring within their networks.

Recommendation: We recommend organizations implement network monitoring and staff resources appropriately to monitor for unusual activity within their networks.



Implement a Security Information and Event Management (SIEM) solution: Whether outsourced to a third party or insourced, an SIEM can provide near real-time alerts for activities that put your organization at risk.


Why it's so Important: SecureWorks has documented how sophisticated threat actors will work to expand access and privileges once inside your network, installing more than one exploit along the way. It is critical for organizations to have visibility into what is happening in their network environments and across their boundaries at all times.

8. Perform Web and Email Filtering


Problem: Email remains a significant threat vector for malicious actors to exploit.

Recommendation: We recommend IT and IT security professionals adopt more stringent web and email security practices across their environments and users.

 **Block commercial webmail access on the network**

 **Implement web and mail proxies:** A “Stop and Inspect” process is essential for ensuring “bad” traffic is identified as early as possible.

 **Ensure high-risk email attachments (i.e., EXE, RAR, SCR) are stripped from all inbound mail**


 **Evaluate in-line traffic filtering:** Consider implementing enhanced, in-line filtering of email and web traffic where executable code is discovered with both signature-based indicators and in-line sandbox discovery. Ensure SSL traffic is decrypted at the boundary and inspected for threat activity as well.


Why it's so Important: End users are still the primary target for both commodity (non-targeted malware) and Advanced Threat (targeted tradecraft) attacks. Social engineering and reconnaissance are on the rise, making phishing and spear phishing campaigns more convincing and enticing for end users to fall prey to these efforts.


9. Perform DNS Monitoring

Problem: DNS is both a frequent target for DDoS attacks and a useful service for malicious code writers.

Recommendation: We recommend organizations put proper security controls and monitoring in place to prevent DNS attacks.

 Rate limit DNS traffic in your network configuration to guard against both inbound and outbound DNS UDP traffic, and to protect against both receiving and participating in a DoS attack.

 Ensure critical network infrastructure (i.e., DNS, domain controllers, routers) are on non-routable IP space and do not respond to ping sweeps.

 Record client DNS requests for as long as practical. This will capture malware server requests if hostile code has been activated at the client.


Why it's so Important: DNS is essential to finding public web sites. Denial of Service (DoS) attackers know that if they can misdirect DNS lookups for your organization, they can deny service to your customers without actually having to take down your web servers. The end result is ultimately the same — a denial of service to your customers — though a DNS attack can be much easier to perpetrate. Attackers can also use DNS to change the location of their command infrastructure without having to replace malware already deployed in the field.

Having a record of client DNS transactions will immediately assist in finding potentially compromised host systems for rapid containment and remediation.

10. Apply Threat Intelligence to Enhance Incident Response and the Security Stack

Problem: Many organizations fail to capitalize on threat intelligence that can enhance the incident response function, provide advance warning of threats, and improve the overall security posture throughout the security stack.

Recommendation: For those organizations with a more mature security stack and incident response function, we recommend the adoption of threat intelligence to further heighten incident response and general security capabilities and all aspects of IT decision-making.

 **Integrate threat intelligence:** IT and IT security teams should utilize threat intelligence to train IR personnel to Tactics, Techniques and Procedures (TTP) of attackers, enhance the security stack and improve overall and response-related decision making. Organizations should allocate the required resources to implement recommendations across the network and environment.

Why it's so Important: Threat intelligence's value to organizations is multifaceted. Threat intelligence can be used to improve security controls up and down the security stack as outlined below. For instance, threat intelligence can provide specific recommendations for IT and IT security teams to follow to prevent a security breach by new malware.

Threat intelligence can raise awareness of the Tactics, Techniques and Procedures (TTP) of threat actors across the IT organization and provide insights to better guard against and respond to a security breach. Threat intelligence can also provide advance warning of threat actors who are specifically targeting the organization so that incident response teams can preempt the attack through internal preparations.

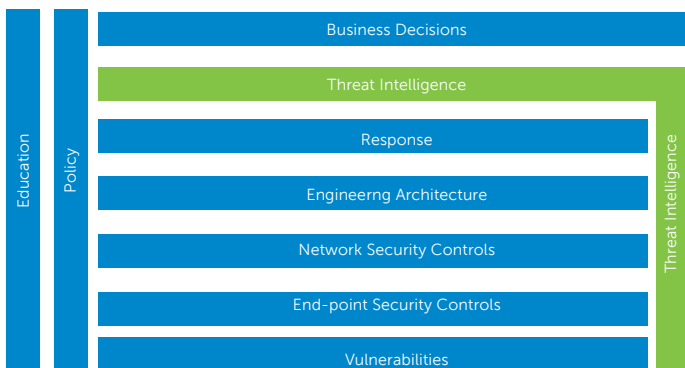
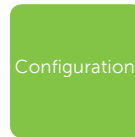


Figure 2: Threat intelligence embedded into the security stack

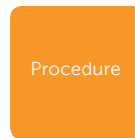
Additional Recommendations



- Adopt server and workstation inventory control
- Sinkhole all dyndns and known bad domains (using opendns as a forwarder)
- Block large portions of foreign IP space known to be used in attacks and not required for corporate needs
- Implement an authenticated web proxy
- Implement Netflow collection on your internal network



- Implement configuration management/standardization
- Implement network segmentation to control data flows, and allow for efficient monitoring and control instrumentation
- Regularly review firewall rulesets and other external ingress/egress paths
- Configure email services to prevent and alert on address spoofing
- Prevent the use of webmail services and potentially other social media/IM and other non-business services from corporate network/resources



- Implement a process for escalation of spear-phishing attempts
- Regularly review server/application connectivity needs and allow exceptions for updates
- Use a privileged account management system
- Assess log management needs and requirements
- Establish tabletop and testing to perform real-world simulations to improve your team's capabilities
- Create a process to monitor updates for third-party apps such as Java, Flash and Acrobat

Additional Information

The SecureWorks Incident Management and Response service provides rapid containment and eradication of threats, minimizing the duration and impact of a security breach. Leveraging elite cyber threat intelligence and global visibility, we can help you prepare for, respond to and recover from even the most complex and large-scale security incidents.

About SecureWorks

SecureWorks provides an early warning system for evolving cyber threats, enabling organizations to prevent, detect, rapidly respond to and predict cyber attacks. Combining unparalleled visibility into the global threat landscape and powered by the Counter Threat Platform — our advanced data analytics and insights engine — SecureWorks minimizes risk and delivers actionable, intelligence-driven security solutions for clients around the world.



For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com