Junior Security Analyst Intro

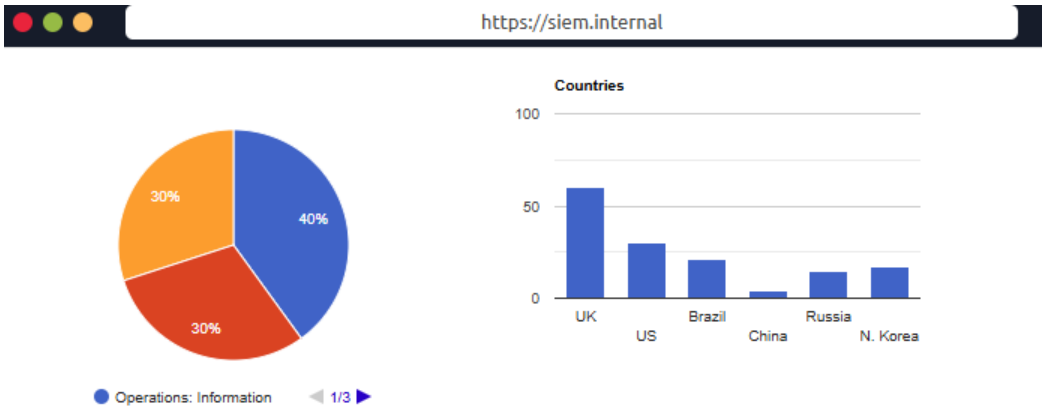
Adrian Cortez

Junior security analysts are responsible for monitoring an organization's security systems and tools to detect potential threats or suspicious activity. They review alerts generated by security information and event management (SIEM) systems, investigate low to moderate severity incidents, and escalate more serious threats to senior analysts.

They often assist with analyzing logs from firewalls, intrusion detection systems, and endpoint protection tools. A key part of their day is documenting incidents, writing reports, and following playbooks to ensure consistent response actions.

Junior analysts also help with maintaining threat intelligence feeds, updating blacklists, and reviewing vulnerability scans. They may contribute to improving detection rules or tuning systems to reduce false positives, while continuously learning about new attack techniques and cybersecurity tools.

In our first exercise, we will use a security monitoring tool, similar to one that SOC analysts use.



Alert Log

Date	Message
April 16th 2024, 05:27:00:347	Successful SSH authentication attempt to port 22 from IP address 221.181.185.159
April 16th 2024, 05:25:28:235	Unauthorized connection attempt detected from IP address 221.181.185.159 to port 22
April 16th 2024, 02:43:22:456	The user John Doe logged in successfully (Event ID 4624)
April 16th 2024, 02:43:20:658	Multiple failed login attempts from John Doe
April 16th 2024, 02:30:20:215	Logon Failure: Specified Account's Password Has Expired (Event ID 535)

Here, we can tell there is a suspicious login from the IP 221.181.185.159

There are several open-source databases such as AbuseIPDB and Cisco Talos Intelligence that allow you to check the reputation and geographic location of IP addresses. Security analysts commonly rely on these resources to help investigate alerts. Additionally, you can contribute to online safety by reporting malicious IP addresses on platforms like AbuseIPDB.

This is a minor incident, so we can escalate to the SOC Team Lead. After receiving permission to block the IP Address, we can block it on our firewall.