

Navigating your SecOps career path

: ~ / \$whoami

- Senior security analyst @GDEV
- Cloud incident response, TH/TI
- Author of quite a few articles on macOS malware
- ex-Yandex, ex-Kaspersky  [kaspersky](#)
-  [/in/mogilin/](#)



Agenda

Security teams responsibilities

What does Security Operations do?

SecOps pipeline

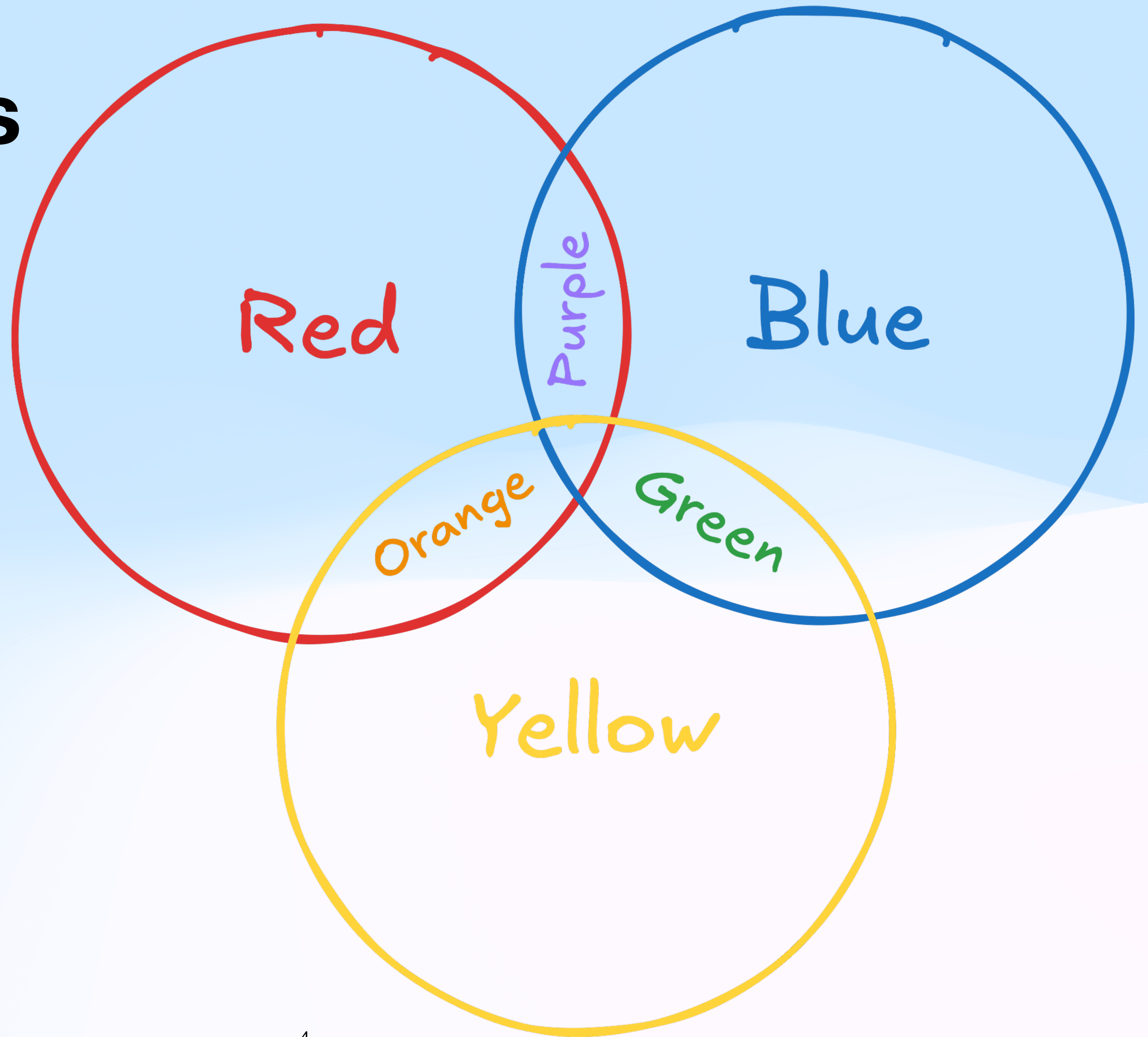
What is SIEM and detection engineering?

Responding to threats: playbooks and automations

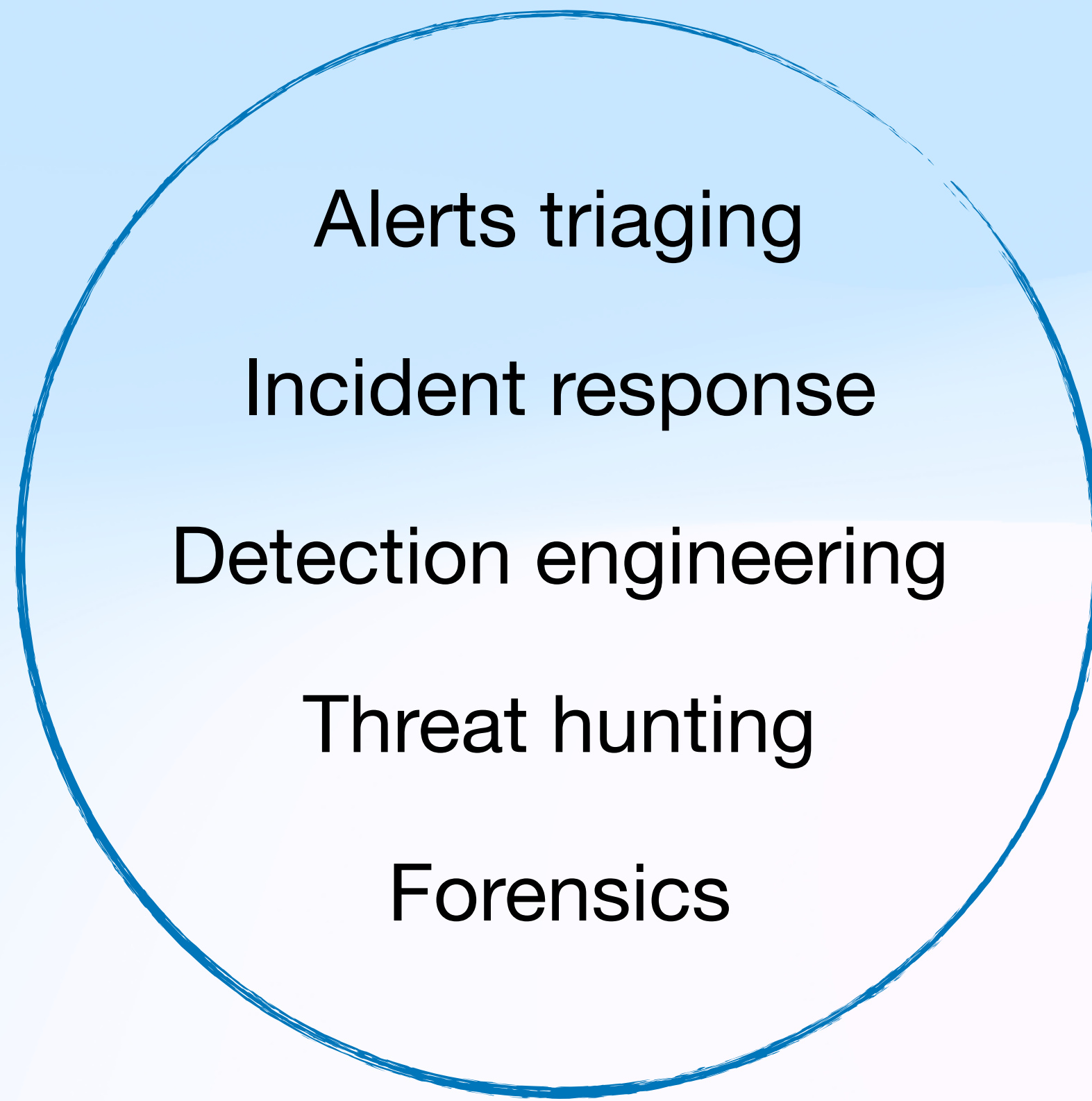
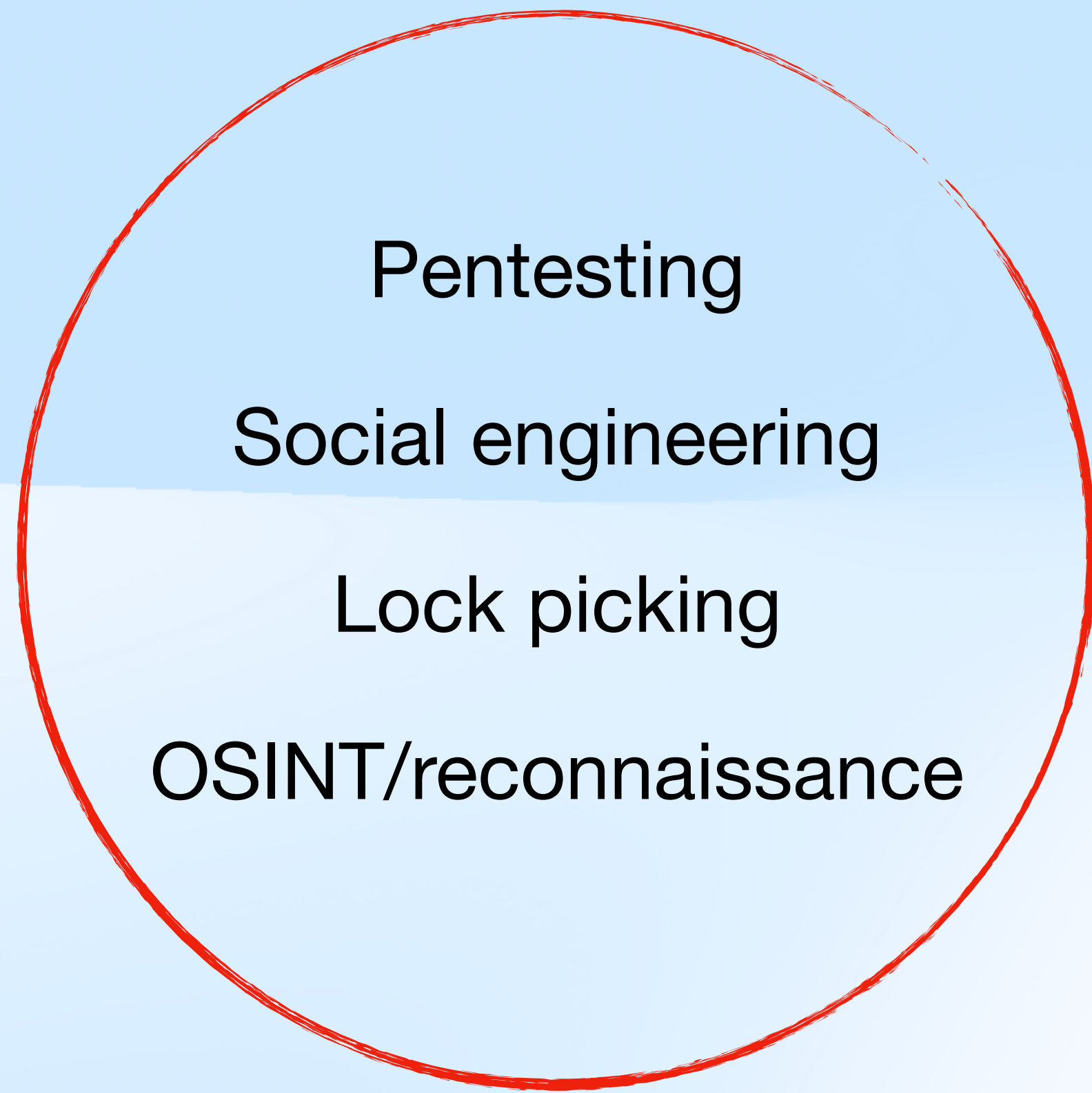
Recovery methods

Certifications to learn SecOps

Security teams



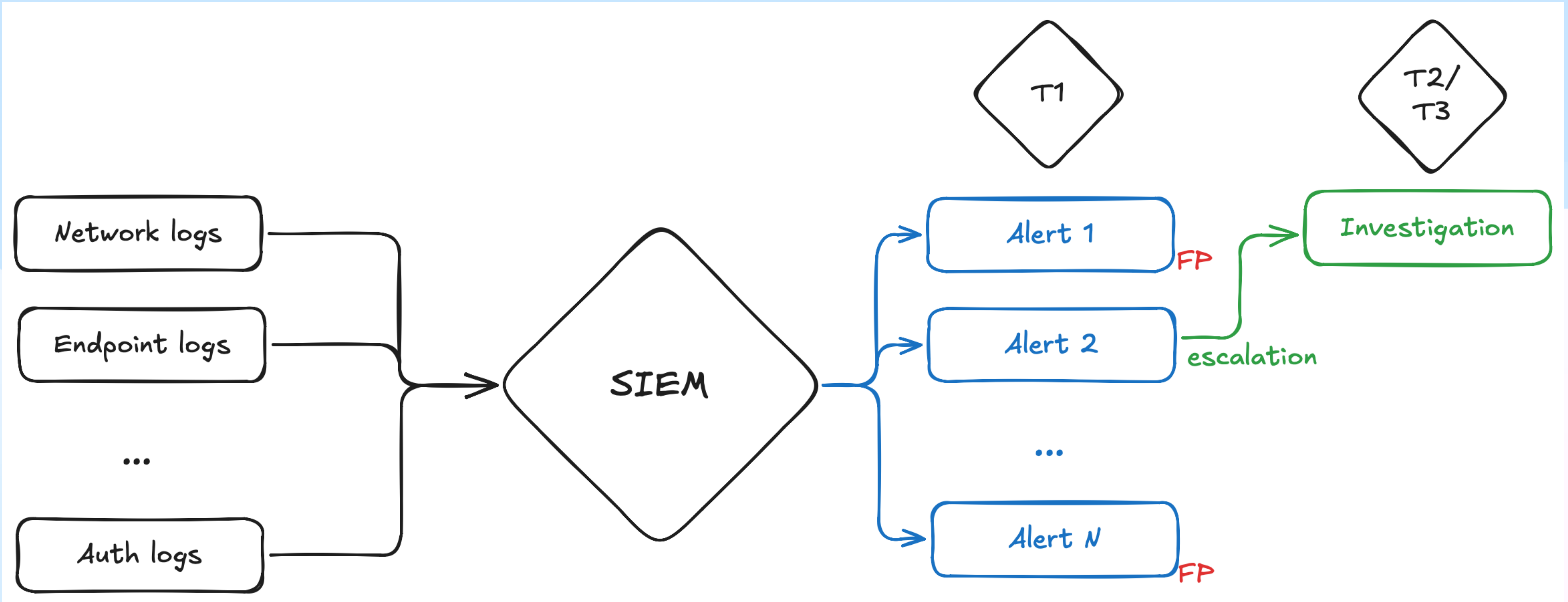
Security teams responsibilities



What does SecOps do?

Helps *detect*, *respond* and *recover* from security threats

Security Operations pipeline



Security Operations actionable steps

1. Detect

Security Information and Event Management

Search Analytics Datasets Reports Alerts Dashboards App Splunk Create App


New Search Save As Create Table View Close

1 status=503 action=purchase Last 60 minutes Q

✓ 108 events (7/28/22 1:11:00.000 PM to 7/28/22 2:11:40.000 PM) No Event Sampling Job || ■ → 🖨 ↓ Smart Mode

Events (108) Patterns Statistics Visualization

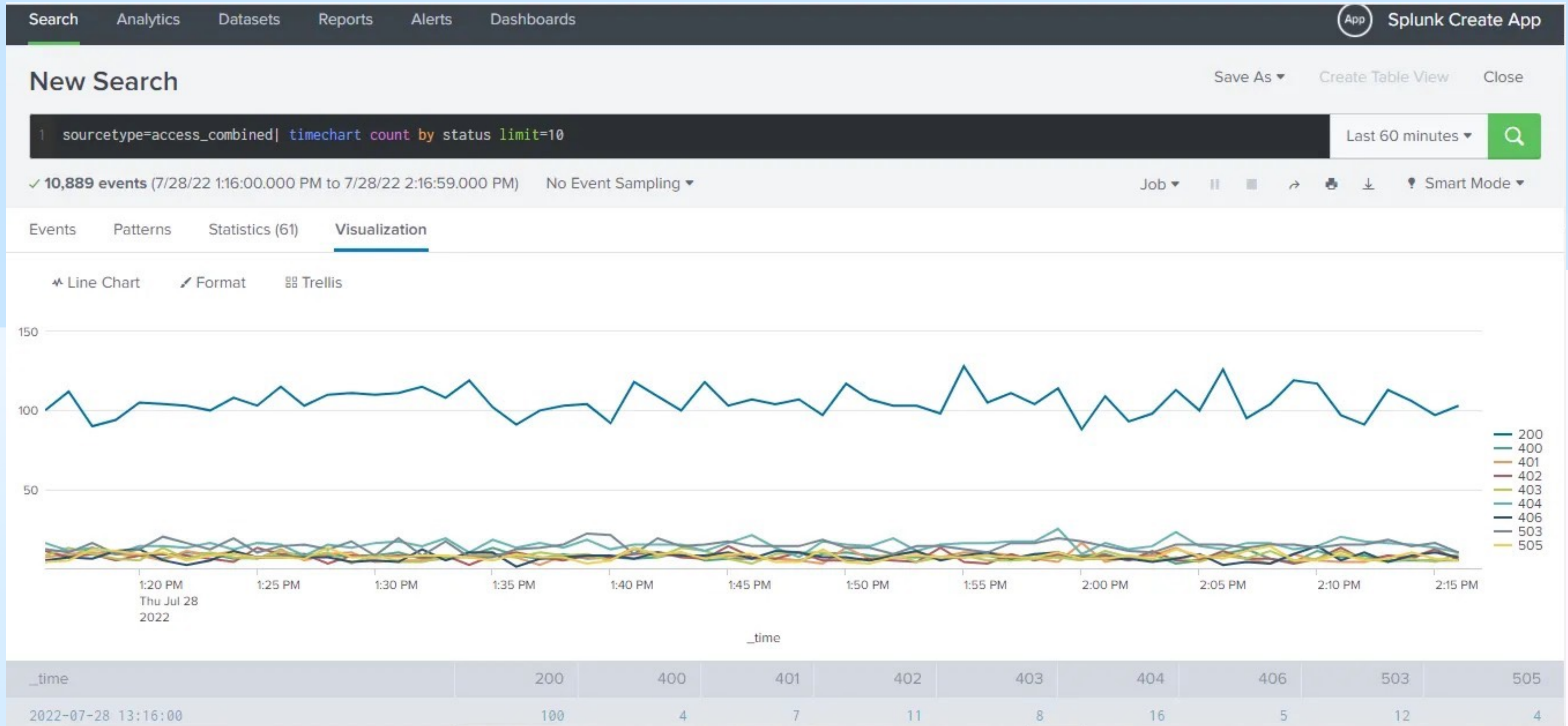
Format Timeline – Zoom Out + Zoom to Selection × Deselect 1 minute per column



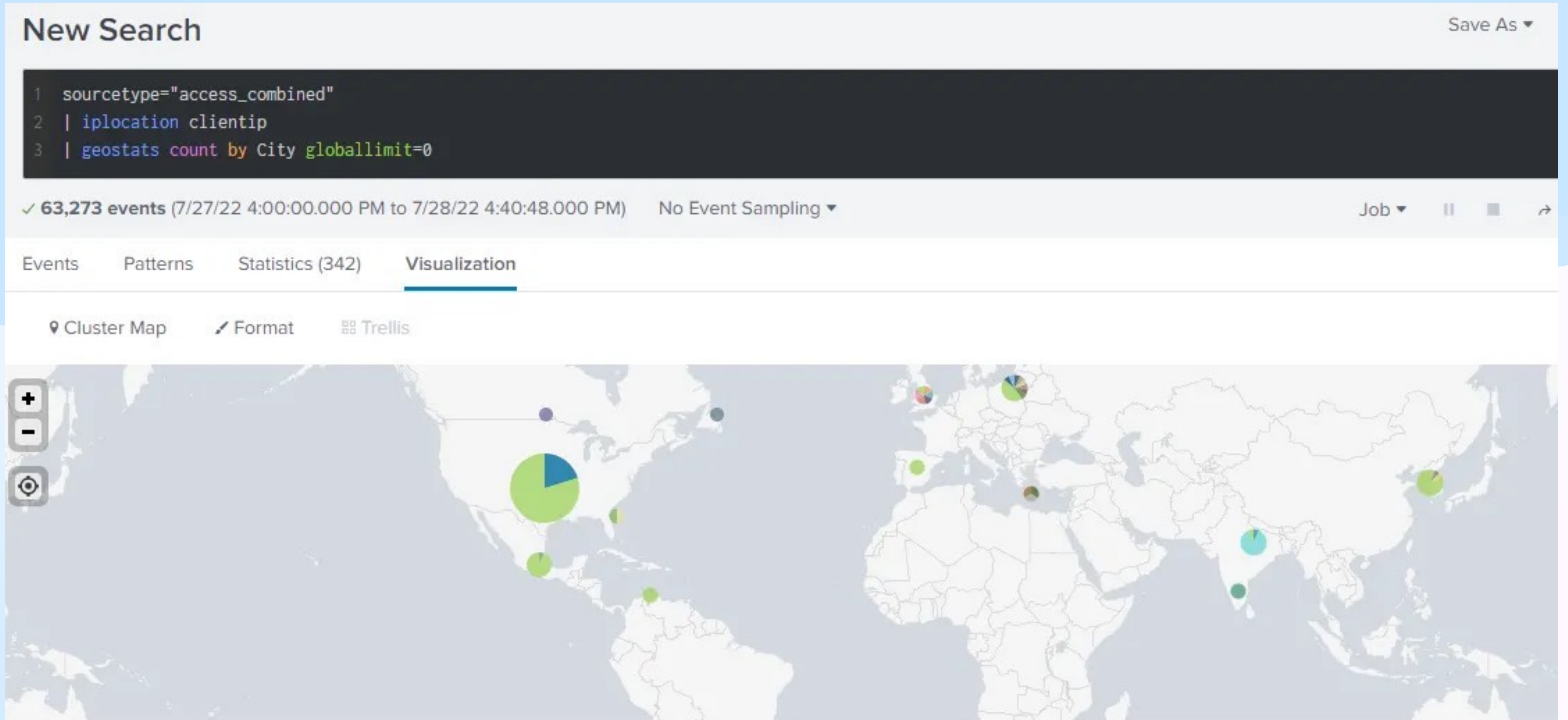
List Format 20 Per Page < Prev 1 2 3 4 5 6 Next >

< Hide Fields All Fields		i	Time	Event
SELECTED FIELDS a host 1 a source 3 a sourcetype 1		>	7/28/22 2:10:55.174 PM	1.16.0.0 - - [28/Jul/2022 18:10:55:174] "GET /cart.do?action=purchase&itemId=EST-7&product_id=CM-1&JSESSIONID=SD1SL6FF10ADFF2 HTTP 1.1" 503 3076 "http://www.buttercupenterprises.com/cart.do?action=purchase&itemId=EST-7&product_id=CM-1" "Mozilla/5.0 (Windows; WOW64) AppleWebKit/537.36 Chrome/39.0.2171.71 Safari/537.36" 907 host = ip-172-31-24-213 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined
INTERESTING FIELDS a action 1 # bytes 100+ a clientip 35 # date_hour 2 # date_mday 1		>	7/28/22 2:10:52.171 PM	194.8.74.23 - - [28/Jul/2022 18:10:52:171] "GET /cart.do?action=purchase&itemId=EST-14&product_id=BS-2&JSESSIONID=SD8SL3FF9ADF F6 HTTP 1.1" 503 1746 "http://www.buttercupenterprises.com/product.screen?product_id=BS-2" "Mozilla/5.0 (Windows; WOW64) AppleWebKit/534.27 Version/5.0.4 Safari/533.20.27" 727 host = ip-172-31-24-213 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined
		>	7/28/22 2:10:27.105 PM	131.178.233.243 - - [28/Jul/2022 18:10:27:105] "GET /cart.do?action=purchase&itemId=EST-15&product_id=ZSG-2&JSESSIONID=SD10SL1 05E3AD556 HTTP 1.1" 503 686 "http://www.buttercupenterprises.com/product.screen?product_id=ZSG-2" "Mozilla/5.0 (iPhone; CPU i

Security Information and Event Management



Security Information and Event Management



Detection rule example

```
## Torg Grabber infostealer C2 and delivery indicators (Splunk SPL)
## Author: Daniel Jeremiah
## Date: 2026-03-30

index=net (sourcetype=proxy* OR sourcetype=pan:traffic OR sourcetype=zeek:http)
| eval url=coalesce(url, uri, request, http_url)
| where match(url, "(?i)https?://(si-dodgei\.digital|j0o\.pw|t4e\.pw|re3\.pw|
technologytorg\.com|gogenbydet\.cc|bbcplay\.top|playbergs\.info|bk\.tara\.net\.bd|
raketa\.tara\.net\.bd)(/|$)")
    OR like(url, "%/api/auth%") OR like(url, "%/api/upload%") OR like(url, "%/core2%")
| stats count min(_time) as firstSeen max(_time) as lastSeen values(url) as urls by
src_ip, dest_ip, dest_port
| sort - lastSeen
```

Security Operations actionable steps

1. Detect
2. Respond

Responding to threats

Playbooks

Set of predefined
actions for
specific situation

Automations

Tools and scripts

Responding to threats: SQL-injection

```
192.168.1.15 - - [29/Apr/2026:08:12:34 +0000] "GET /products.php?id=1' HTTP/1.1" 500  
1024 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
```

```
192.168.1.15 - - [29/Apr/2026:08:12:41 +0000] "GET /products.php?id=1%27 HTTP/1.1" 500  
1024 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
```

```
192.168.1.15 - - [29/Apr/2026:08:12:48 +0000] "GET /products.php?id=1%27-- HTTP/1.1"  
200 3812 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
```

```
192.168.1.15 - - [29/Apr/2026:08:12:55 +0000] "GET /products.php?id=1+AND+1=1-- HTTP/  
1.1" 200 3812 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
```

```
192.168.1.15 - - [29/Apr/2026:08:13:02 +0000] "GET /products.php?id=1+AND+1=2-- HTTP/  
1.1" 200 512 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36"
```

..

```
192.168.1.15 - - [29/Apr/2026:08:14:55 +0000] "GET /products.php?  
id=-1+UNION+SELECT+table_name,2,3+FROM+information_schema.tables+WHERE+table_schema=da  
tabase()-- HTTP/1.1" 200 4234 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
AppleWebKit/537.36"
```

Responding to threats: SQL-injection

Playbook and action items

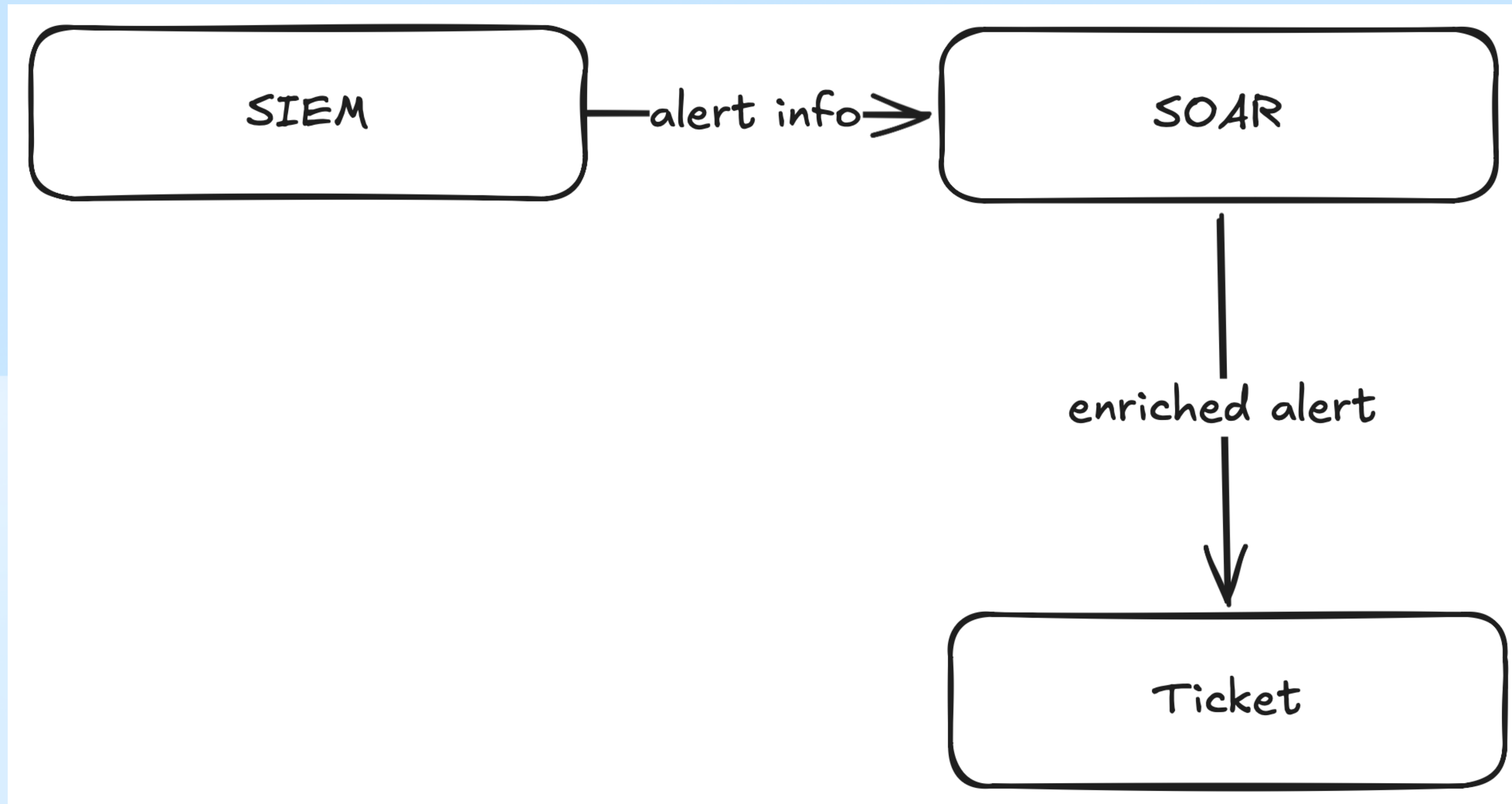
1. Check that there is successful execution (200 OK)
2. Check database logs for executions, retrieve remote IP of attacker / user
3. Ban IP / user from your system and on WAF
4. Assess impact: what info was stolen, is there any PII? Were any of the tables dropped?
5. Prioritize immediate hotfix for vulnerable parameter

Responding to threats: SQL-injection

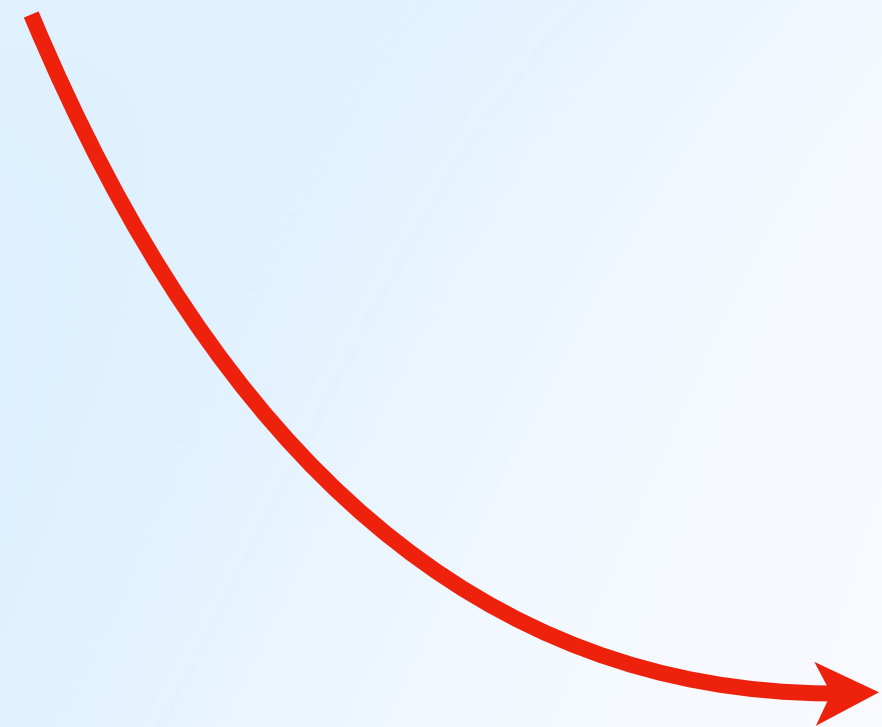
Automation

1. Script (or some CI) to ban IP on WAF
2. Breakglass mechanism to access production servers (or PAM)

Security Orchestration, Automation and Response



Automations in SOAR



Case # 2 - demo 2

Please Subscribe 07/24/21 13:35 07/24/21 13:37 as False Positive 2 minutes 1 case

Details Tasks 0 Observables 2 TTPs

No observable selected + Add observable(s) Export

Filters

+ Add a filter

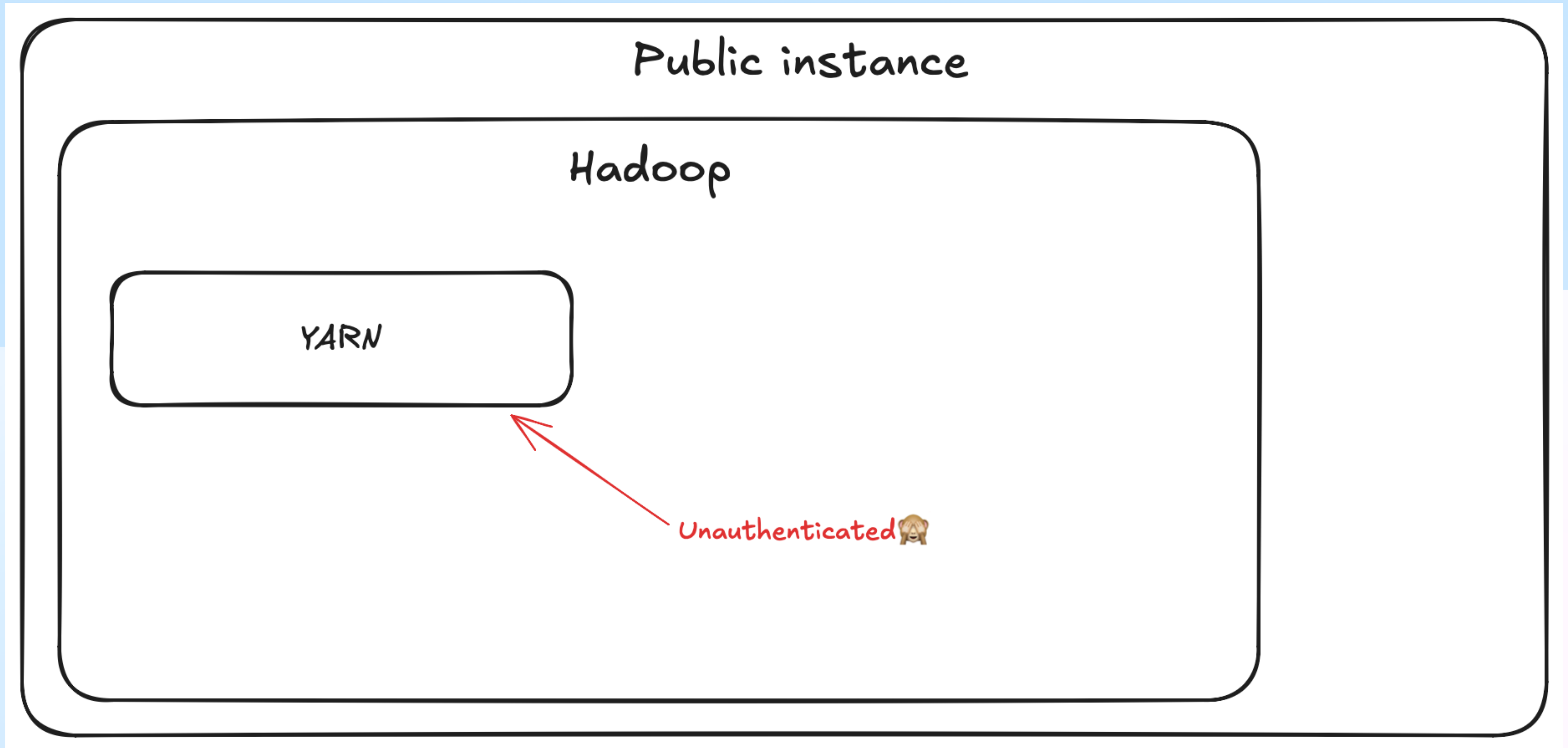
List of observables (2 of 2)

Flags	Type	Value/Filename
<input type="checkbox"/>	hash	08fabadbcbf7811709fd9da698dae9d12238d02b36287111629a0e07eaf04e9d8 test VT:GetReport="12/61"

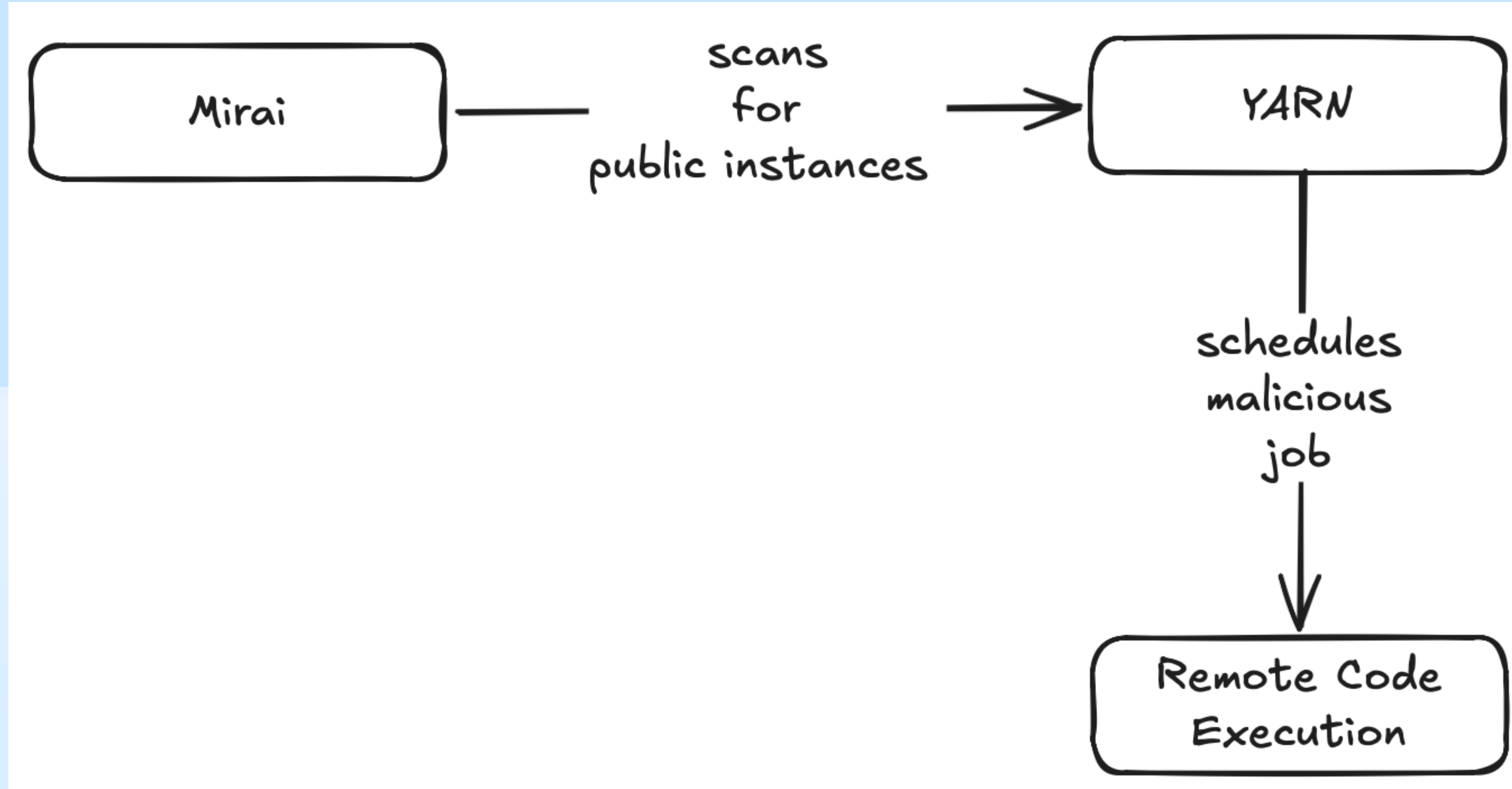
Security Operations actionable steps

1. Detect
2. Respond
3. Recover

Recovery methods: YARN case



Recovery methods: YARN case



Recovery methods (could also be automated!)

1. Forensics
2. Kill malicious pod in Kubernetes
3. Reinstall OS on your computer
4. Reissue compromised tokens
5. Restore backup of a database

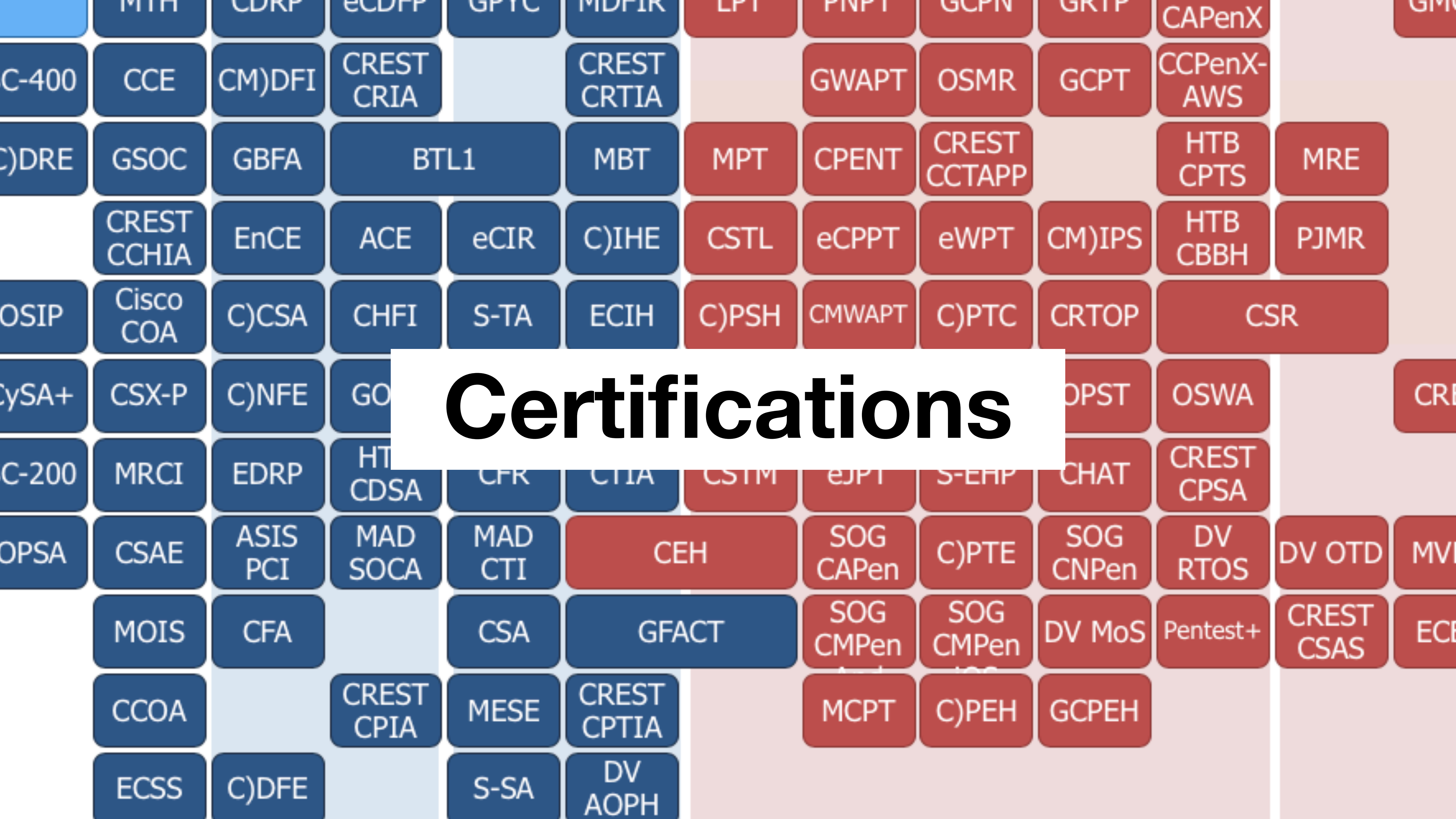
Obligatory AI slide



State of AI in SecOps

1. Using LLM to reason on alert severity
2. Alerts triaging using multi-agent system
3. Using prepared (claude-) skills to automate response / recovery
4. Writing summarized report upon incident containment

Certifications



**Why care about certs if HRs
know only about OSCP?** 🌙

Certifications

- [Security certification roadmap by Paul Jerimy](#)
- [SOC Level 1 & 2 by TryHackMe](#) **FREE!**
- [Blue Team Level 1](#) — more forensics
- OSCP / CPTS — whatever you like!
- Hack The Box labs — good!

Experience vs. certifications

Knows how to patch KDE on FreeBSD

**Triages
100K alerts per sec**



**Guesses your passwords
by hash 🗿**

**But... ehmm... I know
MITRE ATT&CK by heart**



**There were no k8s threats
in my course 😭**

Your questions!



LinkedIn



Blog