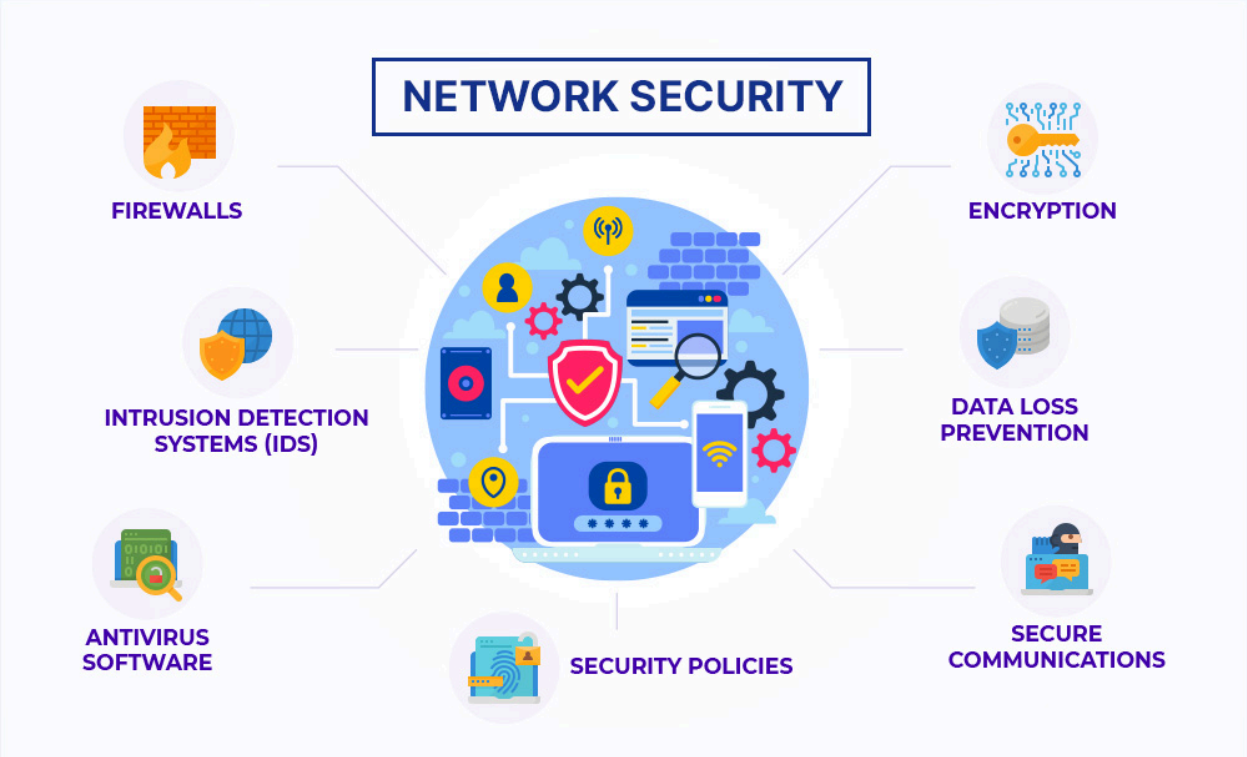
K. Wickenson MOISE

Cybersecurity Analysis

Project: Explore How Security Analysts Protect Networks And Information.



Project in the Serie Foundations Cybersecurity by Google

Here's what I'll cover:

I. Explore the Analyst role and responsibilities.

II. Connect the responsibilities to security.

III. Synthesize the analyst's proactive role.

🔭 Project Spotlight: Exploring the Security Analyst Role in Organizational Defense

The Challenge: Imagine starting as an entry-level security analyst. What initial day-to-day tasks and responsibilities do you envision taking on to help protect the organization's networks and information?

Executive Overview: In this project, I act as the "first responder" for the digital perimeter. I explore the transition from **Reactive Alert** handling to a **Proactive Security Posture**, focusing on Monitoring, Triage, and Mitigation to ensure operational continuity. By viewing security through the lens of a long-term strategist, I aim to move an organization from a **"hope-based"** security model to one that makes attacks too difficult and expensive for adversaries to attempt.

I. Explore the Analyst Roles & Responsibilities

Imagine you've just started as an **Entry-Level Security Analyst**. What initial **day-to-day tasks** and responsibilities do you envision taking on to help protect the organization's networks and information?

As an **Entry-Level Security Analyst**, my primary mission is to act as the "first responder" for the organization's digital perimeter to help protect the organization's networks and information. My initial day-to-day tasks and responsibilities focus on **Monitoring and Triage** to get any Alert Handling to review logs from firewalls, antivirus, and Intrusion Detection Systems (IDS) **and mitigation** of potential threats to ensure operational continuity.

Envisioned Day-to-Day Tasks:

1. **Vulnerability Management Security**
   The primary objective of a Security Analyst isn't just to "catch" hackers; it is to **reduce The attack surface** and **minimize the "dwell time"** (the time an attacker spends in a network before being caught) and also fixing the "holes" they use to get in.

   - **Security Monitoring & Triage (Detection and Early Warning):** No defense is 100% impenetrable. Monitoring is my "**early warning system**". Utilizing SIEM (Security Information and Event Management) tools to monitor real-time alerts and logs across the network. By watching logs and alerts, I'm looking for the first signs of a "breach attempt.
     The Proactive Result: Early detection allows to stop an attack in the "**reconnaissance**" phase. If I catch someone by scanning the network (thanks to my IDS or Firewall logs), I can block them before they ever find a way to steal data.

- **Vulnerability Assessment (Scanning):** This is the most proactive step in my toolkit. Performing regular scans using tools like Nmap to identify open ports or unpatched services that could serve as entry points for attackers and running automated tools for weaknesses (unpatched software, weak passwords, or weak configurations) across the network before an attacker finds them..

- **Incident Response Support:** Assisting in the initial phases of incident response, such as isolating compromised devices or analyzing suspicious packet captures using protocol analyzers.
- **Reporting:** I'll help categorize these risks (High, Medium, Low) and work with the IT team to ensure critical patches are applied.
- **User Education:** Providing guidance to staff on security best practices, such as identifying and reporting phishing attempts.

2. **Phishing Investigation**
   Email is the most common entry point for attackers. I will likely be the person reviewing the "Report Phishing" inbox.
   - **Header Analysis:** I'll inspect email headers to see where a message actually originated.
   - **URL/File Sandboxing:** I'll use secure, isolated environments to test suspicious links or attachments to see if they download malware or steal credentials.

3. **Incident Response Support**
   While Senior Analysts usually lead major investigations, I will play a vital supporting role.
   - **Evidence Collection:** I'll gather the "**who, what, and where**" of an event collecting timestamps, IP addresses, and affected machine names.
   - **Containment:** Under guidance, I might perform basic containment tasks, such as disabling a compromised user account or isolating a workstation from the network.

This table below simplifies and demonstrates day-to-day the Frequency and Objective of every Task.

Task	Frequency	Proactive Objective
Log Review	Constant	Identify anomalies *before* they become breaches.
Threat Intelligence	Daily	Stay updated on new malware and hacking trends. Anticipate trends to make defense 'too expensive' for hackers.
Vulnerability Scanning	Daily/Constant	Identify unpatched services and reduce the "attack surface". Find 'holes' using Nmap before attackers do.
Documentation	Per Incident	Detailed note-taking for audit trails and compliance.
Security Awareness	Periodic	Helping educate employees on safe digital habits.

Analyst Mindset

The most valuable thing I could do in my first six months and more is **documentation**. If I find a fix for a recurring false positive, write it down. Creating "Runbooks" (step-by-step guides) not only helps the team but also for the same future problem-solving.

4. **Threat Intelligence: Anticipating the Move**
   By staying updated on the latest hacking trends and suspicious IPs (Where I can discuss in a investigation workflow), I will not just waiting for an alert I am looking for specific **"Indicators Of Compromise" (IOCs)** that are currently trending in the Industry/organization.

The Big Picture: Defense in Depth

Collectively, these tasks ensure that even if one layer fails, another is there to catch the threat.

- **Vulnerability Management** makes it hard to get in.
- **Firewalls/IDS** catch those who try to get in.
- **Antivirus/EDR** stops those who actually manage to get in.
- **I as an Analyst** connect the dots to ensure the same trick doesn't work twice.

By performing these day-to-day tasks, I am transitioning the organization from a "**hope we don't get hacked**" strategy to a "**we are actively making it too expensive and difficult for them to try**" strategy.

Analyst Mindset:
Every time I have to close a ticket, ask myself: *"What could I have scanned before or from one to six months ago that would have prevented this ticket from ever existing?"*

II. Connect the Responsibilities to Security: (Connecting Responsibilities to the "Security Pillar")

Every daily task serves a specific purpose within the **CIA Triad (Confidentiality, Integrity, and Availability)**, which I have consistently prioritized throughout my 10+ years of IT experience.

- **Protecting Confidentiality:** By managing access controls and ensuring only authorized users can access sensitive databases (using SQL and specialized DBMS tools), I prevent unauthorized data exfiltration.

- **Ensuring Integrity:** Through system maintenance and software deployment, I ensure that data remains accurate and has not been altered by malicious actors.

- **Guaranteeing Availability:** By proactively troubleshooting network connectivity **(LAN/WAN)** and hardware failures, I minimize downtime and ensure that critical resources are available when the organization needs them.

III. Synthesize the analyst's proactive role: (The Proactive Role: Moving Beyond Reactive Defense)

A modern Security Analyst does not just wait for an alarm to go off; they are **proactive**. This mindset is what I aim to bring to the organization.

Synthesis of the Proactive Analyst: The proactive Analyst continuously works to **reduce the attack surface**. Instead of simply fixing a server after it crashes, I focus on **Risk Mitigation** and **Threat Detection**.

This involves:

- **Continuous Learning:** Staying current with **Emerging Cybersecurity Technologies** to anticipate how attackers might evolve their tactics.

- **Hardening Systems:** Applying the **NIST Cybersecurity Framework** to standardize security protocols and ensure the organization is adhering to global security benchmarks.

- **Strategic Optimization:** Using my background in system administration and networking to "**Security-Harden**" existing IT infrastructure before vulnerabilities can be exploited.

Technical Toolbox Highlighted in this Project

Category	Tools & Frameworks
Monitoring	SIEM, IDS, Firewalls, Packet Sniffers
Scanning	Nmap, Vulnerability Scanners
Data/Systems	SQL, Linux, Windows Server, NIST Framework

💡 KEY TAKEAWAY: Competencies Demonstrated

- **Vulnerability Management:** Reducing the attack surface and minimizing **"dwell time"** (the time an attacker spends in a network before being caught) by proactively fixing security "holes."

- **Proactive Detection:** Utilizing **SIEM (Security Information and Event Management) tools and IDS logs** to stop attacks during the **"reconnaissance"** phase.

- **Network Hardening:** Performing regular scans with **Nmap** to identify open ports or unpatched services before an attacker exploits them.

- **The CIA Triad in Practice:** Connecting infrastructure maintenance directly to the core security pillars **Confidentiality** (access control), **Integrity** (data accuracy), and **Availability** (uptime/troubleshooting).

- **NIST Framework Alignment:** Applying the **NIST Cybersecurity Framework** to standardize security protocols and ensure adherence to global security benchmarks.