Incident Response

What is Incident Response (IR)?

Incident Response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack (also known as an incident). IR involves people, process, and technology, to detect and respond to the attack. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

What is an Incident Response plan?

An IR plan includes a policy that specifically defines what constitutes an incident, who is responsible for responding to the incident within the company, and what step-by-step process should be followed when an incident occurs.

What are some examples of incidents?

Some common categories of incidents: are unauthorized access to critical resources, denial of service of a web application, endpoint compromised by malware (via phishing attack), suspected breach (exposure) of sensitive information (medical records, customer contacts), and loss of personal identifiable information (email addresses, usernames/passwords).

Who is responsible for IR in a company?

Security is a C-level and board level issue. Ultimately senior executives are responsible for ensuring that a robust IR plan is in place. When a major incident happens, the head of IT/security provides updates to the CEO/CIO and the board, depending on the severity of incident and measures taken to respond to the attack and mitigate the risk of a similar breach in the future.

Who should be on the IR team?

The most effective IR teams are cross-functional and include representatives from senior-level executives to HR, finance, PR, IT and security teams so every chain of command understands how to identify and react to an incident that may affect them. For example, depending on the magnitude of an incident, forensics will be conducted by the security team and corrective actions will be taken by network/system administrators. Business functions such as finance or human resources will have protocols to follow, as confidential financial or employee information is often at risk when there is a cyberattack.

How do you ensure IR readiness?

IR planning, testing, and execution needs to be championed from the executive level to maintain the focus and resources required for developing and sustaining an effective IR plan. Once a plan is in place, regular readiness drills (like fire drills) should also be conducted on a monthly or quarterly basis so all team members have a chance to practice their response before an incident happens.

How can investment in IR show value in tight budget situations?

Senior management needs to be made aware of the business risks facing an organization to show the value of an IR team and repeatable processes to their executive boards. This can be done by providing data on attempted attacks, mitigated incidents, cyberattacks, and recent breaches encountered in their industry segment. Another way to provide convincing and unbiased metrics is to engage a third party managed detection and response (MDR) service provider to evaluate and manage your response plan.

Arctic Wolf offers an affordable SOC-as-a-Service that deploys in less than 60 minutes, continuously monitors and analyzes your IT infrastructure for cyberattacks, and ensures proactive detection and rapid response to threats. It implements incident response and reporting best practices to provide hard data on any attempted breaches. This service also saves costs, as less time and resources are spent on forensics analysis and chasing false positives.

ARCTIC WOLF

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com