The importance of escalation

Security analysts are hired to protect company assets and data, including knowing when and how to escalate security incidents.
In this video, we'll define security incident escalation and discuss your role in making decisions that help protect your organization's data and assets.
So what is incident escalation?
And why is it so important for security professionals?
Incident escalation is the process of identifying a potential security incident, triaging it, and (if appropriate) handing it off to a more experienced team member.
It's important to also recognize that not every incident needs to be escalated.
In this video, we'll cover what types of incidents should be escalated.
As an entry-level analyst, it's unlikely that you'll be responding to security incidents independently.
However, it's important that you know how to evaluate and escalate incidents to the right individual or team when necessary.
Let's discuss the essential skills needed to properly escalate security incidents.
There are two essential skills that will help you identify security incidents that need to be escalated: attention to detail and an ability to follow an organization's escalation guidelines or processes.
Attention to detail will help you quickly identify when something doesn't seem right within the organization's network or systems.
Following a company's escalation guidelines or processes will help you know how to properly escalate the issue you've identified.
Larger organizations' security teams have many levels, and each level, or member, of that team plays a major role in protecting the company's assets and data.
However, smaller and medium sized companies have only one or two people responsible for the organization's security.
For now, we'll focus on the roles in bigger organizations.
From the Chief Information Security Officer, also known as the CISO, to the engineering team, public relations team, and even the legal team, every member of the security team matters.
Each team member's role depends on the nature and scope of the incident.
These roles are highlighted within a company's escalation process.
Even the smallest security incident can become a much larger issue if not addressed.
And that's where you come in!
Imagine you're working at your desk and notice what appears to be a minor incident, but you decide to take a break before addressing or escalating it.
This decision could have major consequences.
If a small issue goes unescalated for too long, it has the potential to become a larger problem that costs the company money, exposes sensitive customer data, or damages the company's reputation.
However, with a high-level of attention to detail, and an ability to follow your organization's escalation guidelines and processes, it may be possible to avoid exposing the business, and its customers, to harmful incidents.

As an entry-level analyst, you play an important role.
You help the security team identify issues within the network and systems and help make sure the right person on the team is alerted when incidents occur.
Think about an assembly line.
Would the final step in the line be negatively impacted if the first step were done incorrectly, or not at all?
Of course it would!
Every decision you make helps the entire security team protect an organization's assets and data.
Knowing when and how to escalate security incidents is one of many important decisions you'll need to make on a daily basis.
Later in this course, we'll discuss the various levels of security incidents.
Knowing those levels will help you determine the level of urgency needed to escalate different incident types.

Revision #1
Created 2024-01-07 12:09:03 UTC by naruzkurai
Updated 2024-01-07 12:09:13 UTC by naruzkurai