BSides London 2023

Scaling Detection and Response Teams

Enabling Efficient Investigations

WHOAMI

James Dorgan
@FranticTyping

What I Do:
Principal Incident Responder
CSIRT @ Coinbase

What I've Done:
10+ Years in Incident
Response, MDR, Research

What I Like:
Incident Response
Detection Engineering
CSIRT Continuous Improvement

Agenda

- **Challenges in Scaling Detection and Response Teams**
  - Why Focus on Efficient Investigations?
  - Symptoms of Low Investigation Maturity
- **Case Studies:**
  - Automating Investigation & Response Workflows
  - Building Context into Detections
  - Bringing Employees into the Triage Process

Why Focus on Efficient Investigations?

Logging Maturity

- Modern SIEM Solutions
- Broad Logging Coverage
- Efficient Data Accessibility

Detection Maturity

- Vendor Detections
- Open Source Projects
- MITRE ATT&CK®
- Threat Detection Lifecycles

Investigation Maturity

- Push Everything into JIRA
- “All the data you need is in the SIEM”
- Good luck; Have Fun

Response Maturity

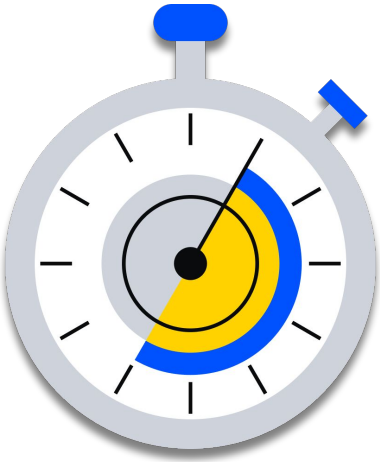
- Low Volume (Hopefully)
- IR Playbooks
- Vendor Capabilities

Phases Adapted From The Funnel of Fidelity (Jared Atkinson - SpecterOps)

Choose Your Own ~~Adventure~~ Investigation

Case Management / ALERT-11409

An anomalous SSO login suceeded for the user foo.bar@coinbase.com from the IP Address 12.12.12.12 (Geolocated: France)



What recent logins does this user have? - *[IdP Logs / 2FA Logs]*

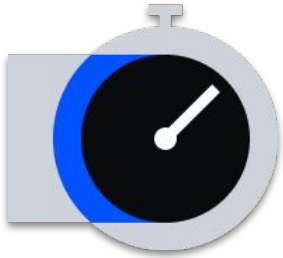
What team does the user work in, and where are they located?
- [HR Tool Lookup]

What devices are assigned to the user? - *[Asset Management Tool]*

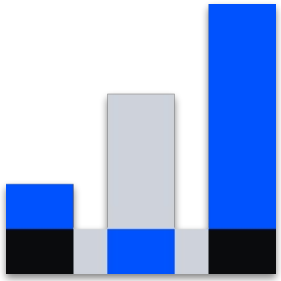
Are the devices and user currently online? - *[Slack / EDR Tooling]*

What recent alerts have we had for the user's account and their devices?
- *[Alert / Incident DB]*

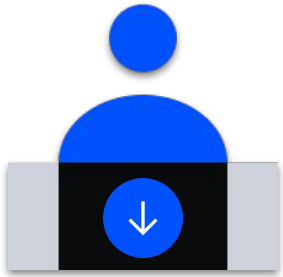
Symptoms Of Limited Investigation Maturity



Delayed Alert Triaging



No Shared Investigative Baseline

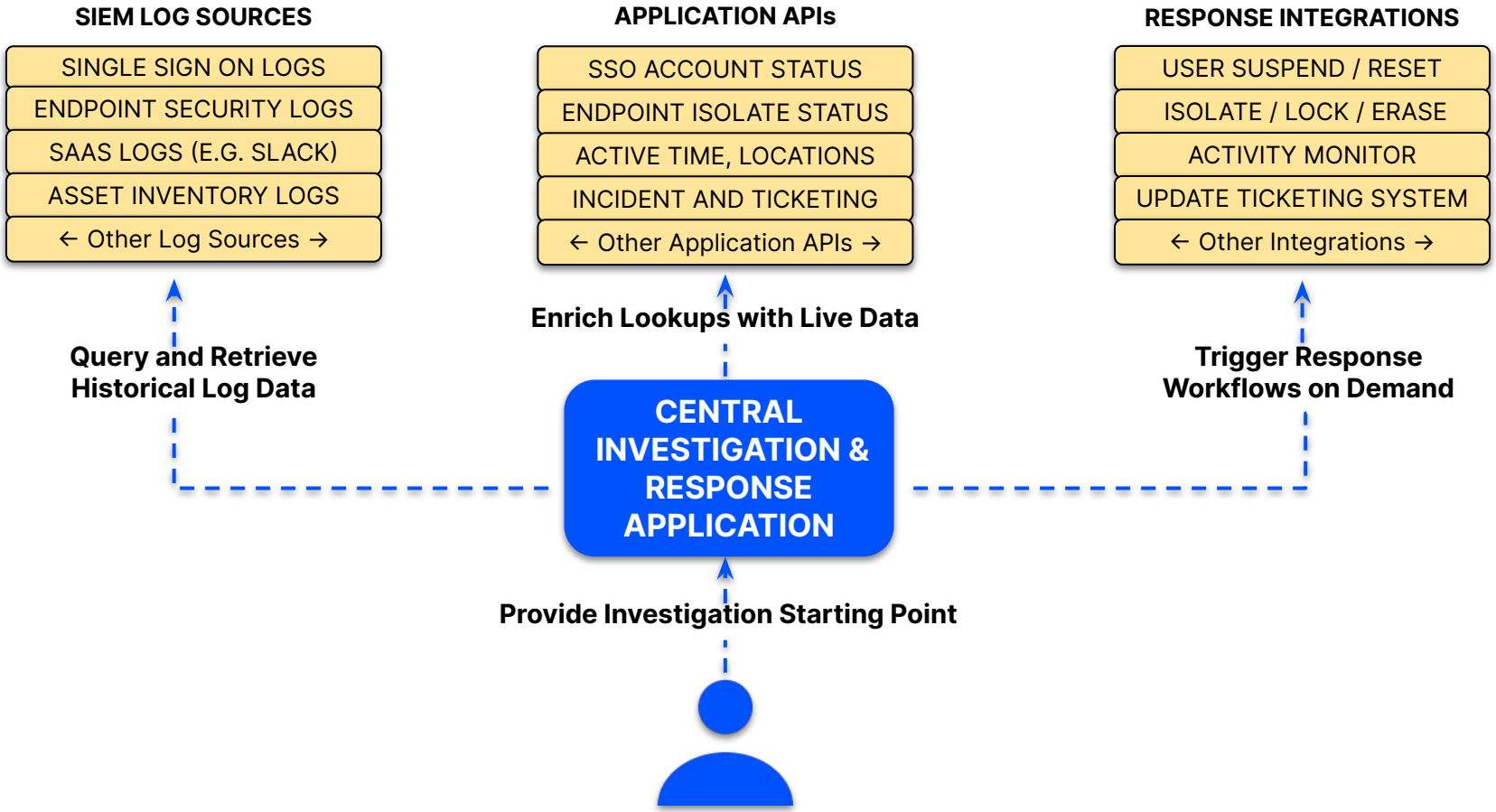


Increased Analyst Fatigue

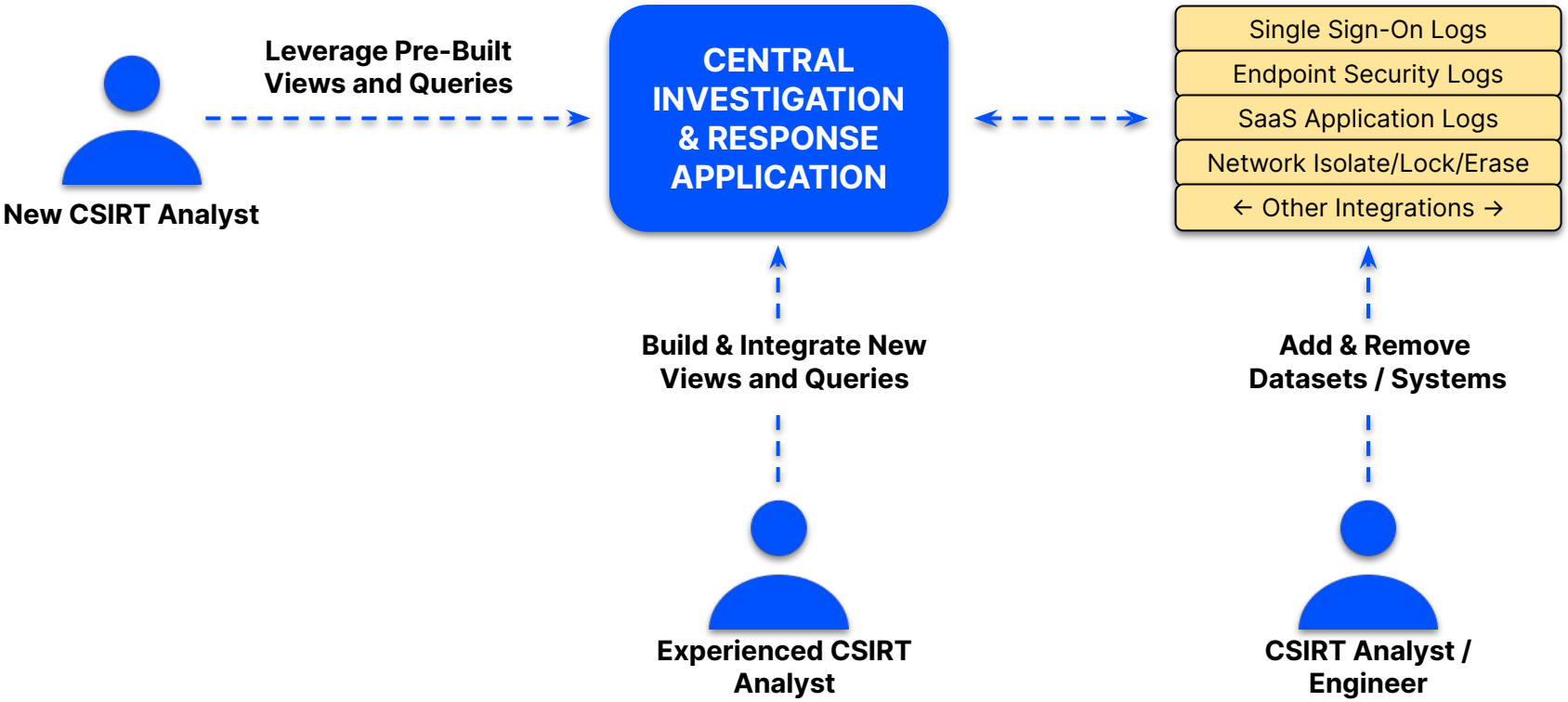
It takes too long, per detection, to perform a meaningful investigation

Automating Investigation & Response Workflows

The High Level Vision

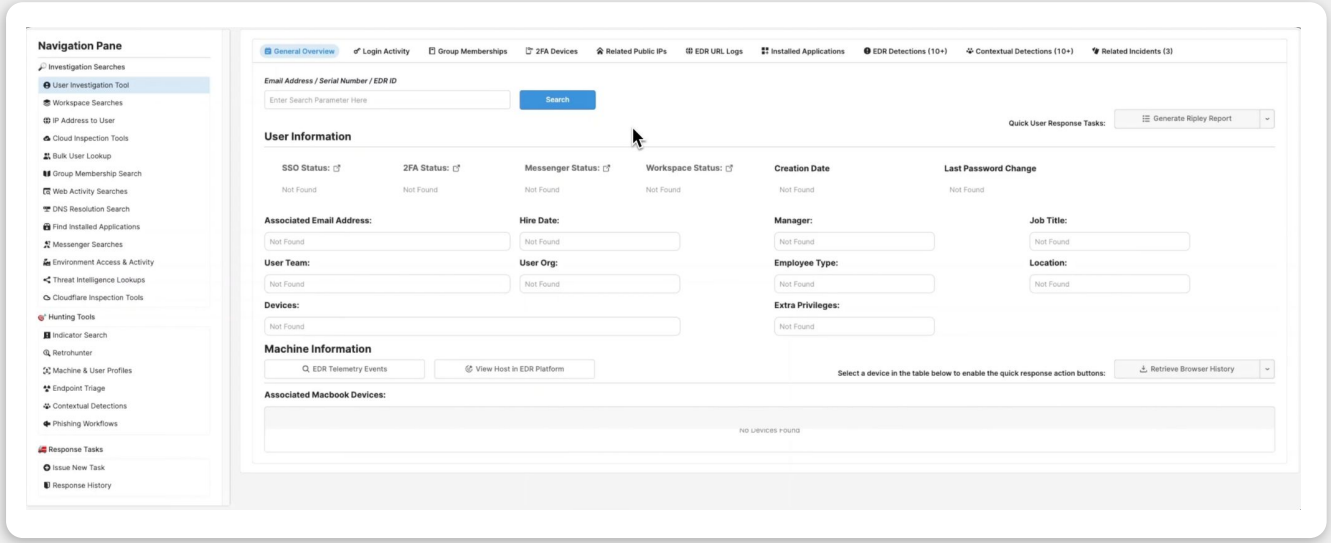


Unexpected Side Benefits



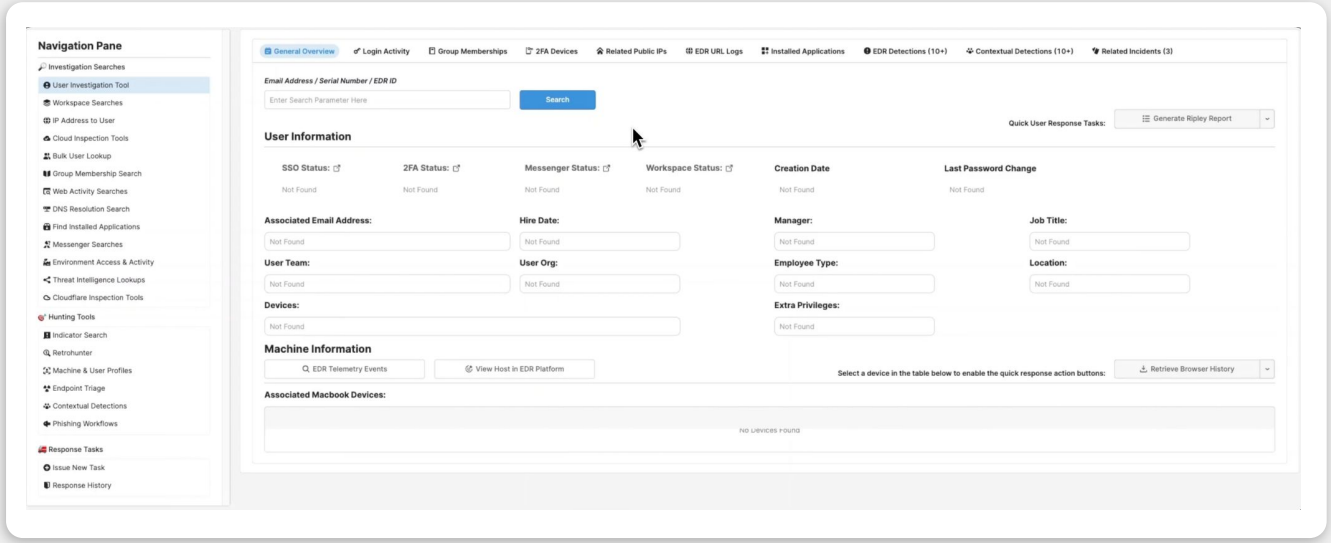
Investigation Demo

- Overview of the Investigation & Response Application
- Establish Key Investigation Information about a User

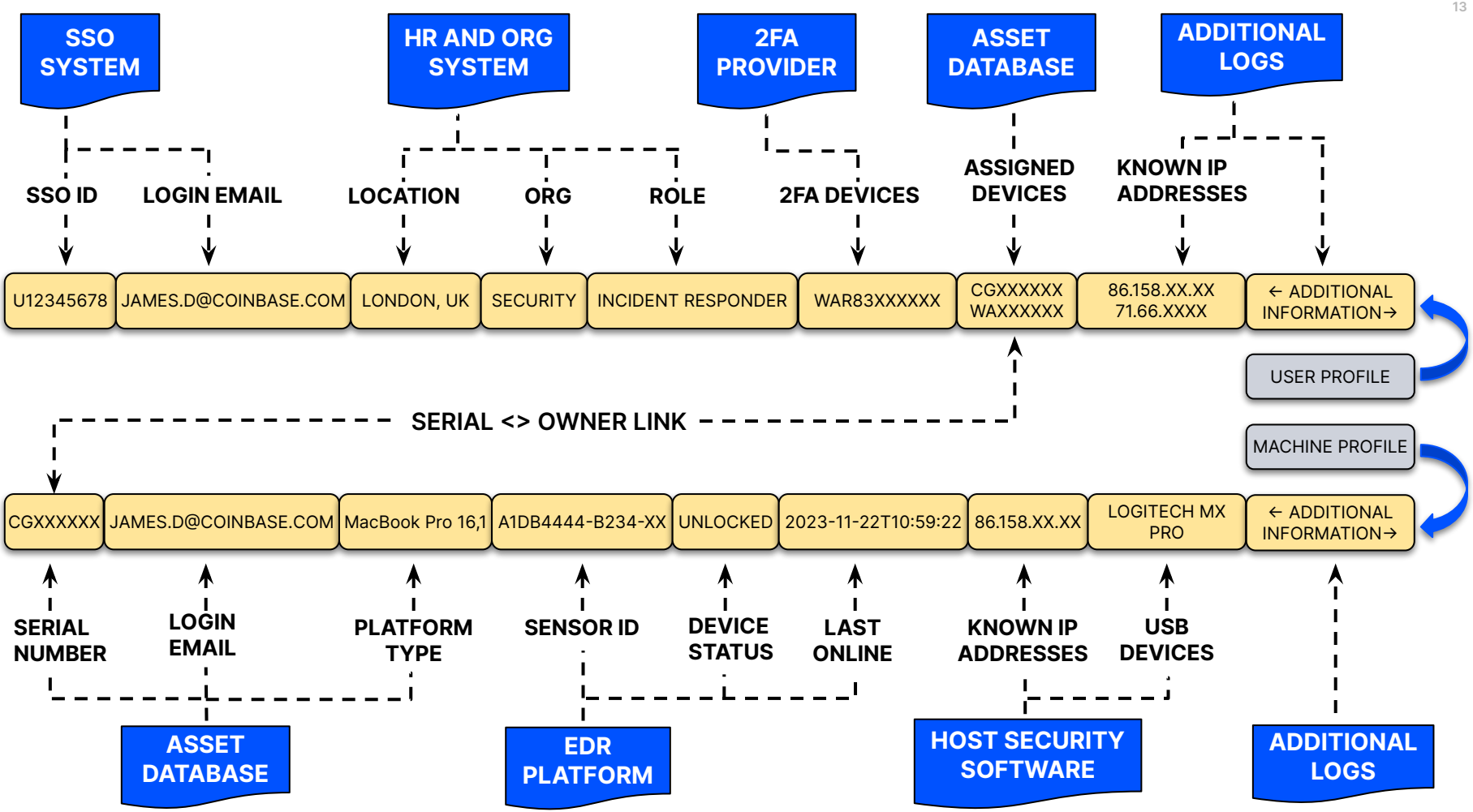


Response Demo

- Overview of Response Capabilities
- Suspend a target user from all relevant systems

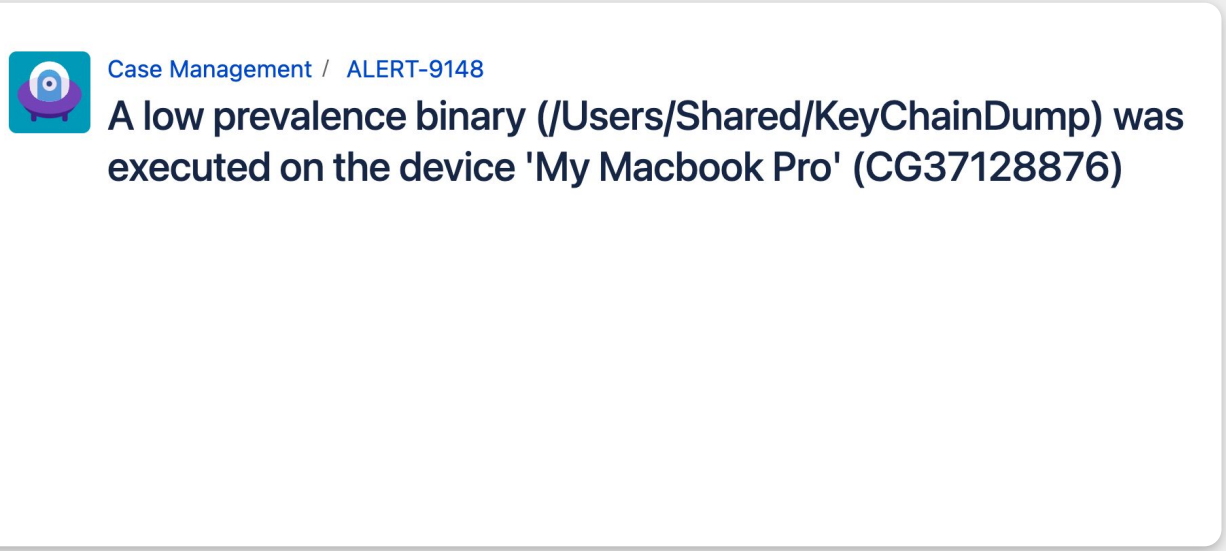


Building Context into Detections


SSO SYSTEM
HR AND ORG SYSTEM
2FA PROVIDER
ASSET DATABASE
ADDITIONAL LOGS
SSO ID
LOGIN EMAIL
LOCATION
ORG
ROLE
2FA DEVICES
ASSIGNED DEVICES
KNOWN IP ADDRESSES
U12345678
JAMES.D@COINBASE.COM
LONDON, UK
SECURITY
INCIDENT RESPONDER
WAR83XXXXXX
CGXXXXXX WAXXXXXX
86.158.XX.XX 71.66.XXXX
← ADDITIONAL INFORMATION→
USER PROFILE
SERIAL <> OWNER LINK
MACHINE PROFILE
CGXXXXXX
JAMES.D@COINBASE.COM
MacBook Pro 16,1
A1DB4444-B234-XX
UNLOCKED
2023-11-22T10:59:22
86.158.XX.XX
LOGITECH MX PRO
← ADDITIONAL INFORMATION→
SERIAL NUMBER
LOGIN EMAIL
PLATFORM TYPE
SENSOR ID
DEVICE STATUS
LAST ONLINE
KNOWN IP ADDRESSES
USB DEVICES
ASSET DATABASE
EDR PLATFORM
HOST SECURITY SOFTWARE
ADDITIONAL LOGS

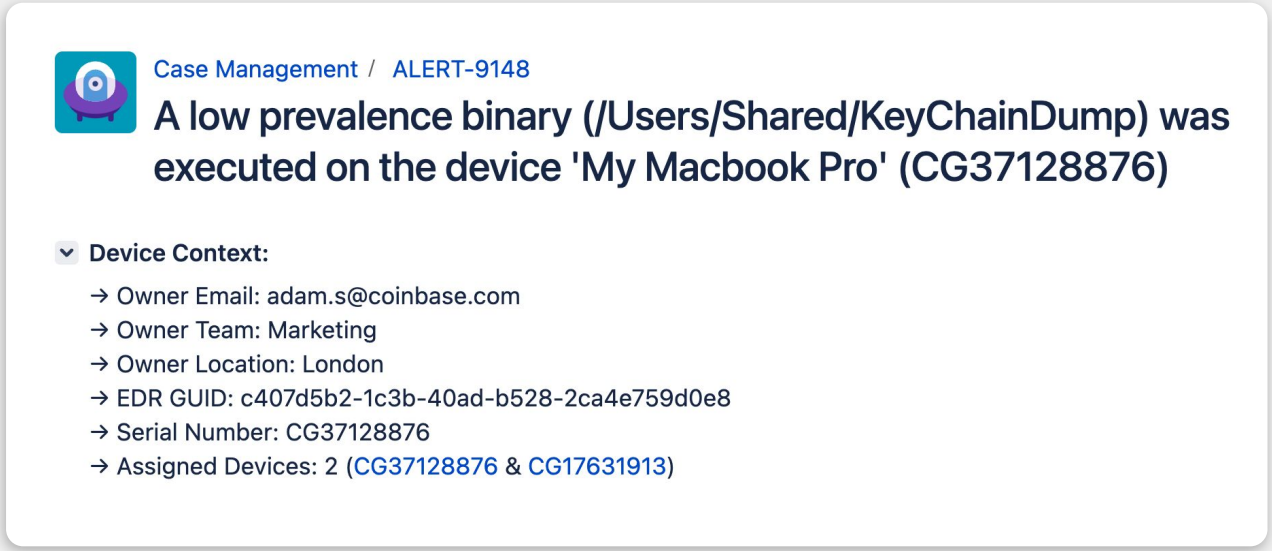
Post-Detection Enrichment

- Use Pivot Points in detections to pull in relevant context from the User & Machine Profiles



Post-Detection Enrichment

- Use Pivot Points in detections to pull in relevant context from the User & Machine Profiles



Example Threat Detection

- Search for 2FA Enrollment Events
- Exclude events where the enrollment came from IPs assigned to the user's corporate devices

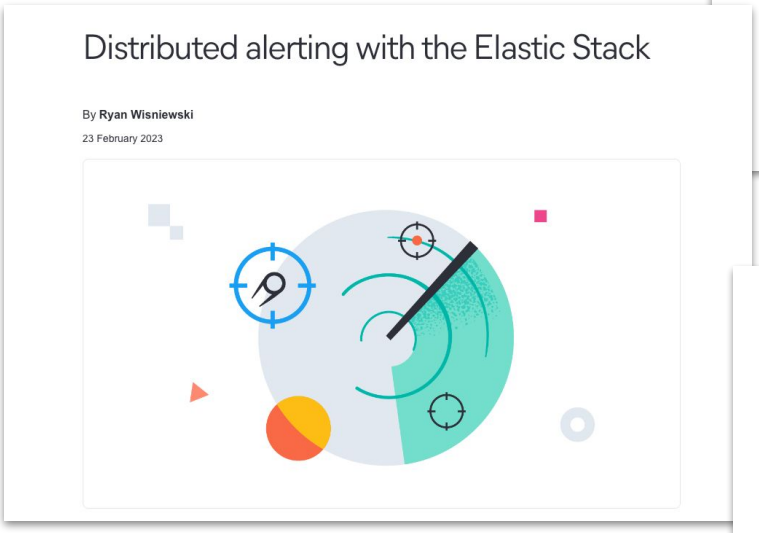
```
SELECT
        EMAIL,
        IP_ADDRESS as IP
FROM 2FA_LOGS
        LEFT JOIN MACHINE_PROFILES MP
        ON (
                EMAIL = MP.OWNER
                AND ARRAY_CONTAINS(IP,MP.KNOWN_IPS)
        )
WHERE
        EVENT_TYPE = 'enrollment'
        AND MP.SERIAL IS NULL
```

Bringing Employees into the Triage Process

Employees as a Data Source

- The most efficient investigation route is often to just ask someone what they did

Sharing is Caring



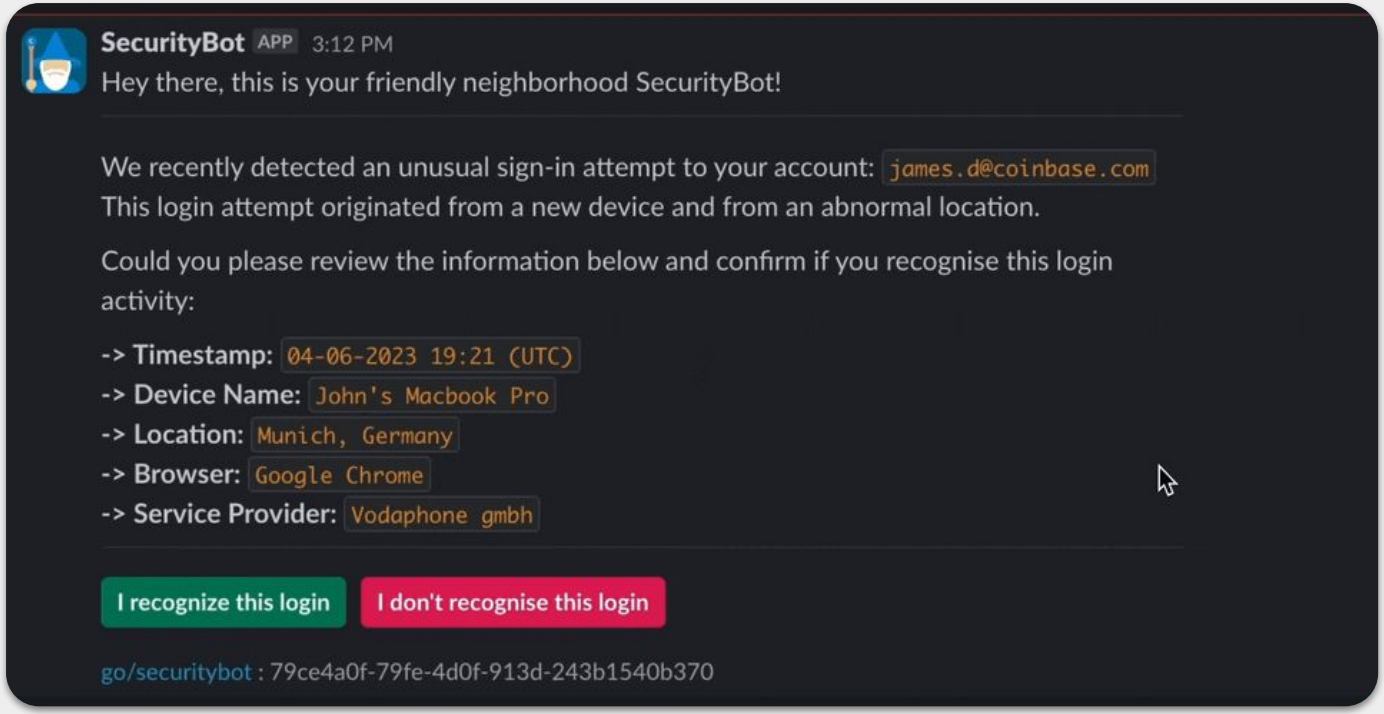
Elastic

DropBox

Palantir

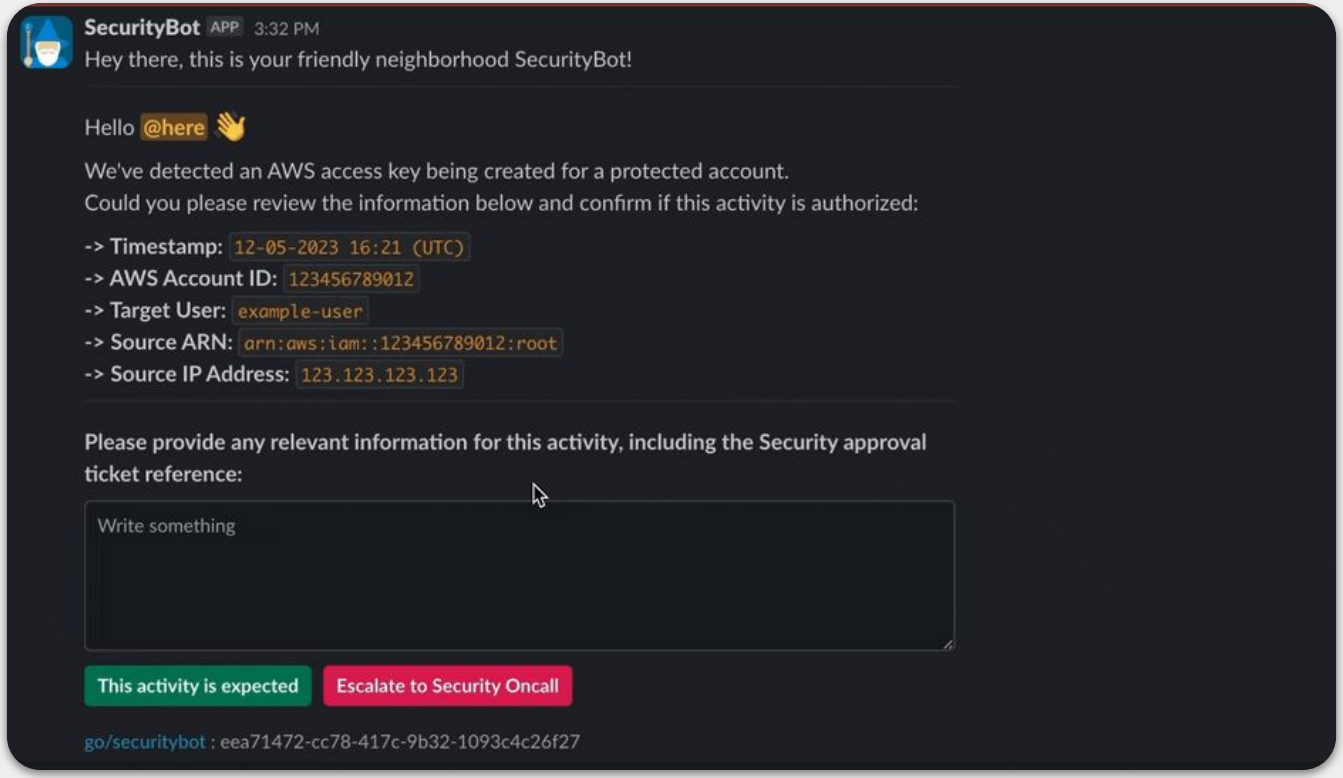
Employee Triage Example #1

- Anomalous login attempts are summarized and sent directly to the user for review



Employee Triage Example #2

- High-risk activities are sent to team channels for triage and context gathering
- 2FA is required before an alert can be dismissed

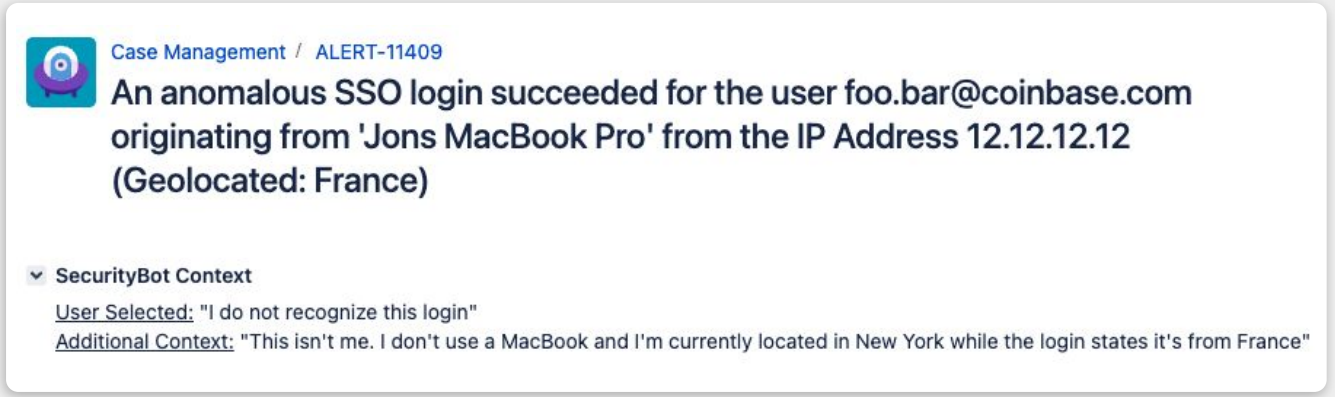


Detection Enrichment

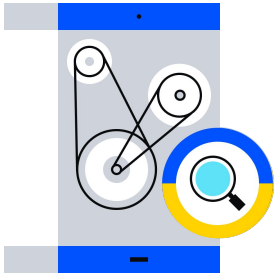
- A data source, not an authority
- Last 12 months:

700+ Interactions

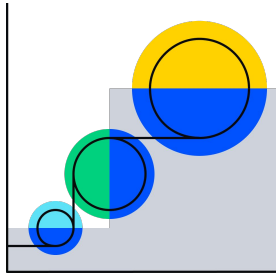
200+ Resolved Detections



Key Takeaways



Centralize & Automate Investigation Tasks



Build & Develop Team Investigation Baselines

Enrich Detections with Key Investigative Facts

James Dorgan
@FranticTyping