Incident response teams

Hi again! In this section, we'll discuss how incident response teams manage incidents.

You may have been part of a team before. Whether it was a sports team, or a team in the workplace or at school,
teams are most successful when everyone uses their diverse strengths to work towards a common goal.

Incident response teams aren't any different.
A successful response to security incidents doesn't happen in isolation.
It requires a team of both security and non-security professionals working together with defined roles.

Computer security incident response teams, or CSIRTs, are a specialized group of security professionals that are trained in incident management and response.
The goal of CSIRTs are to effectively and efficiently manage incidents, provide services and resources for response and recovery, and prevent future incidents from occurring.

Security is a shared responsibility, which is why CSIRTs must work cross functionally with other departments to share relevant information.
For example, if an incident resulted in the breach of sensitive data,
like financial documents or PII, then the legal team must be consulted.
Some regulatory compliance measures may require organizations to publicly disclose a security incident within a certain timeframe.
This means that CSIRTs must collaborate with the organization's public relations team to coordinate efforts for public disclosure.

So how exactly does a CSIRT function?
First, there's the security analyst.
The analyst's job is to investigate security alerts to determine if an incident has occurred.
If an incident has been detected,
the analyst will determine the criticality rating of the incident.
Some incidents can be easily remediated by the security analyst and don't require escalation.
But if the incident is highly critical, it gets escalated to the technical lead, who provides technical leadership by
guiding security incidents through their lifecycle.

During this time, the incident coordinator tracks and manages the activities of the CSIRT and other teams involved in the response effort.
Their job is to ensure that incident response processes are followed and that teams are regularly updated on the incident status.
Not all CSIRTs are the same.

Depending on the organization, a CSIRT can also be referred to as an Incident Handling Team, or IHT, or Security Incident Response Team, SIRT.
Depending on an organization's structure, some teams can also have a broader or specialized focus.
For example, some teams may be solely dedicated to crisis management and others may be incorporated with a SOC.
Roles can have different names too. For example, a technical lead can also be known as an Ops lead.

Regardless of the team's title or focus, they all share the same goal: incident management and response.

Now that you know a bit about incident response teams, we'll continue to learn about how incident response teams plan, organize, and respond to incidents.
I'll meet you in the next video.

Revision #1
Created 5 September 2023 10:21:02 by naruzkurai
Updated 1 November 2023 01:10:46 by naruzkurai