Security Engineer Intro

Introduction

Security engineers form the backbone of an enterprise's cyber security posture. In this room, we will get an introduction to the security engineer role and learn the day-to-day activities of a security engineer. It is highly recommended that before continuing on this room, you have completed the Pre Security path.

Learning Objectives

- Why does the need for security engineers arise?
- What are the qualifications required to become a security engineer?
- What does a security engineer do in a typical day of work?

We might also discuss some additional roles and responsibilities that a security engineer in some places might have. Let's move forward to the next task to continue on our journey.

What is a Security Engineer?

Why Do Organizations Need Security?

As the internet age transforms how organizations work worldwide, it also brings challenges. While there is no doubt that technology has made the life of organizations a lot easier by opening new avenues of collaboration and innovation, we often hear about organizations getting hacked, losing customer data, getting ransomed, and facing other types of cyber attacks. In responding to these threats, organizations can either go back to the old ways of doing business without getting any aid from modern technology, putting them at a disadvantage, or they can move forward and ensure the security of the digital side of their business. Hence, just like any organization will protect its physical assets and dedicate whole departments to them, a company's digital assets must also be secured. It must be noted here that organizations do all of this to ensure their primary goal is achieved without hindrance.

The Role of a Security Engineer

Keeping in view the above-mentioned need for security, organizations hire security engineers. In order to hire a security engineer, an organization perceives a security engineer as someone who:

- Owns the overall security of an organization. The main person responsible for securing an organization's digital assets.
- Ensures that the organization's cyber security risk is minimized at all times.
- Devises strategies and creates systems that minimize the risk posed by cyber security threats to an organization.
- Periodically conducts tests to ensure the robustness of the cyber security posture of an organization, identifies weak points, and prepares mitigations.
- Develops and implements secure network solutions.
- Architects and engineers trustworthy, reliable, and secure systems.
- Collaborates and coordinates with other teams to establish security protocols across the organization.

Qualifications Required for a Security Engineer
As you might have noticed, the security engineer role mentioned above is very broad and might require a whole department instead of a single person. This is because this role is defined loosely and varies from organization to organization. An engineer takes large problems, breaks them down into smaller chunks, and then solves them. Therefore a security engineer is someone that follows this process for security problems. Meaning that even though you might have a job description, each day might be quite different since you are faced with various problems. Overall, when hiring a security engineer, organizations look for the following basic requirements:

- 0-2 years of experience with IT administration, helpdesk, networks or security operations.
- Basic understanding of computer networks, operating systems, and programming.
- Basic understanding of security concepts such as Governance, Risk and Compliance (GRC).

****

Answer the questions below:

Who ensures that an organization's cyber security risk is minimized at all times?
Answer: Security engineer

Core Responsibilities of a Security Engineer

In the previous task, we established that a security engineer is responsible for an organization's security posture. In this task, we will expand on the general expectations that an organization has from a security engineer in order to help them achieve their

goals in this role. Although loosely defined, a security engineer will often be responsible for the areas that follow.

Asset Management/Asset Inventory
One of the primary steps in ensuring an organization's security is to maintain an organization's asset inventory. In terms of cyber security, this will mean managing and maintaining an inventory of an organization's digital assets. Security engineers can only own an organization's security if they know what assets the organization has. They must also ensure that this asset inventory is regularly maintained and updated and includes all the required information about assets such as asset name, type, IP addresses, physical location, place in the network, applications running on an asset, access permissions (only within the organization or public-facing), and the asset owner details.

Security Policies
An organization needs robust security policies to maintain a sound security posture. A security engineer helps the organization create security policies based on established Security Principles. These policies are then implemented organization-wide, and the security engineer ensures that the implementation follows the letter and spirit of the policies. Sometimes, a need arises for granting exceptions to the security policies due to business needs. In such scenarios, the security engineer consults the security principles to allow or deny exceptions and suggest mitigating steps to minimize risks.

Secure by Design
A security engineer ensures that the organization is secure by design. The engineer understands that the security posture receives the most Return on Investment (ROI) if it follows a secure-by-design philosophy. This means that the security engineer takes steps to implement a Secure Network Architecture, ensures the organization's Windows, Linux, and Active Directory are hardened, and software development follows the Secure Software Development Lifecycle.

Security Assessment and Assurance
While securely designing the organization's network and infrastructure might be an excellent first step, a security engineer understands that their job is far from done after that. They understand that security is hard work that requires continuous effort. While a security engineer must ensure everything is done correctly, a compromise requires just one loophole to be successful. To mitigate risks from a continuously evolving threat landscape, a security engineer plans to conduct regular security assessments, audits, and red-teaming and purple-teaming exercises to continuously improve the security posture. While security engineers might not be performing assessments and audits themselves, they are primarily involved in helping schedule these activities, creating

Request for Quotations (RFQs) for external parties to perform these activities, and helping prioritize and implement the findings from them.

****

Answer the questions below:

Where are details about an organization's digital assets, such as name, IP address, and owner, stored?
Answer: Asset Inventory

Sometimes security policies can't be followed because of business needs. What avenue does a security engineer have to fulfil business needs in these cases?
Answer: Exceptions

What philosophy, if followed, provides the most Return on Investment (ROI)?
Answer: Secure by design

Continuous Improvement

An organization's security is not a one-time job but a continuous effort. Similarly, the security engineer's job doesn't end once policies are designed and implemented. Rather, it is a journey towards continuous improvement. The following steps help a security engineer carry out this role.

Ensuring Awareness

A security engineer might be tasked with maintaining a certain security awareness level in the organization. Humans are the building blocks of any organization, and as is often said, humans are the weakest link in an organization's security. A security engineer periodically runs awareness sessions targeting primarily social engineering attacks to ensure that humans don't make mistakes that can compromise an organization's security. Awareness sessions are also organized for specific teams to ensure they follow security principles related to their area of expertise, like secure software development or secure network architecture.

Managing Risks

The executive management of most organizations looks at security from the lens of minimizing risks. Security is essential to businesses because ignoring it can result in

operational disruptions, data leakage, lawsuits, or other forms of risk. Therefore, a security engineer is often tasked with identifying security risks, determining their likelihood and impact, and finding solutions to minimize those risks. It must be noted that eliminating all risks might not be possible when running business operations. Sometimes, a decision has to be made to accept a risk and move on. In such a scenario, the security engineer might perform some mitigating actions to lower the risk. Accepting or mitigating risks is often a business decision, and a security engineer acts as a trusted advisor of the management that helps them take this decision by providing subject matter expertise. Let's take the example of an organization that uses a database software for its supply chain that runs on a vulnerable version of Linux. This software is essential to the organization's operations. Updating the software, so that it can run on the latest OS version that is not vulnerable, without impacting operations might take significant effort (more than a year). It will require engagement with the vendor, who has not yet tested the software on the latest OS version. Deploying the software without testing on the latest OS version will risk causing problems in the organization's operations. In such a scenario, the vulnerable OS version poses a security risk. A security engineer might suggest mitigating the risk by hardening the OS through additional controls and adding a reverse proxy in front of the vulnerable system to avoid exposing it to the internet. While these steps will not eliminate the risk, they will significantly reduce it without affecting the organization's operations.

Change Management

Organizations keep evolving with time, which also results in changes in their security posture. To ensure a robust security posture, the security engineer keeps track of changes in the organization's digital assets that can affect the security posture and takes measures to improve the security posture with the organization's evolution. Let's assume an organization wants to upgrade the e-commerce module of its website for its corporate customers. The new module will require a risk assessment, penetration testing, and vulnerability assessment before integrating with the website. The security engineer will ensure that all these requirements are fulfilled and that the integration will not introduce security vulnerabilities. Furthermore, it will also be ensured that the new module follows all the security policies and guidelines laid out by the organization.

Vulnerability Management

The threat landscape is continuously evolving. New software versions are released, and vulnerabilities are found in the older versions. The security engineer's job often includes monitoring vulnerabilities across the organization and planning to patch or minimize their risk. Vulnerabilities are generally patched according to severity, as we will learn in the Vulnerability Management room.

Compliance and Audits
A significant part of a security engineer's duties includes ensuring compliance with regulatory and organizational requirements. Depending on the industry, clientele, and location of the organization, it might be subject to various compliance standards such as PCI-DSS, HIPAA, SOC2, ISO27001, NIST-800-53, and more. A security engineer works closely with both internal and external auditors to detect any non-compliance issues and effectively address them. Additionally, they are responsible for upholding the organization's security certifications as needed.

****

Answer the questions below:

What is considered the weakest link in an organization's security?
Answer: Humans

An organization's security evolves with the organization. What helps a security engineer keep the organization secure through these changes?
Answer: Change management

Additional Roles and Responsibilities

As discussed previously, the security engineer's role is often loosely defined and broad-based. In certain organizations, a security engineer might need to take up some additional responsibilities to help other teams, which we will cover in this task.

Managing Security Tooling
A security engineer might sometimes be required to configure or fine-tune security tools such as SIEMs, Firewalls, WAFs, EDRs, and more. In some organizations, that might also be the primary responsibility of a security engineer. In such a role, a security engineer might also be making decisions or providing input to decision-makers about tools to procure based on the organization's requirements and the engineer's assessments of competitive tools.

Tabletop Exercises
Tabletop exercises are often conducted to gauge the operational readiness of an organization from a security point of view. Certain scenarios are identified to be exercised, and security team members must explain their respective roles in the scenarios under discussion. For example, a scenario might include the compromise of an endpoint device through a phishing email. All the team members will then explain

their respective steps per the organization's playbooks. The security engineer is sometimes required to conduct these exercises.

Disaster Recovery and Crisis Management
A robust security posture requires organizations to plan for untoward incidents, disasters, or crises. In any such scenario, the top priority of the executive management is to maintain business continuity. A security engineer might be involved in disaster recovery, business continuity, and crisis management planning as part of the different compliance frameworks and the organization's internal policies. The role of a security engineer in these areas might differ depending on the organization.

****

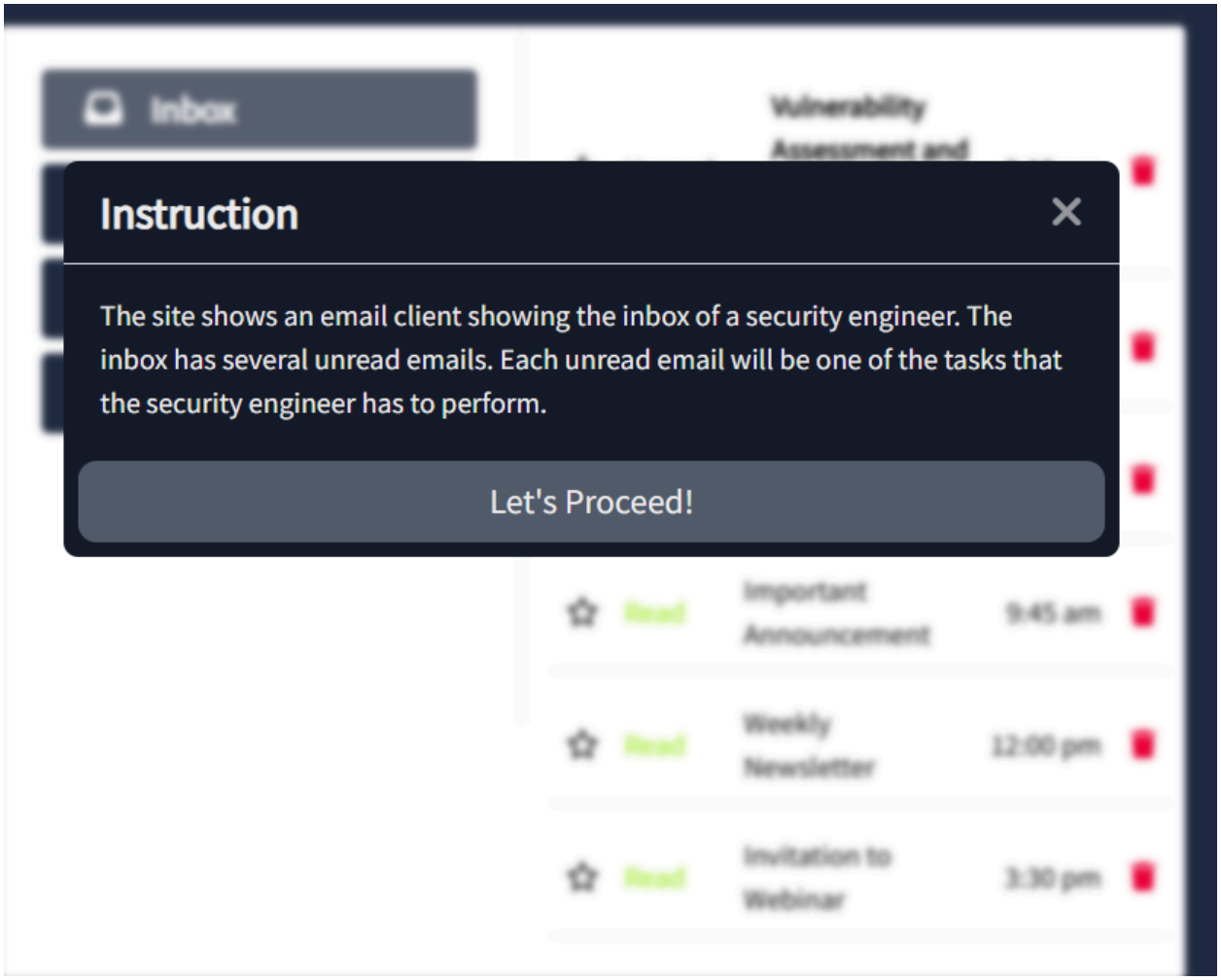
Answer the questions below:

What is a theoretical exercise carried out to gauge the operational readiness of an organization from a security point of view?
Answer: Tabletop exercise

What is the priority of the management in case of a disaster or crisis?
Answer: Business Continuity

Walking in Their Shoes

While performing their duties, security engineers must consider various aspects of running a business apart from keeping it secure. These considerations may include business operations, cost, ease of implementation, ease of use, and more. Although the most secure system is the one that is shut off and disconnected from power, such a system doesn't achieve any business objectives. Hence, a security engineer must consider business objectives and security when making decisions.
To experience what decisions a security engineer might take while performing their duties, hop on to the static site. You can do this by clicking the View Site button below



****

Answer the questions below:

What is the flag shown on the completion of the static site?
Answer: THM{S3CUR1TY_3NG1N33R5_R0CK}

Conclusion

That was a brief introduction to the day-to-day activities of a security engineer. To conclude, we learned that a security engineer:

- Owns the responsibility of an organization's cyber security.
- Ensures that the systems and infrastructure of an organization are built securely.
- Helps maintain this security posture through continuous improvement and changes in the organization's digital assets.

- Takes on additional roles and responsibilities to help other teams achieve the collective goal of a secure organization.