Alex *Security Operations Engineer*

My role

I'm the firefighter of the Security team. My objective is to **prevent malicious attacks** and **mitigate active risks** to my organization as they pop up, as **quickly** as possible. In order to do that, I develop detection tooling that generates **trustworthy alerts**, and take part in an **on-call** rotation where I serve as an **Incident Responder**.

*"I need to be **jack of all trades**: When SecOps get paged, it could be about anything, and there's a high probability that the incident concerns something **you've never dealt with before**. The sky could be falling and there's **a lot at stake** and so the role of a security operations person can be pretty **stressful**."*

JTBD

- **Manage incident response**

  When I am on-call, I need to respond to and manage incidents as they pop up, so as to mitigate the risk to my organization as quickly as possible.

- **Real-time documentation**

  As an incident unfolds, I want to document as much of what is happening as possible, so that later on I could use that information as part of updating or creating a runbook, and possibly creating an RCA (Root Cause Analysis).

- **Building detection tools**

  When I'm not on-call, I want to build tools that enhance our detection and alerting capabilities, so as to improve my organization's security stance.

- **Short-term project management**

  As an incident unfolds, I want to assign tasks and coordinate the work of multiple individuals across my organization, so I can move as quickly as possible to remediate the risk.

Skills & Personal Traits

- Great ability to divide my focus effectively and deal with interruptions, such as new alerts, new data, and urgent requests from colleagues
- Good at thinking quickly on my feet and maintaining my composure in stressful situations
- Can think like an attacker as well as a defender
- Enjoy building tools (has coding skills)
- Passionate about improving processes
- Effective communicator: articulate both verbally and in writing
- Enjoys the variance of SecOps work
- Feels relatively comfortable with handling unknown unknowns

Frustrations

- It is cumbersome to edit description of timeline in real-time, and it's especially difficult to do in hindsight. Often the timeline documentation isn't completed.
- Often important parts of the info I need in order to handle the incident are either not communicated fully, or are being communicated in an unstructured manner which makes aggregation and searching difficult.

Key Tools

GitLab Issues
Tracking, documentation

PagerDuty
Initiation standpoint, where pages are sent through

Slack, Zoom, GitLab Issues
Communication

Google Docs
Real-time documentation

Terminal, coding environment
Mostly Python, some Go - for building and/or running tools

The Hive
A security incident management tracking tool
• Cortext - part of The Hive, allows for easy automation

A cloud management console
To access the infrastructure

Various tools for triage and mitigation:
• **Docker** - to reproduce security issues and test approaches
• **Accounts for different environments** - to test against
• **ELK stack** - to go over logs
• **Stackdriver or BigQuery** - long-term storage, used for incidents that are open for a long period of time

Collaboration with other teams

- Infrastructure
- Legal
- Compliance, AppSec
- Support

If a particular feature or tool is involved in an incident:

- Development teams
- Various SMEs