Escalate with a purpose

You previously learned about security incident escalation and the skills needed to help you escalate incidents. In this reading, you'll learn the importance of escalating security issues and the potential impact of failing to escalate an issue.

Incident escalation

Security incident escalation is the process of identifying a potential security incident. During this process, potential incidents are transferred to a more experienced department or team member. As a security analyst, you'll be expected to recognize potential issues, such as when an employee excessively enters the wrong credentials to their account, and report it to the appropriate person. When you join a new organization, you'll learn about the specific processes and procedures for escalating incidents.

Notification of breaches

Many countries have breach notification laws, so it's important to familiarize yourself with the laws applicable in the area your company is operating in. Breach notification laws require companies and government entities to notify individuals of security breaches involving personally identifiable information (PII). PII includes identification numbers (e.g., Social Security numbers, driver's license numbers, etc.), personal medical records, addresses, and other sensitive customer information. As an entry-level security analyst, you'll need to be aware of various security laws, especially because they are regularly updated.

Low-level security issues

Low-level security issues are security risks that do not result in the exposure of PII. These issues can include the following and other risks:

- An employee having one failed login attempt on their account
- An employee downloading unapproved software onto their work laptop

These issues are not significant security challenges, but they must be investigated further in case they need to be escalated. An employee typing in a password two to three times might not be of concern. But if that employee types in a password 15 times within 30 minutes, there might be an issue that needs to be escalated. What if the multiple failed login attempts were a malicious actor attempting to compromise an employee's account? What if an employee downloads an internet game or software on their work laptop that is infected with malware? You previously learned that malware is software designed to harm devices or networks. If malware is downloaded onto an organization's network, it can lead to financial loss and even loss of reputation with the organization's customers. While low-level security issues are not considered significant security threats, they should still be investigated to ensure they result in minimal impact to the organization.

The escalation process

Every company has different protocols and procedures, including unique escalation policies. These policies detail who should be notified when a security alert is received and who should be contacted if the first responder is not available. The policy will also determine how someone should specifically escalate an incident, whether it's via the IT desk, an incident management tool, or direct communication between security team members.

Key takeaways

Incident escalation is essential for protecting an organization's data. Every organization might have a different way of escalating security incidents. A security analyst should be aware of the escalation protocols that are in place at their organization. Both small and large security issues should be escalated to the appropriate team or team member.

Mark as completed