Roles in response

So far, you've been introduced to the **National Institute of Standards and Technology (NIST) Incident Response Lifecycle**, which is a framework for incident response consisting of four phases:

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-incident activity

As a security professional, you'll work on a team to monitor, detect, and respond to incidents. Previously, you learned about a **computer security incident response team (CSIRT)** and a **security operations center (SOC)**. This reading explains the different functions, roles, and responsibilities that make up CSIRTs and SOCs.

Understanding the composition of incident response teams will help you navigate an organization’s hierarchy, openly collaborate and communicate with others, and work cohesively to respond to incidents. You may even discover specific roles that you’re interested in pursuing as you begin your security career!

Command, control, and communication

A **computer security incident response team (CSIRT)** is a specialized group of security professionals that are trained in incident management and response. During incident response, teams can encounter a variety of different challenges. For incident response to be effective and efficient, there must be clear command**,** control, and communication of the situation to achieve the desired goal.

- **Command** refers to having the appropriate leadership and direction to oversee the response.
- **Control** refers to the ability to manage technical aspects during incident response, like coordinating resources and assigning tasks.
- **Communication** refers to the ability to keep stakeholders informed.

Establishing a CSIRT organizational structure with clear and distinctive roles aids in achieving an effective and efficient response.

Roles in CSIRTs

CSIRTs are organization dependent, so they can vary in their structure and operation. Structurally, they can exist as a separate, dedicated team or as a task force that meets when necessary. CSIRTs involve both nonsecurity and security professionals. Nonsecurity professionals are often consulted to offer their expertise on the incident. These professionals can be from external departments, such as human resources, public relations, management, IT, legal, and others. Security professionals involved in a CSIRT typically include three key security related roles:

1. **Security analyst**
2. **Technical lead**
3. **Incident coordinator**

Security analyst

The job of the **security analyst** is to continuously monitor an environment for any security threats. This includes:

- Analyzing and triaging alerts
- Performing root-cause investigations
- Escalating or resolving alerts

If a critical threat is identified, then analysts escalate it to the appropriate team lead, such as the technical lead.

Technical lead

The job of the technical lead is to manage all of the technical aspects of the incident response process, such as applying software patches or updates. They do this by first determining the root cause of the incident. Then, they create and implement the strategies for containing, eradicating, and recovering from the incident. Technical leads often collaborate with other teams to ensure their incident response priorities align with business priorities, such as reducing disruptions for customers or returning to normal operations.

Incident coordinator

Responding to an incident also requires cross-collaboration with nonsecurity professionals. CSIRTs will often consult with and leverage the expertise of members from external departments. The job of the incident coordinator is to coordinate with the relevant departments during a security

incident. By doing so, the lines of communication are open and clear, and all personnel are made aware of the incident status. Incident coordinators can also be found in other teams, like the SOC.

Other roles

Depending on the organization, many other roles can be found in a CSIRT, including a dedicated communications lead, a legal lead, a planning lead, and more.

Note: Teams, roles, responsibilities, and organizational structures can differ for each company. For example, some different job titles for incident coordinator include incident commander and incident manager.

Security operations center

A **security operations center (SOC)** is an organizational unit dedicated to monitoring networks, systems, and devices for security threats or attacks. Structurally, a SOC (usually pronounced "sock") often exists as its own separate unit or within a CSIRT. You may be familiar with the term *blue team*, which refers to the security professionals who are responsible for defending against all security threats and attacks at an organization. A SOC is involved in various types of blue team activities, such as network monitoring, analysis, and response to incidents.

SOC organization

A SOC is composed of SOC analysts, SOC leads, and SOC managers. Each role has its own respective responsibilities. SOC analysts are grouped into three different tiers.

Tier 1 SOC analyst

The first tier is composed of the least experienced SOC analysts who are known as level 1s (L1s). They are responsible for:

- Monitoring, reviewing, and prioritizing alerts based on criticality or severity
- Creating and closing alerts using ticketing systems
- Escalating alert tickets to Tier 2 or Tier 3

Tier 2 SOC analyst

The second tier comprises the more experienced SOC analysts, or level 2s (L2s). They are responsible for:

- Receiving escalated tickets from L1 and conducting deeper investigations
- Configuring and refining security tools
- Reporting to the SOC Lead

Tier 3 SOC lead

The third tier of a SOC is composed of the SOC leads, or level 3s (L3s). These highly experienced professionals are responsible for:

- Managing the operations of their team
- Exploring methods of detection by performing advanced detection techniques, such as malware and forensics analysis
- Reporting to the SOC manager

SOC manager

The SOC manager is at the top of the pyramid and is responsible for:

- Hiring, training, and evaluating the SOC team members
- Creating performance metrics and managing the performance of the SOC team
- Developing reports related to incidents, compliance, and auditing
- Communicating findings to stakeholders such as executive management

Other roles

SOCs can also contain other specialized roles such as:

- **Forensic investigators**: Forensic investigators are commonly L2s and L3s who collect, preserve, and analyze digital evidence related to security incidents to determine what happened.
- **Threat hunters**: Threat hunters are typically L3s who work to detect, analyze, and defend against new and advanced cybersecurity threats using threat intelligence.

Note: Just like CSIRTs, the organizational structure of a SOC can differ depending on the organization.

Key takeaways

As a security analyst, you will collaborate with your team members and people outside of your immediate team. Recognizing the organizational structure of an incident response team, such as a CSIRT or SOC, will help you understand how incidents move through their lifecycle and the responsibilities of different security roles throughout the process. Knowing the role that you and other professionals have during an incident response event will help you respond to challenging security situations by leveraging different perspectives and thinking of creative solutions.

Resources for more information

Here are some resources if you'd like to learn more about SOC organization or explore other incident response roles:

- The security operations ecosystem
-
- Cyber career pathways tool
-
- Detection and Response

at Google: Episode 2 of the Hacking Google series of videos

Revision #1
Created 5 September 2023 10:30:47 by naruzkurai
Updated 1 November 2023 01:10:46 by naruzkurai