1H23 Cycle

Name:	John Doe
Position:	Senior Information Security Analyst
Team:	SOC/CSIRT

Major Initiatives

SIEM Deployment

I led this project and my responsibilities were:

- This
- This
- That

At the end of the semester, the project is doing well and I'm confident we'll deliver in time. As the leader of the project, I made sure every stakeholder is informed.

Incident Management Improvements

I assessed the IR process and identified many gaps for improvement:

- Gap 1
- Gap 2
- Gap N

Within this project, I tackled all gaps and after this, the Time to Respond dropped by 30 minutes and the friction with other teams greatly reduced (feedback from team members).

Participation in Incidents

- **Leaked Credentials:** I led this incident aggregating information and technically instructing the team. We were able to revoke the credentials 20 minutes after the ticket was open and all tasks were closed in 2 days with no business impact. [LINK]

Collaboration and Mentorship

- Presented the SIEM Project in English to explain the fundamentals. [LINK]
- Partnered with John Smith to make sure the log sources in SIEM were aligned with the Infosec strategy. [LINK]
- Onboarded more people in the project, showing the status and what was done.

Outside of Work

- Blog post: A simple study of mail security features inspired by a discussion in a war room. [LINK]
- Blog post: Some insights I had after implementing the network and port scan detection rules in SIEM. [LINK]

2H23 Cycle

Name:	John Doe
Position:	Senior Information Security Analyst
Team:	SOC/Threat Detection

Major Initiatives

Chronicle SIEM Deployment

I broke the project into two branches to help us organize our tasks: Log Ingestion and Rule Migration.

Log Ingestion

I listed all log sources and synced with the Engineering team to prioritize them in the selected order. Regularly we synced to diminish doubts and at the end, all log sources were successfully ingested in SIEM.

Rule Migration

I was responsible for migrating the detection rules and sorted them according to the log ingestion order. In four months, I migrated all the rules, updated the playbooks, and spread the knowledge. [LINK]

The highlights for this task are:

- Rule X: Could not be migrated due to this.
- Rule Y: Caused a 500 USD reduction per month because of this.
- Rule Z: Was deprecated because of that.

At the end, we reached our objectives and the measured cost reduction is 30%.

MITRE Automation

Wrote a script to automate the detection rule mapping [...]. This script greatly reduced the time needed to create such mappings (>99% reduction), allowing the analysts to work on the analysis and not on the mapping itself. Ultimately, it allowed the team to issue more coverability reports during the cycle with less effort.

Participation in Incidents

- **Malware X War Room:** Participated in the war room to handle the malware X. This malware was detected by a new rule written by me and I provided insights on how to handle this incident. This detection made in the early stage avoided any financial loss. [LINK]

Collaboration and Mentorship

- I presented the new SIEM to the whole team and showed how to create rules, and manage some features, like Reference Lists. Sharing this knowledge is important to avoid bottlenecks in SIEM and give more autonomy to authorized people.
- Mentored Jane Doe, a Junior Infosec Analyst. She started her career and during our mentorship sessions, I helped her understand all areas in Infosec and find the one she likes the best. At this point, she decided to work in Appsec as a result of our conversations.

Outside of Work

- Attended "Threat Hunting DLL-injected C2 Beacons using Memory Forensics". I watched this presentation from Active Countermeasures to learn a bit more about detecting suspicious activities in Windows, as I was migrating the Windows rules from Splunk to SIEM at the time.
- Studies on MITRE ATT&CK best practices. I've watched some talks, read documentation, and attended an online course about MITRE ATT&CK to learn how to get more from this framework in Threat Detection. It was fundamental to

me to have the insight to write the script that maps MITRE ATT&CK data from Chronicle rules to MITRE Navigator.

- Read Intelligence-Driven Incident Response and wrote a blog post about it. In a conversation with a colleague on how to better integrate CTI, Threat Detection, and CSIRT, he suggested that I read this book. Here I learned the process of doing that as well as how the many concepts Intel uses work together. I decided to summarize my takeaways in a blog post to use later.