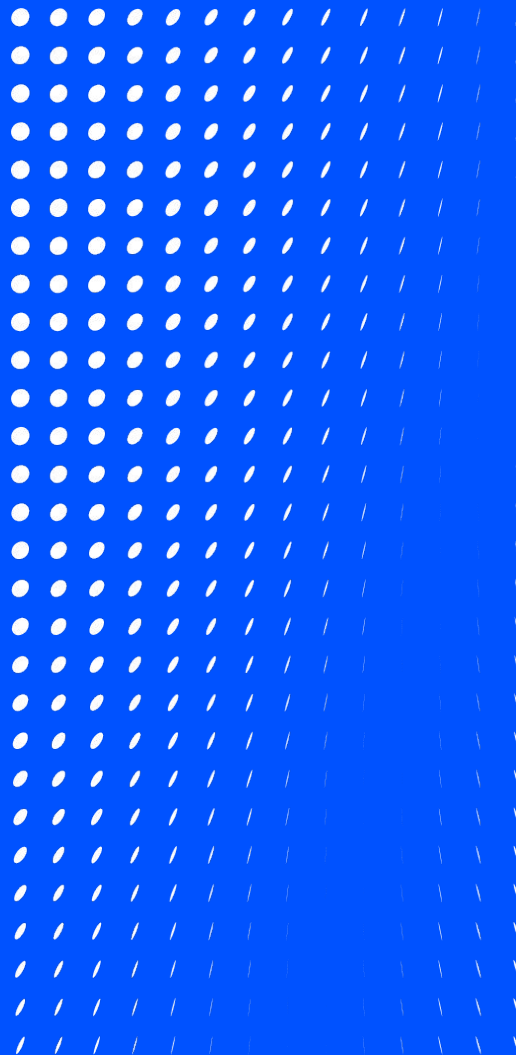




BSides London 2023

Scaling Detection and Response Teams

Enabling Efficient Investigations





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



- **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?

4



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

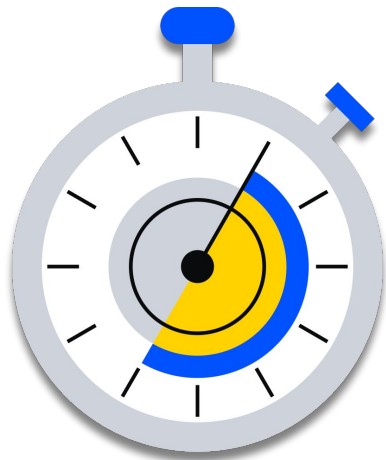
- Low Volume (Hopefully)
- IR Playbooks
- Vendor Capabilities

C Choose Your Own ~~Adventure~~ Investigation



Case Management / ALERT-11409

An anomalous SSO login succeeded 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]*

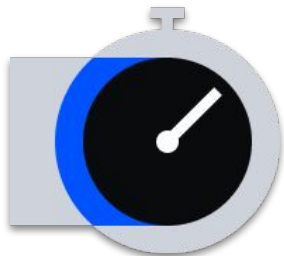
What devices are assigned to the user? - *[Asset Management Tool]*

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

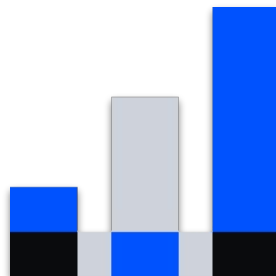
What recent alerts have we had for the user's account and their devices?
- *[Alert / Incident DB]*

⦿ Symptoms Of Limited Investigation Maturity

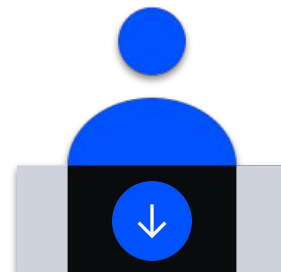
6



**Delayed Alert
Triageing**



**No Shared
Investigative Baseline**



**Increased Analyst
Fatigue**

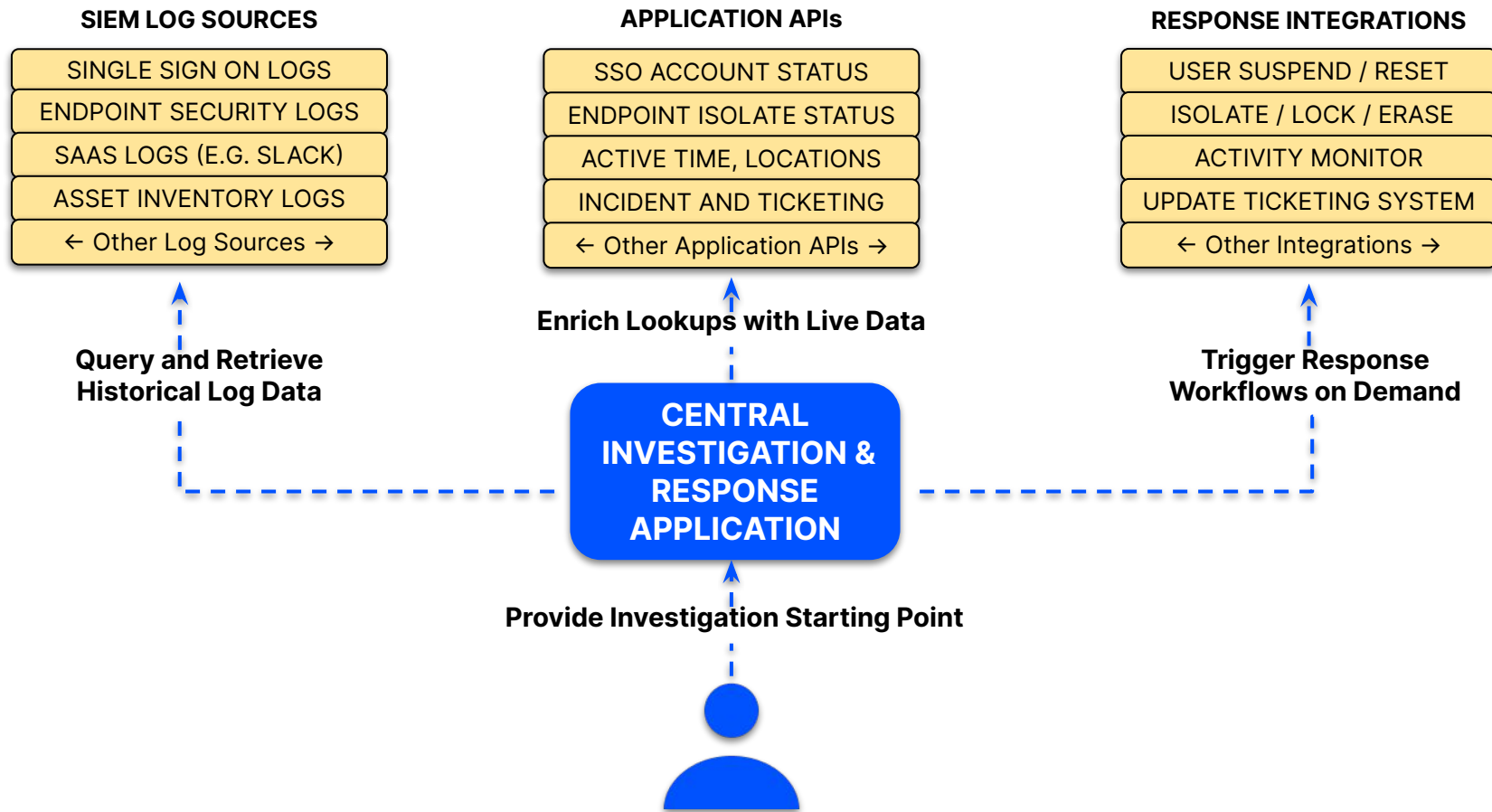
It takes too long, per detection, to perform a meaningful investigation



Automating Investigation & Response Workflows

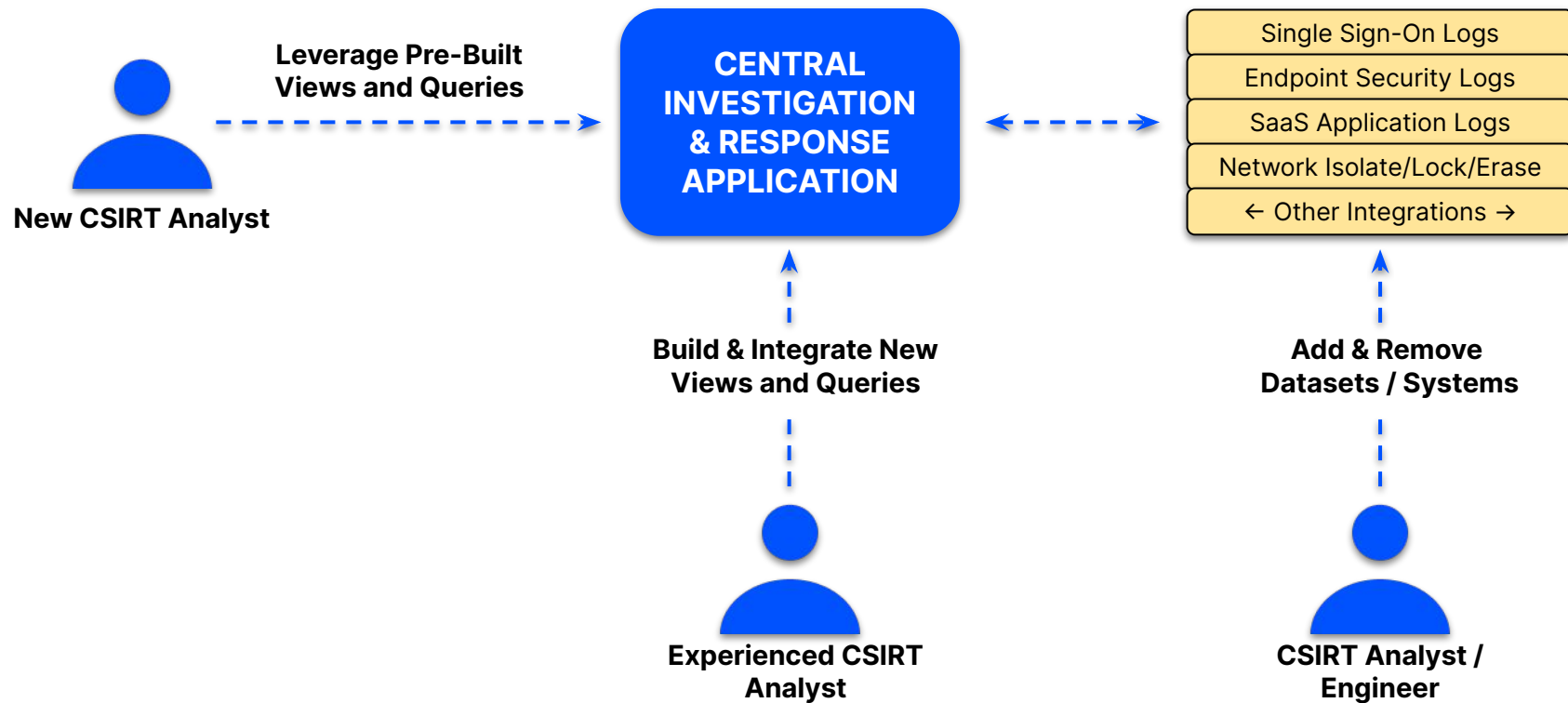
The High Level Vision

8



Unexpected Side Benefits

9





Investigation Demo

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

The screenshot displays the 'Investigation & Response' application interface. On the left is a 'Navigation Pane' with a tree view containing categories like 'Investigation Searches', 'Hunting Tools', and 'Response Tasks'. The main area is titled 'General Overview' and features a search bar for 'Email Address / Serial Number / EDR ID'. Below this, the 'User Information' section is active, showing a grid of status fields (SSO, 2FA, Messenger, Workspace) all marked 'Not Found'. It also includes input fields for 'Associated Email Address', 'Hire Date', 'User Team', 'User Org', 'Manager', 'Employee Type', 'Job Title', 'Location', and 'Extra Privileges'. A 'Machine Information' section at the bottom shows a table for 'Associated Macbook Devices' with the message 'NO DEVICES FOUND'. A 'Quick User Response Tasks' dropdown menu is visible in the top right corner.



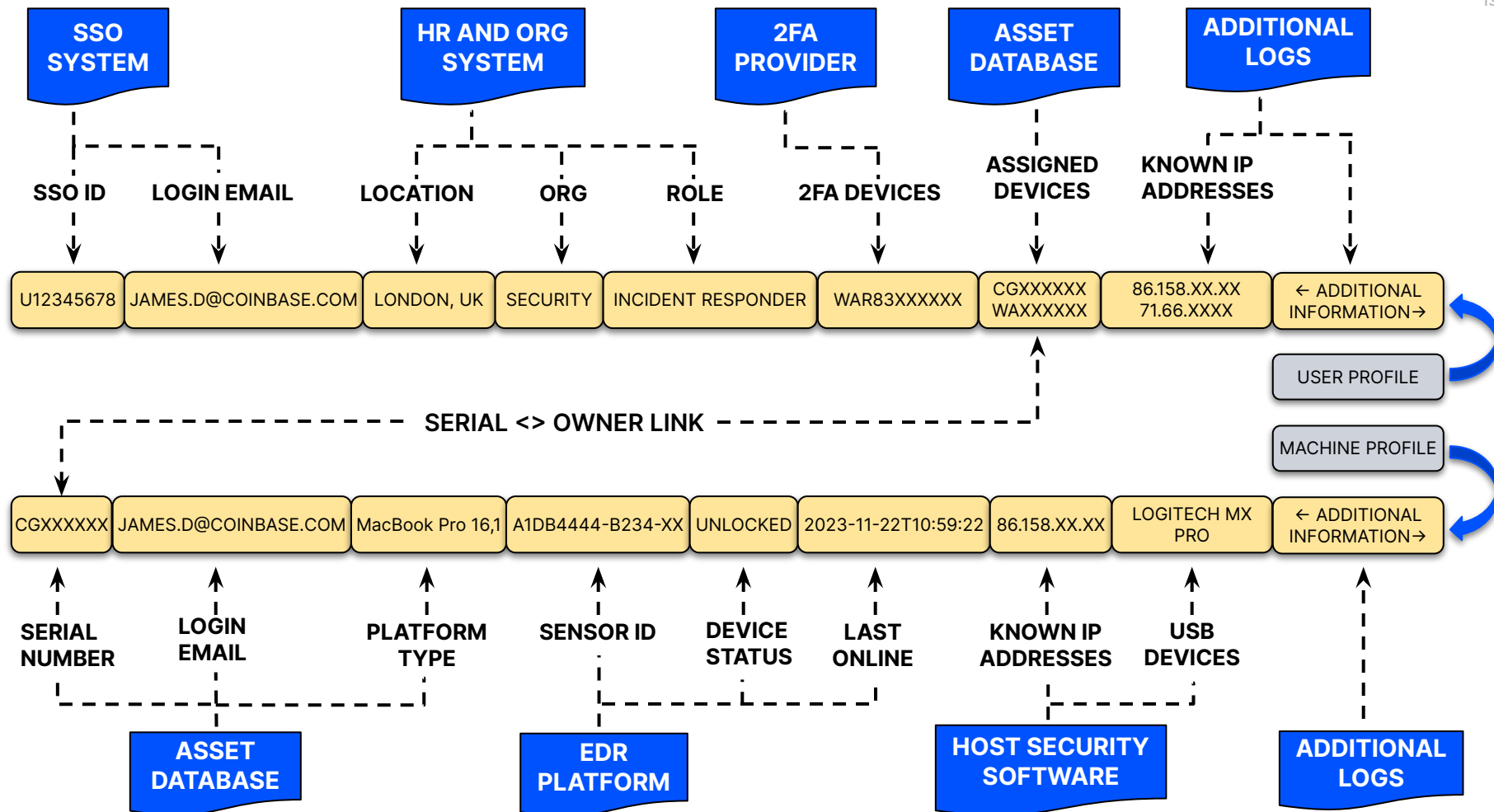
Response Demo

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

The screenshot displays a security response dashboard. On the left is a 'Navigation Pane' with a tree view containing categories like 'Investigation Searches', 'User Investigation Tool', 'Workspace Searches', 'IP Address to User', 'Cloud Inspection Tools', 'Bulk User Lookup', 'Group Membership Search', 'Web Activity Searches', 'DNS Resolution Search', 'Find Installed Applications', 'Messenger Searches', 'Environment Access & Activity', 'Threat Intelligence Lookups', 'Cloudflare Inspection Tools', 'Hunting Tools', 'Indicator Search', 'Retrohunter', 'Machine & User Profiles', 'Endpoint Triage', 'Contextual Detections', 'Phishing Workflows', 'Response Tasks', 'Issue New Task', and 'Response History'. The 'User Investigation Tool' is selected. The main panel has a top navigation bar with tabs: 'General Overview' (active), 'Login Activity', 'Group Memberships', '2FA Devices', 'Related Public IPs', 'EDR URL Logs', 'Installed Applications', 'EDR Detections (10+)', 'Contextual Detections (10+)', and 'Related Incidents (3)'. Below the tabs is a search bar labeled 'Email Address / Serial Number / EDR ID' with a 'Search' button. A 'Quick User Response Tasks' dropdown menu is set to 'Generate Egle Report'. The 'User Information' section contains fields for SSO Status, 2FA Status, Messenger Status, Workspace Status, Creation Date, and Last Password Change, all showing 'Not Found'. Below this are fields for Associated Email Address, Hire Date, Manager, Job Title, User Team, User Org, Employee Type, and Location, also showing 'Not Found'. The 'Devices' section shows 'Not Found'. The 'Machine Information' section has buttons for 'EDR Telemetry Events' and 'View Host in EDR Platform'. The 'Associated Macbook Devices' section shows 'NO DEVICES FOUND'. A 'Retrieve Browser History' button is at the bottom right.



Building Context into Detections





Post-Detection Enrichment

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



Case Management / ALERT-9148

A low prevalence binary (/Users/Shared/KeyChainDump) was executed on the device 'My Macbook Pro' (CG37128876)



Post-Detection Enrichment

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



Case Management / ALERT-9148

A low prevalence binary (/Users/Shared/KeyChainDump) was executed on the device 'My Macbook Pro' (CG37128876)

▼ **Device Context:**

- Owner Email: adam.s@coinbase.com
- Owner Team: Marketing
- Owner Location: London
- EDR GUID: c407d5b2-1c3b-40ad-b528-2ca4e759d0e8
- Serial Number: CG37128876
- Assigned Devices: 2 ([CG37128876](#) & [CG17631913](#))



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



Case Management / ALERT-11409

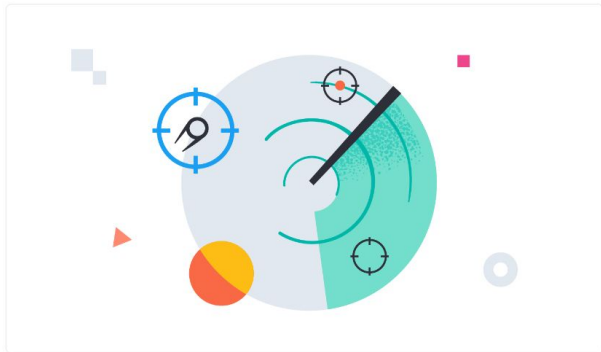
An anomalous SSO login succeeded for the user foo.bar@coinbase.com originating from 'Jons MacBook Pro' from the IP Address 12.12.12.12 (Geolocated: France)

Sharing is Caring

Distributed alerting with the Elastic Stack

By Ryan Wisniewski

23 February 2023



Elastic

Meet Securitybot: Open Sourcing Automated Security at Scale

DropBox

Democratizing Security Detection



Palantir · [Follow](#)

Published in Palantir Blog · 13 min read · Jun 2, 2022



21

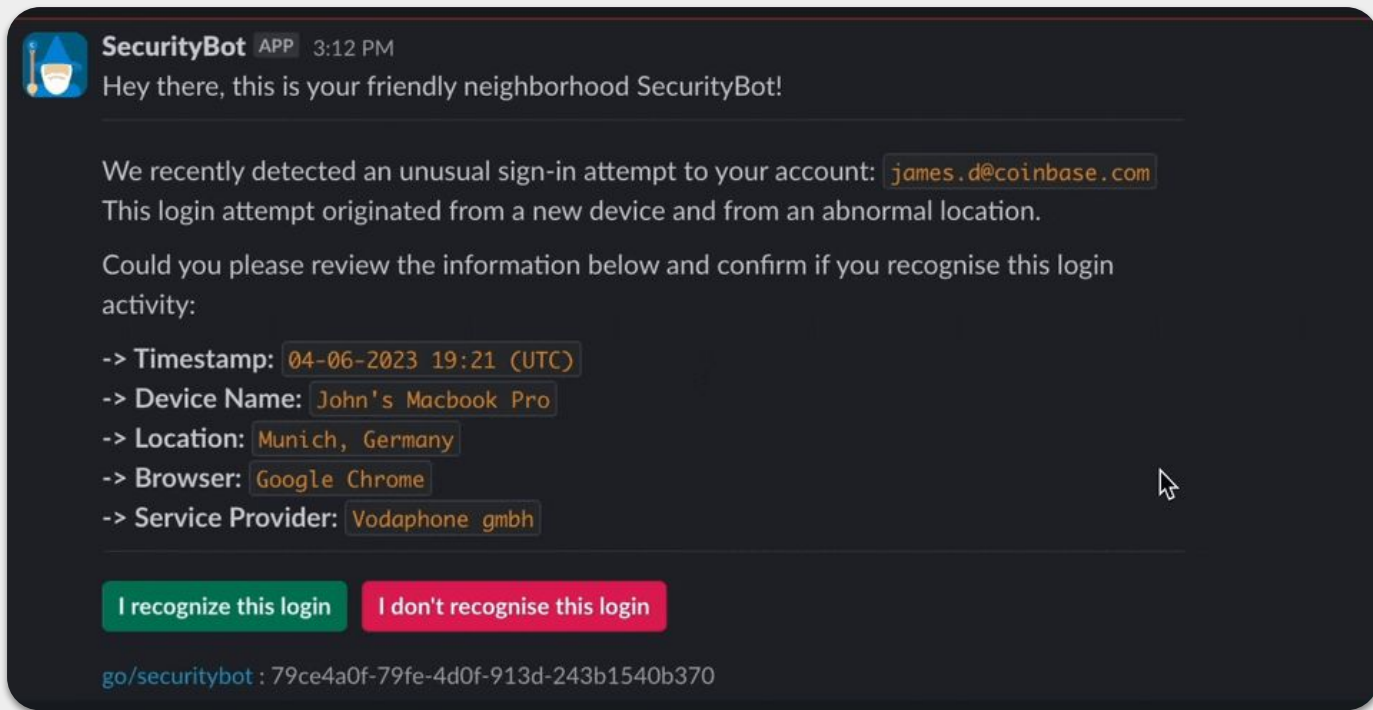


Palantir



Employee Triage Example #1

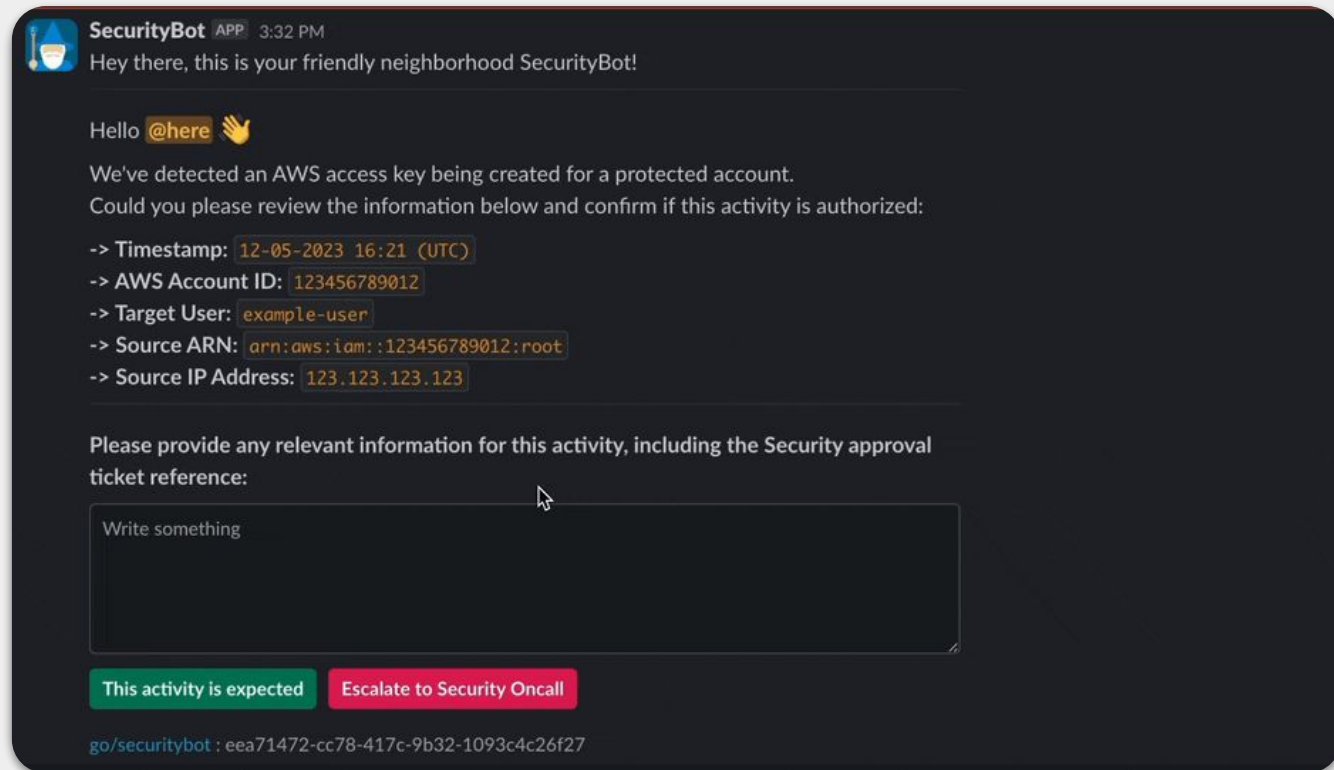
- Anomalous login attempts are summarized and sent directly to the user for review





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



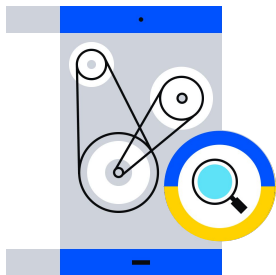
Case Management / ALERT-11409

**An anomalous SSO login succeeded for the user foo.bar@coinbase.com
originating from 'Jons MacBook Pro' from the IP Address 12.12.12.12
(Geolocated: France)**

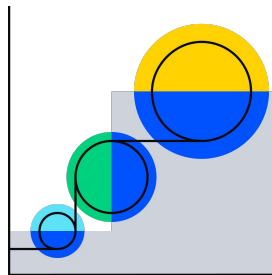
▼ SecurityBot Context

User Selected: "I do not recognize this login"

Additional Context: "This isn't me. I don't use a MacBook and I'm currently located in New York while the login states it's from France"



**Centralize &
Automate
Investigation Tasks**



**Build & Develop
Team Investigation
Baselines**



**Enrich Detections
with Key Investigative
Facts**