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
- /in/mogilin/

Agenda

Security teams responsibilities

What does Security Operations do?

SecOps pipeline

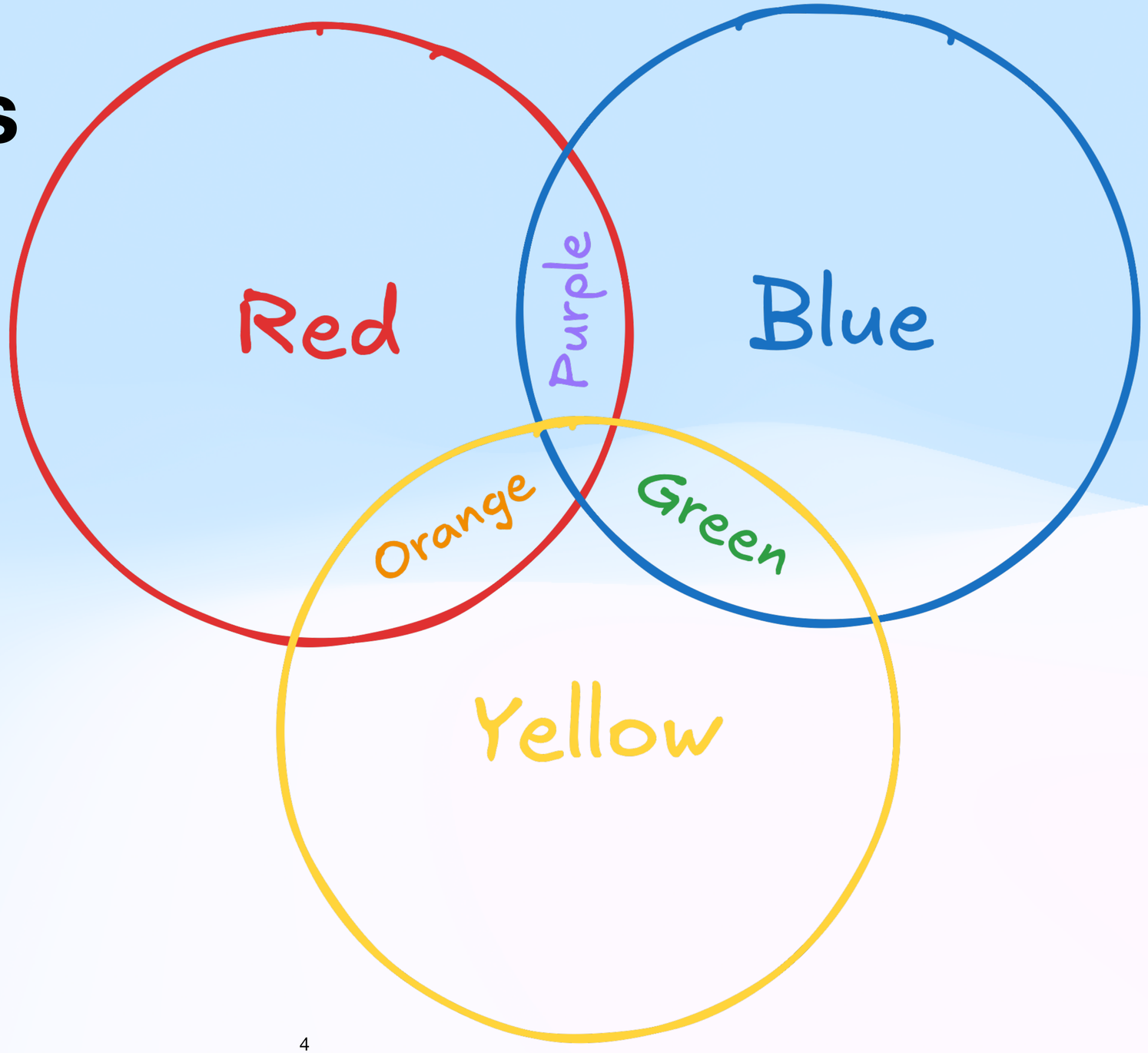
What is SIEM and detection engineering?

Responding to threats: playbooks and automations

Recovery methods

Certifications to learn SecOps

Security teams

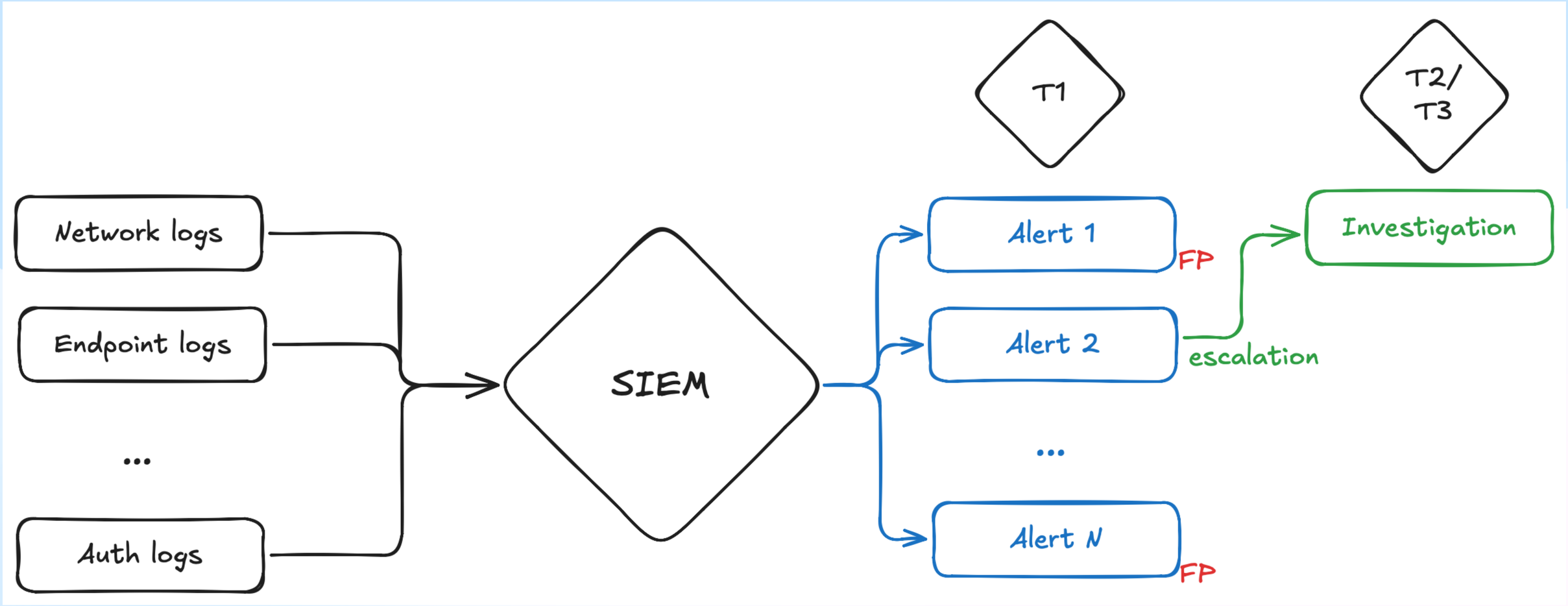


Security teams responsibilities

What does SecOps do?

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

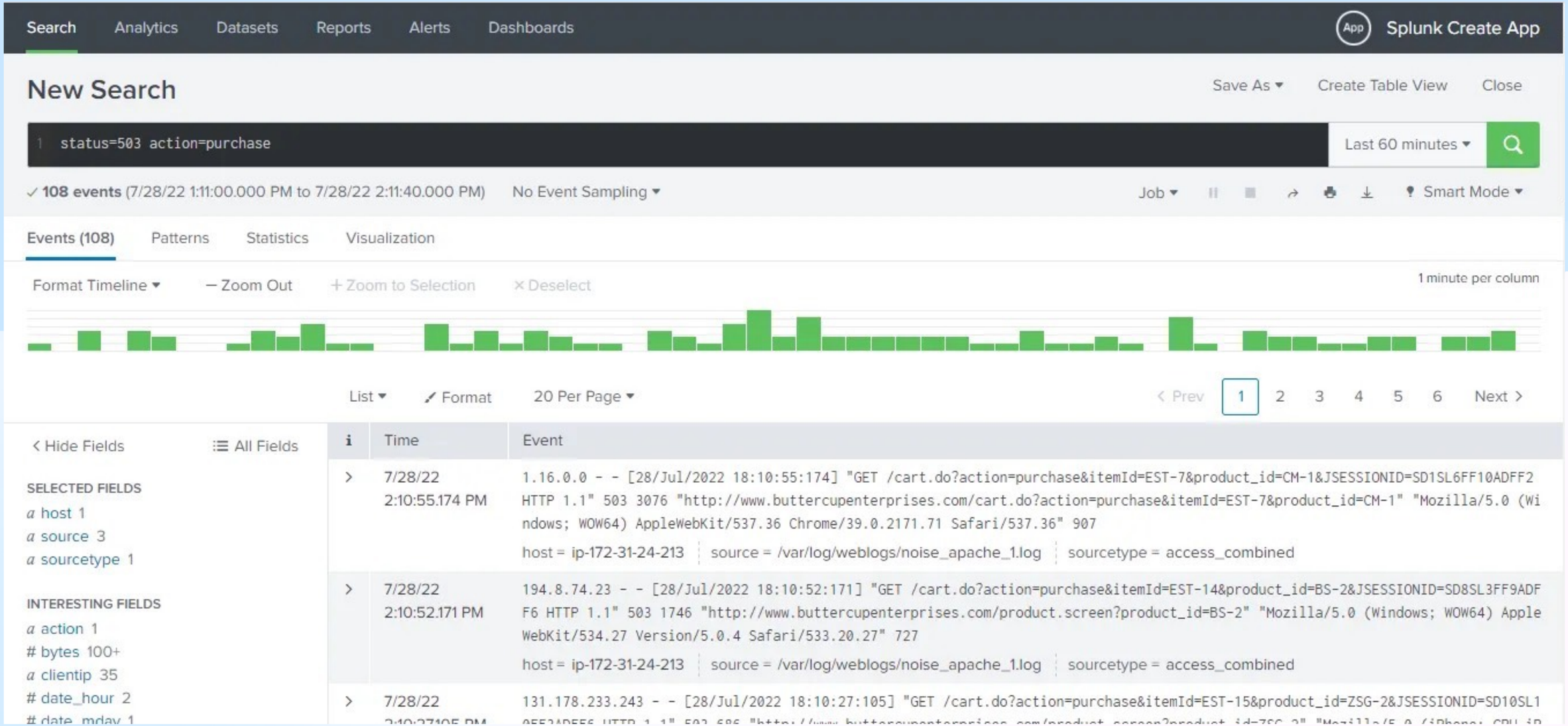
Security Operations pipeline



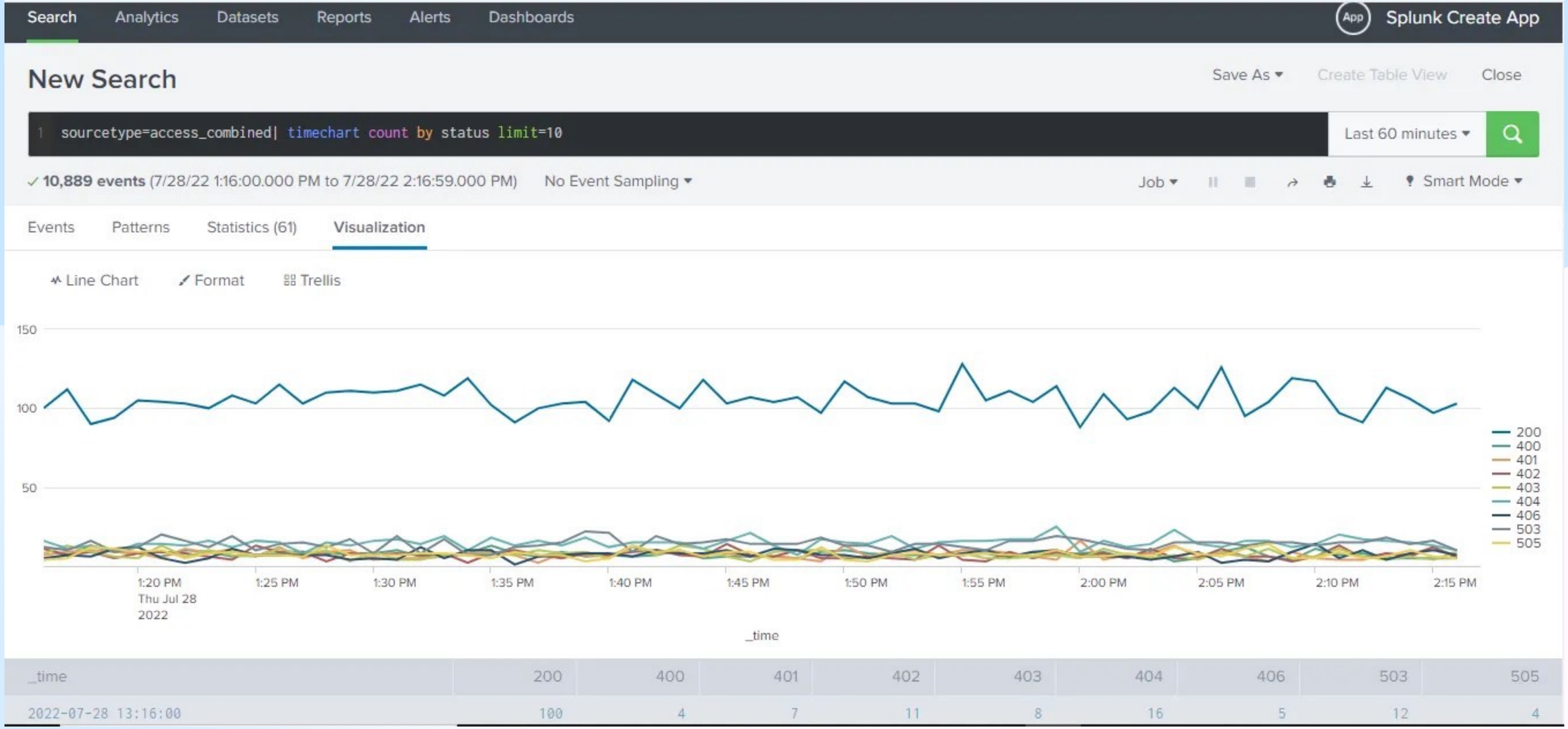
Security Operations actionable steps

1. Detect

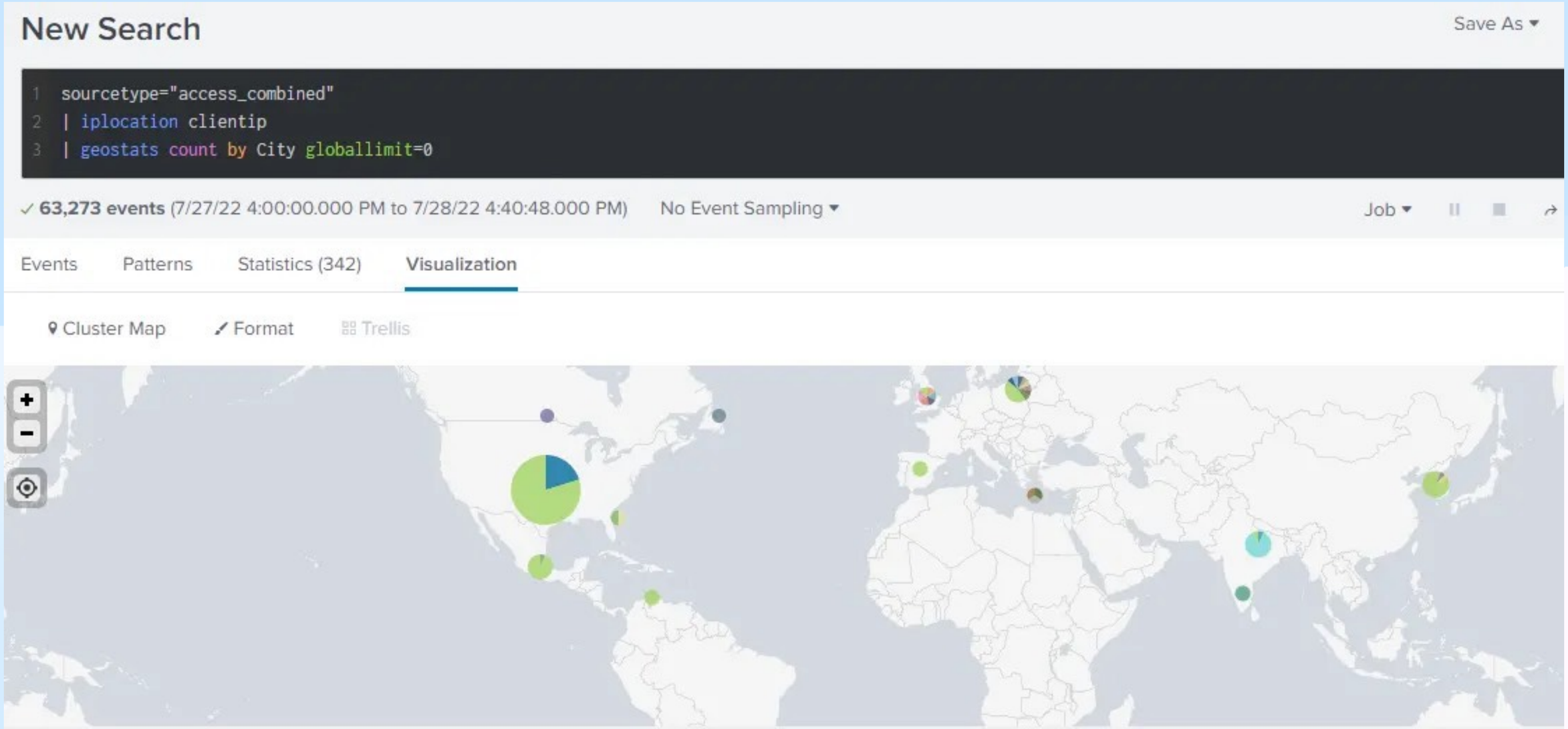
Security Information and Event Management



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

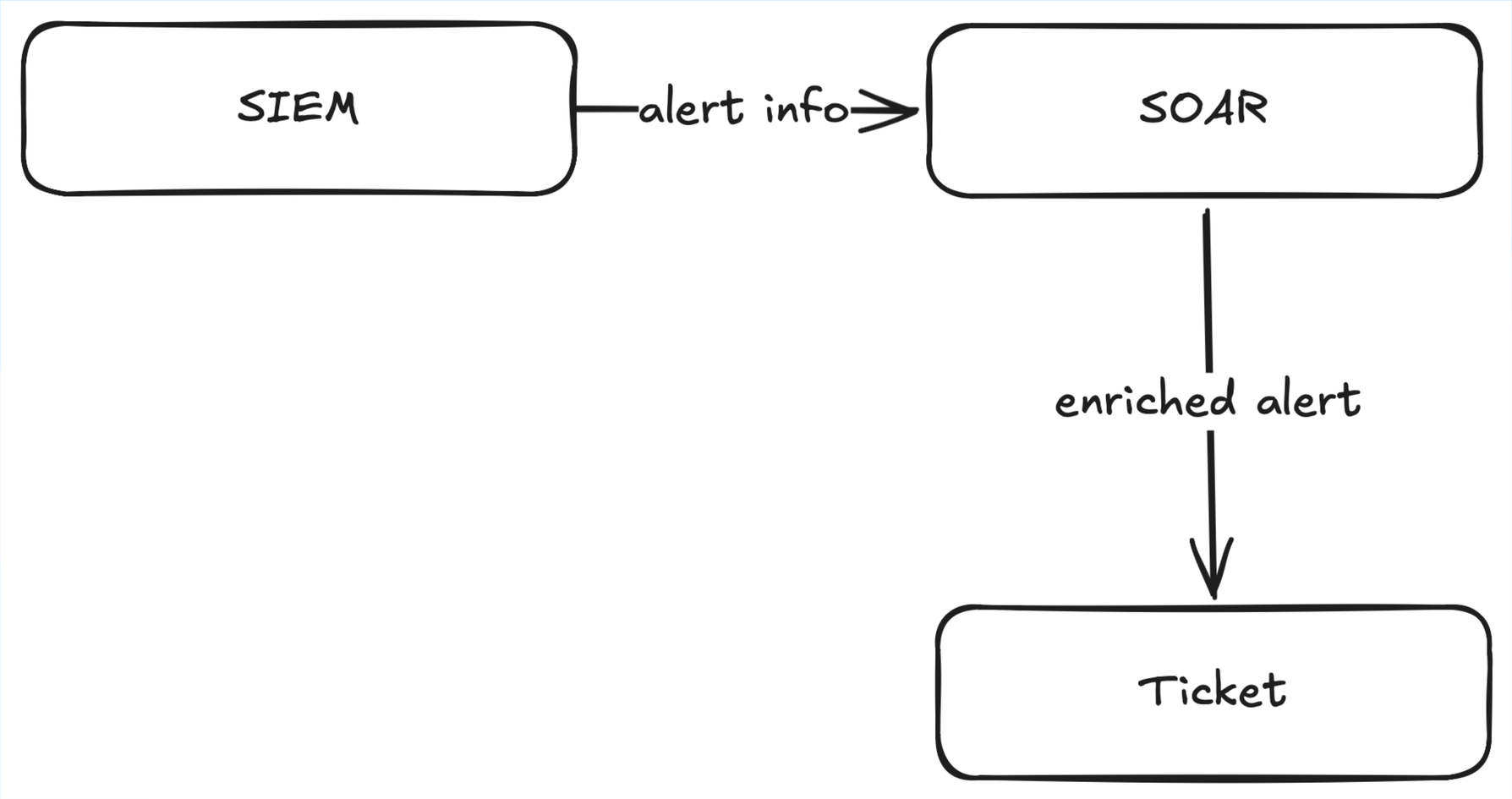
1. Check that there is successful execution (200 OK)
2. Check database logs for executions, retrieve remote IP of attacker / user
3. Ban IP / user from your system and on WAF
4. Assess impact: what info was stolen, is there any PII? Were any of the tables dropped?
5. Prioritize immediate hotfix for vulnerable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

Responding to threats: SQL-injection

Automation

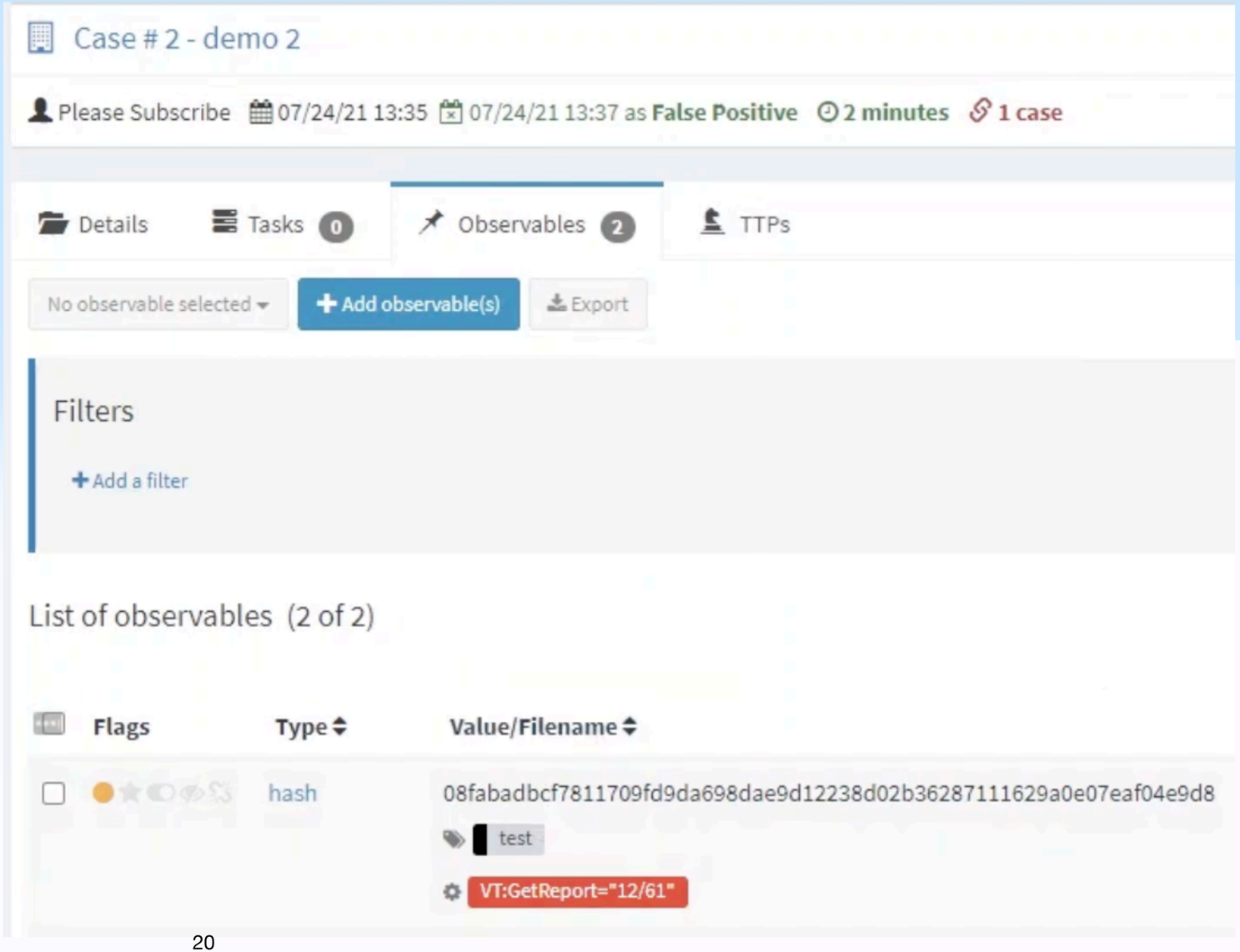
1. Script (or some CI) to ban IP on WAF
2. Breakglass mechanism to access production servers (or PAM)

Security Orchestration, Automation and Response



Automations in SOAR

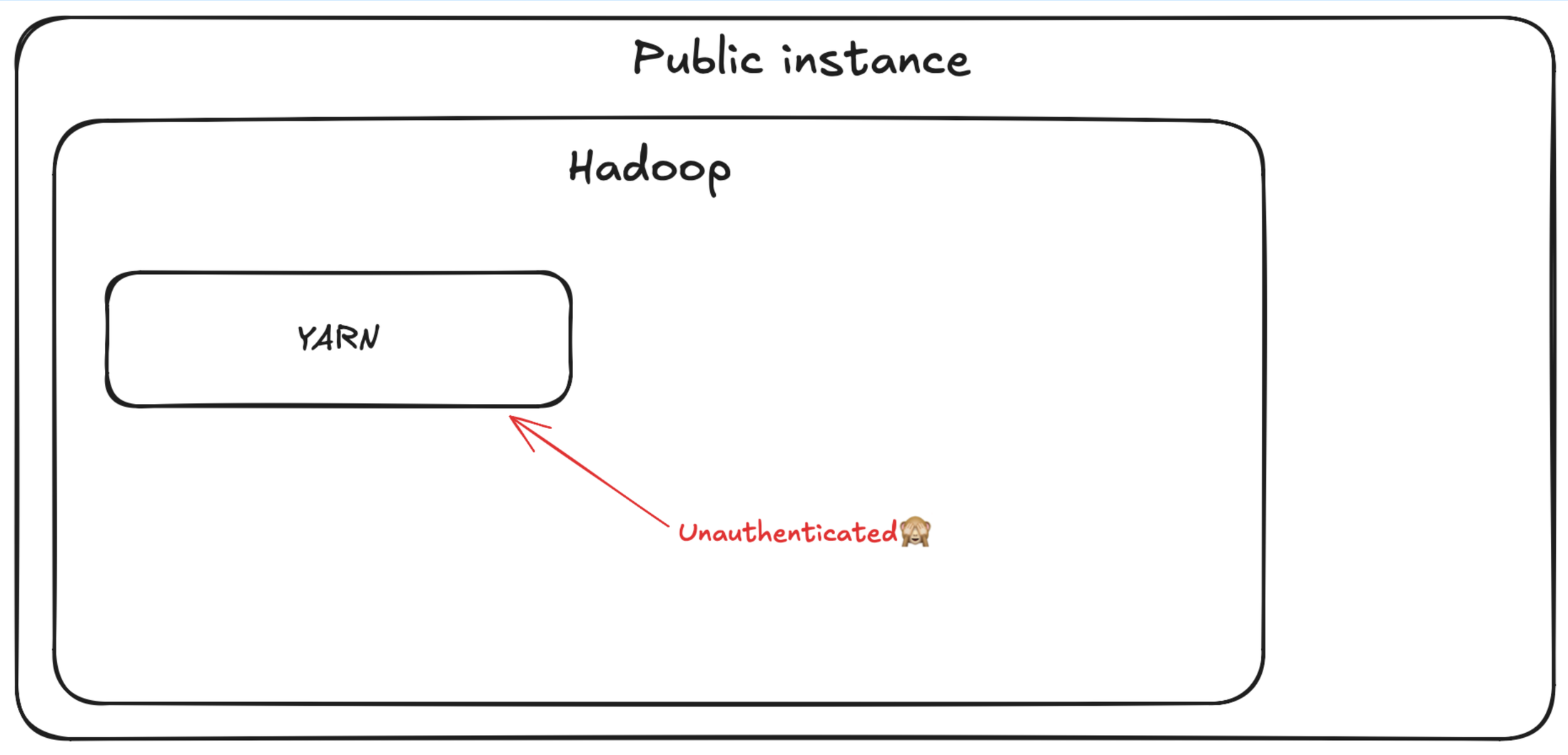
VirusTotal



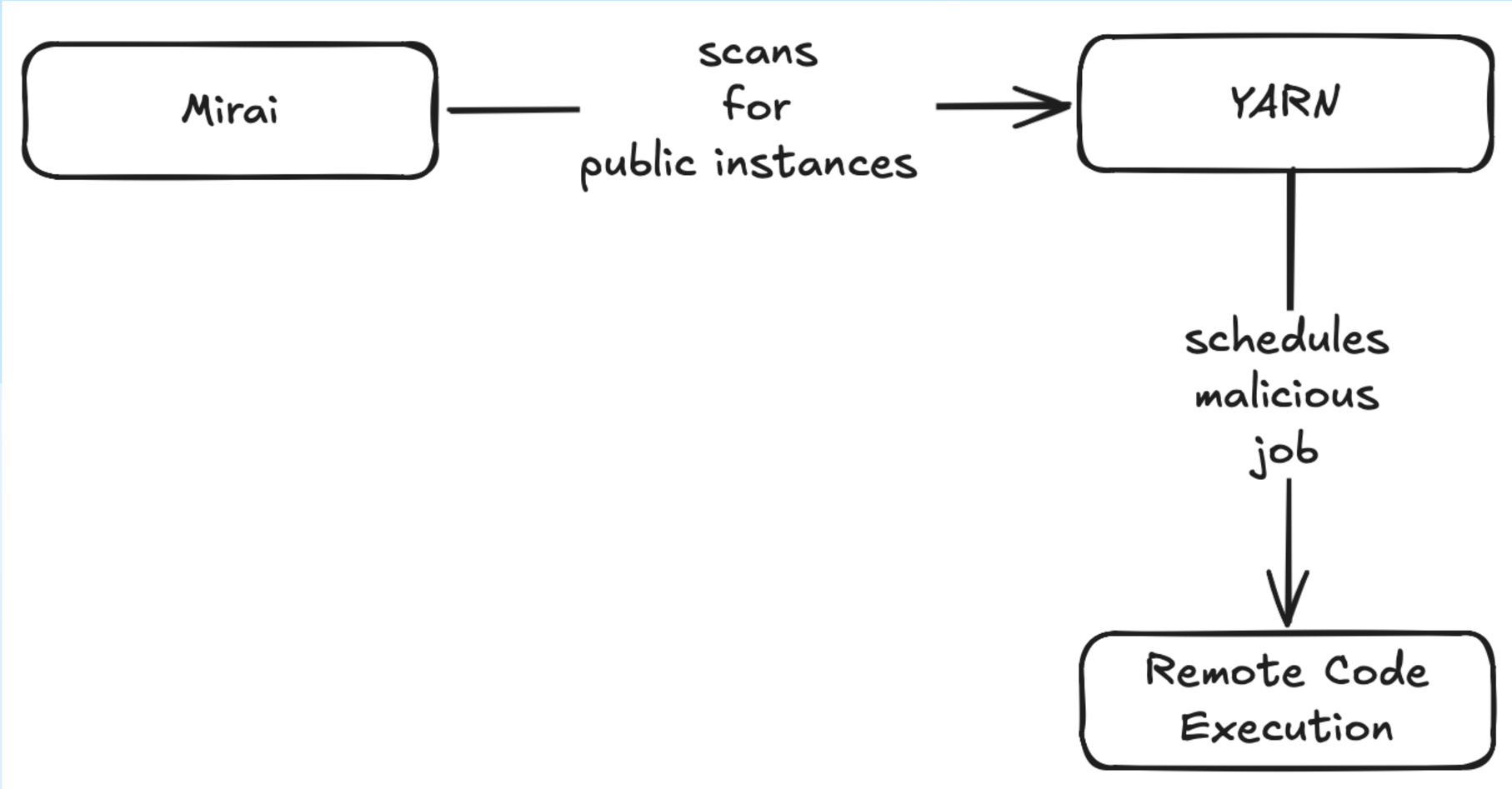
Security Operations actionable steps

1. Detect
2. Respond
3. Recover

Recovery methods: YARN case



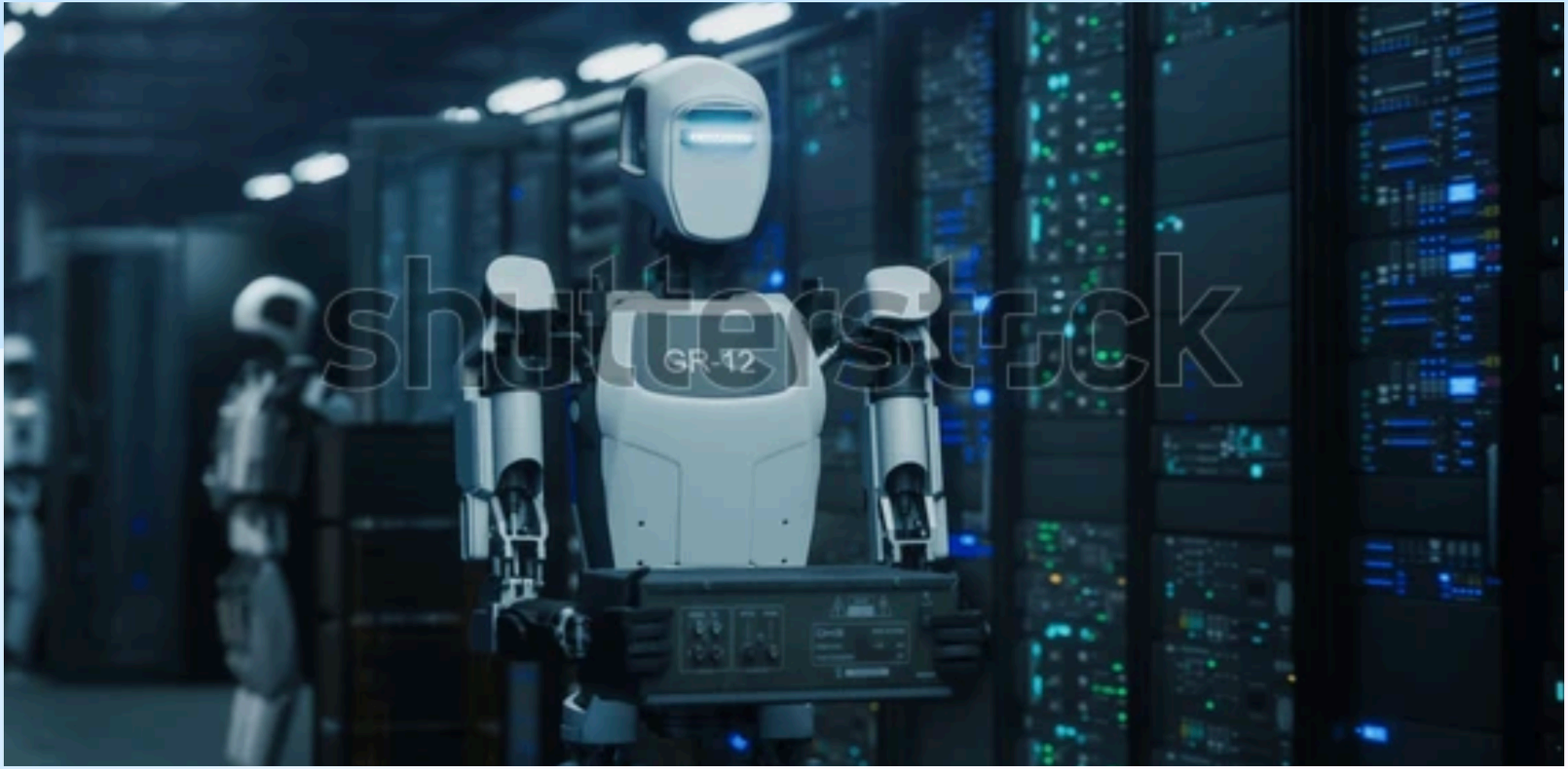
Recovery methods: YARN case



Recovery methods (could also be automated!)

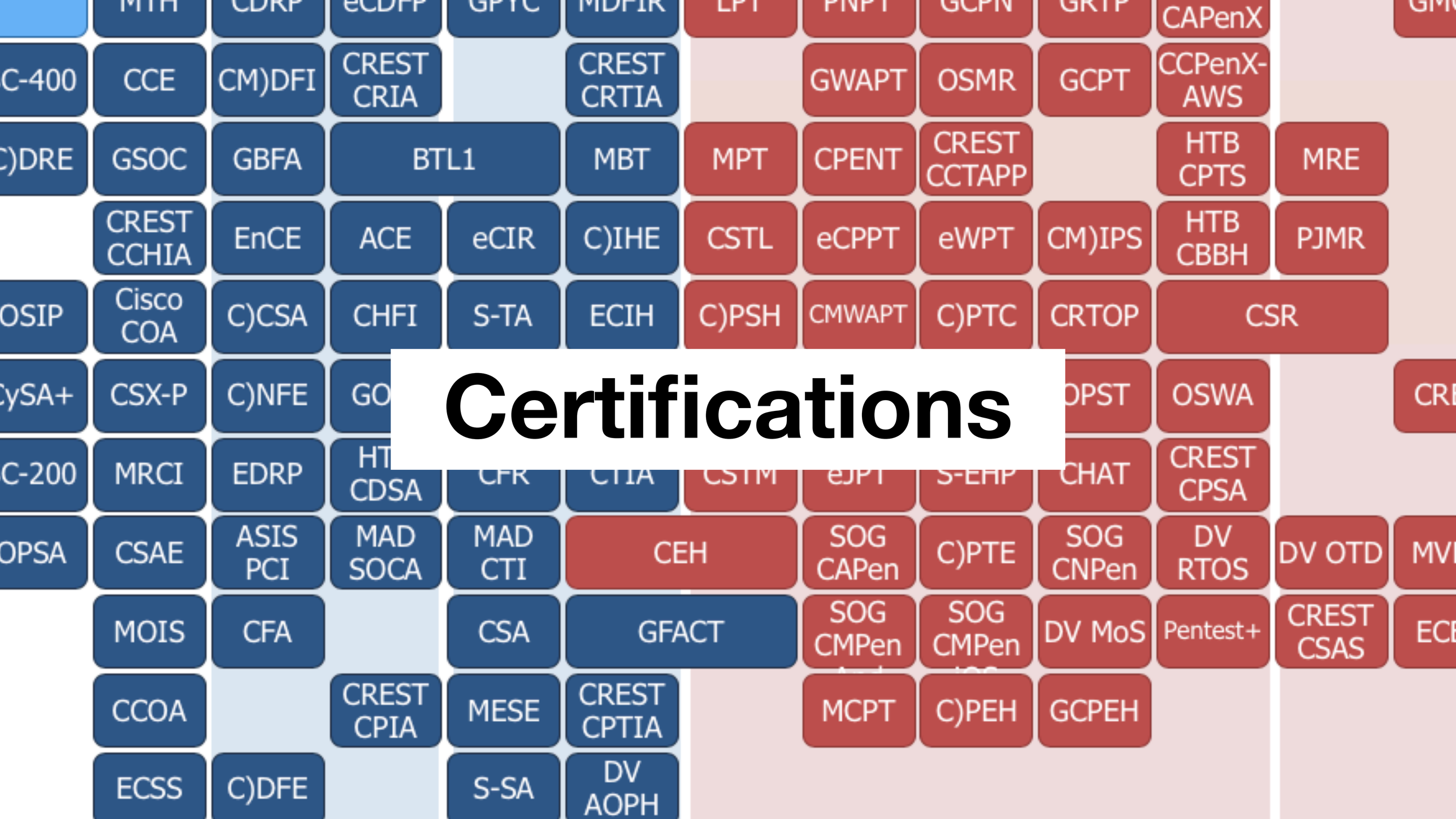
1. Forensics
2. Kill malicious pod in Kubernetes
3. Reinstall OS on your computer
4. Reissue compromised tokens
5. Restore backup of a database

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
MTH
CDRP
eCDFP
GPYC
MDFIR
LPT
PNPT
GCPN
GRTP
CAPenX
C-400
CCE
CM)DFI
CREST CRIA
CREST CRTIA
GWAPT
OSMR
GCPT
CCPenX-AWS
C)DRE
GSOC
GBFA
BTL1
MBT
MPT
CPENT
CREST CCTAPP
HTB CPTS
MRE
CREST CCHIA
EnCE
ACE
eCIR
C)IHE
CSTL
eCPPT
eWPT
CM)IPS
HTB CBBH
PJMR
OSIP
Cisco COA
C)CSA
CHFI
S-TA
ECIH
C)PSH
CMWAPT
C)PTC
CRTOP
CSR
CySA+
CSX-P
C)NFE
GO
OPST
OSWA
CR
C-200
MRCI
EDRP
HT
CDSA
CFR
CTIA
CSTM
eJPT
S-EHP
CHAT
CREST CPSA
OPSA
CSAE
ASIS PCI
MAD SOCA
MAD CTI
CEH
SOG CAPen
C)PTE
SOG CNPen
DV RTOS
DV OTD
MV
MOIS
CFA
CSA
GFACT
SOG CMPen
SOG CMPen
DV MoS
Pentest+
CREST CSAS
EC
CCOA
CREST CPIA
MESE
CREST CPTIA
MCPT
C)PEH
GCPEH
ECSS
C)DFE
S-SA
DV AOPH

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