Escalation timing

You previously learned about the potential impact even the smallest incident can have on an organization if the incident is not escalated properly. You also discovered just how important your role as an entry-level analyst will be to the effectiveness of an organization's escalation process.

This reading will go into more detail about the role you'll play in protecting an organization's data and assets when it comes to escalating incidents.

Your decisions matter

Security is a fast-paced environment with bad actors constantly trying to compromise an organization's systems and data. This means security analysts must be prepared to make daily decisions to help keep a company's data and systems safe. Entry-level security analysts help the security team escalate potential security incidents to the right team members. A big part of your role as a security analyst will be making decisions about which security events to escalate before they become major security incidents.

Trust your instincts and ask questions

Confidence is an important attribute for a security analyst to have, especially when it comes to the escalation process. The security team will depend on you to be confident in your decision-making. You should be intentional about learning the organization's escalation policy. This will help you gain confidence in making the right decisions when it comes to escalating security events. But remember to ask questions when necessary. It shows that you're committed to constantly learning the right way to do your job.

All security events are not equal

An important part of escalation is recognizing which assets and data are the most important for your organization. You can determine this information by reading through your onboarding materials, asking your supervisor directly about which assets and data are most important, and reviewing your company's security policies. When you have that type of understanding, it allows you to recognize when one incident should be given a higher priority over others. You previously learned about the following incident classification types:

- **Malware infections:** Occur when malicious software designed to disrupt a system infiltrates an organization's computers or network
- **Unauthorized access:** Occurs when an individual gains digital or physical access to a system, data, or application without permission
- **Improper usage:** Occurs when an employee of an organization violates the organization's acceptable use policies

Identifying a specific incident type allows you to properly prioritize and quickly escalate those incidents. Remember, an incident which directly impacts assets that are essential to business operations should always take priority over incidents that do not directly impact business operations. For example, an incident where unauthorized access has been gained to a manufacturing application should take priority over an incident where malware has infected a legacy system that does not impact business operations. As you gain experience in the cybersecurity field, you will learn how to quickly assess the priority levels of incident types.

Quick escalation tips

A big part of your role in cybersecurity will be determining when to escalate a security event. Here are a few tips to help with this:

- Familiarize yourself with the escalation policy of the organization you work for.
- Follow the policy at all times.
- Ask questions.

Key takeaways

Incident escalation will be an important part of your role within a security team. Entry-level analysts are expected to identify and escalate incidents related to their daily work. Reading and understanding your organization’s escalation policy will be helpful in this responsibility. The escalation policy will describe how and to whom you should escalate incidents. When in doubt, never be afraid to ask a supervisor about the escalation process. This will help you stay knowledgeable about your job and make informed decisions.