SOAR IN SOC

From Reactive to Proactive

I WHOAMI

HAYDEN COVINGTON

Current: SOC @ Black Hills Information Security
SOC SecOps Lead
DFIR Consultant
Detection Engineering
Threat Hunting
SOAR Engineering
Alert Monitoring

Previously: SOC @ a shipyard
Tier 2 SOC, CSIRT
Detection Engineering
Insider Threat
SOAR Engineer

S O A R

Security Orchestration Automation and Response

(S)ECURITY ...

Specialized for security use cases & functions

. . . (O)RCHESTRATION, (A)TUOMATION, (R)ESPONSE

Enables in-depth automated actions on a number of levels

THE CHALLENGES

Why even get a SOAR?

AVERAGE WEEKLY MALWARE ALERTS . . .

That an organization receives in a week

17,000

19%

. . . NUMBER OF THOSE ALERTS DEEMED TO BE RELIABLE

(And that seems *very* high to me)

WHAT A SOAR ENABLES

AN INTENTIONAL WORD CHOICE

REDUCED ALERT FATIGUE

FASTER RESPONE TIME

CASE GROUPING

LESS MANUAL PROCESS

... AMONG MANY OTHER THINGS

HOW DOES IT DO THAT?

STREAMLINE	ENRICH
AUTOMATE	RESPOND

SO, WHAT CAN IT DO?

STREAMLINE

ENRICH

TRIAGE

AUTOMATE

RESPOND

SOAR'IN

Case study of Elastic's use of a SOAR called Tines

750 HOURS SAVED ANNUALLY

"ALERTS" BECOME "CASES"

Alert = Standalone indicator
Case = Combined, grouped indicators

---

3 FTES

ANALYST AUGMENTATION

Elastic states that their implementation performs the work of three full time analysts

https://www.tines.com/case-studies/elastic/

BHIS'IN

Early, **rough** metrics from the BHIS SOC's implementation

CASE GROUPING, RISK SCORING

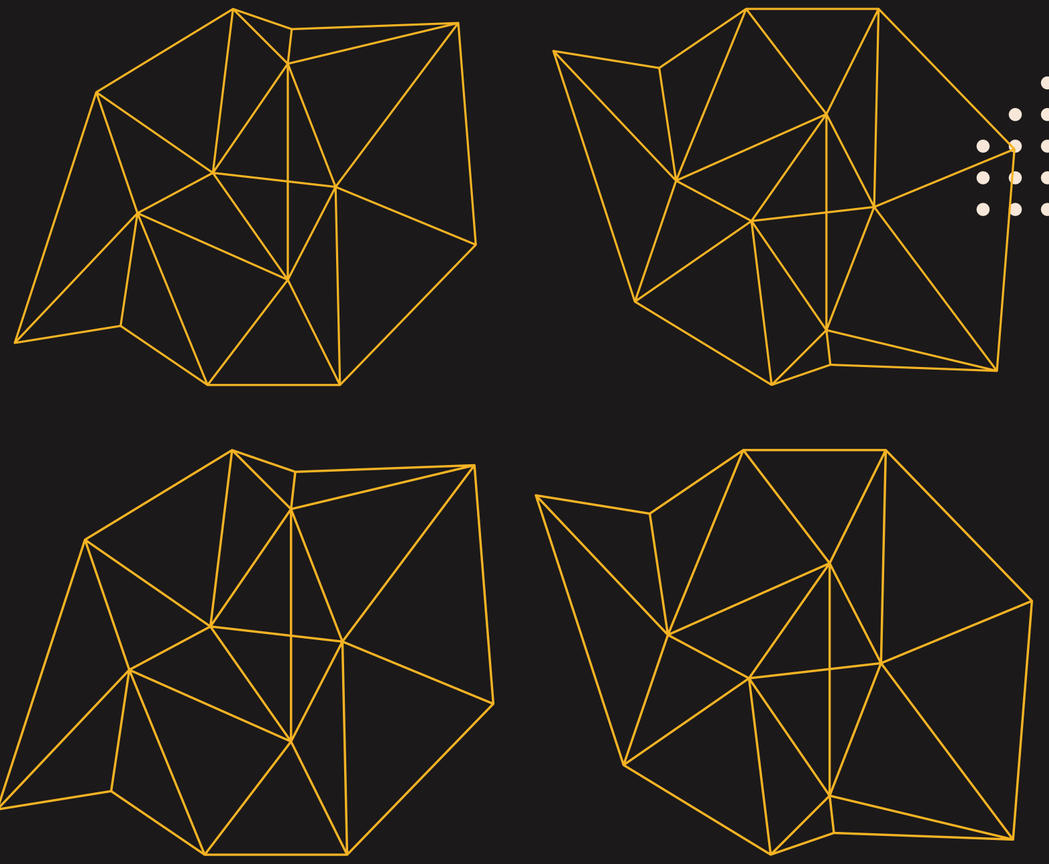
Rather than individual alerts, implementing comprehensive risk scoring + case grouping

~60% LESS NOISE

COMPLEX CASES

Complex cases + risk scoring results in greater effectiveness

~90% MORE FOCUS



SO . . .

WHY DOESN’T EVERYONE HAVE A SOAR?

BARRIER TO ENTRY

PRICETAG

A SOAR can be expensive, ranging anywhere from tens to hundreds of thousands a year

EXPERTISE

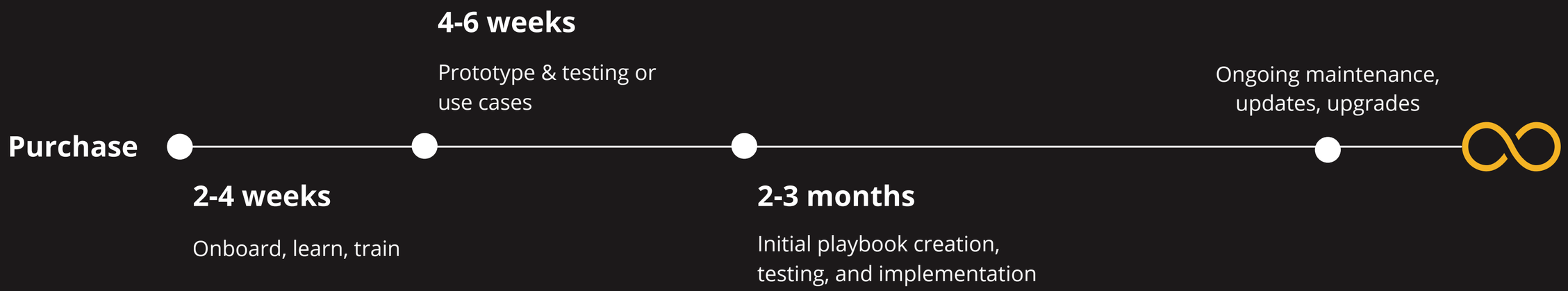
“SOAR Engineer” - like “AWS Engineer”, anything with a specialized engineer role tells me it can get complex fast

COMMITMENT

Long-term time commitment to build and maintain

IMPLEMENTATION TIMELINE

A rough example, depending on complexity and use case ...



... And this is assuming a level of technical expertise on your team

SKILLSET OF A SOAR ENGINEER

PROGRAMMING / SCRIPTING

- PYTHON
- BASH (TRANSFERABLE)
- POWERSHELL (TRANSFERABLE)

SKILLSET OF A SOAR ENGINEER

UNDERSTANDING OF SECURITY OPERTAIONS

- WHAT THE ISSUES ARE
- HOW TO ADDRESS THEM
- QUALITY CONTROL

SKILLSET OF A SOAR ENGINEER

API FAMILIARITY

- “WHAT IS AN API”
- HOW TO USE THEM AT THE DEEPEST LEVEL
- CHAINING REQUESTS

SKILLSET OF A SOAR ENGINEER

DATA MANIPULATION

- NORMALIZATION
- PARSING
- JSON, UNSTRUCTURED, STRUCTURED

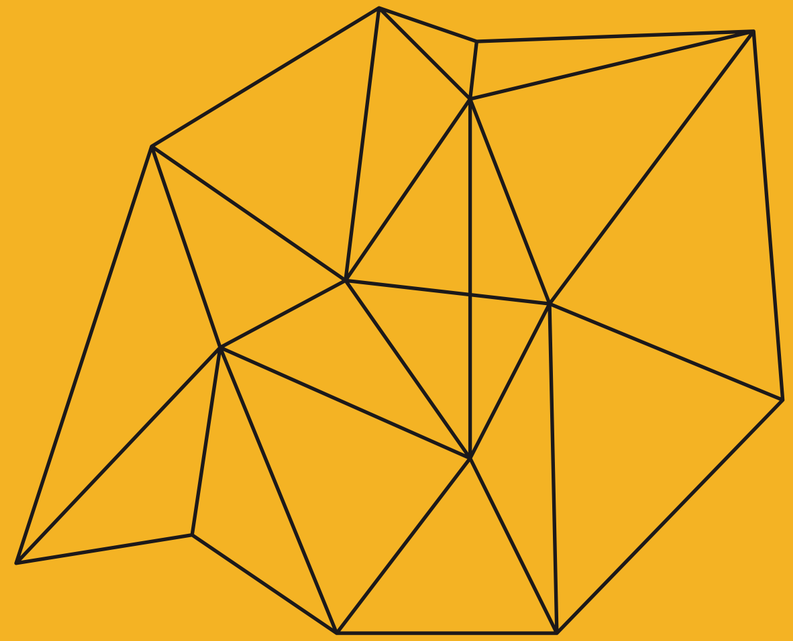
AND ABOVE ALL ELSE . . .

ANALYTICAL THINKING & PROBLEM SOLVING

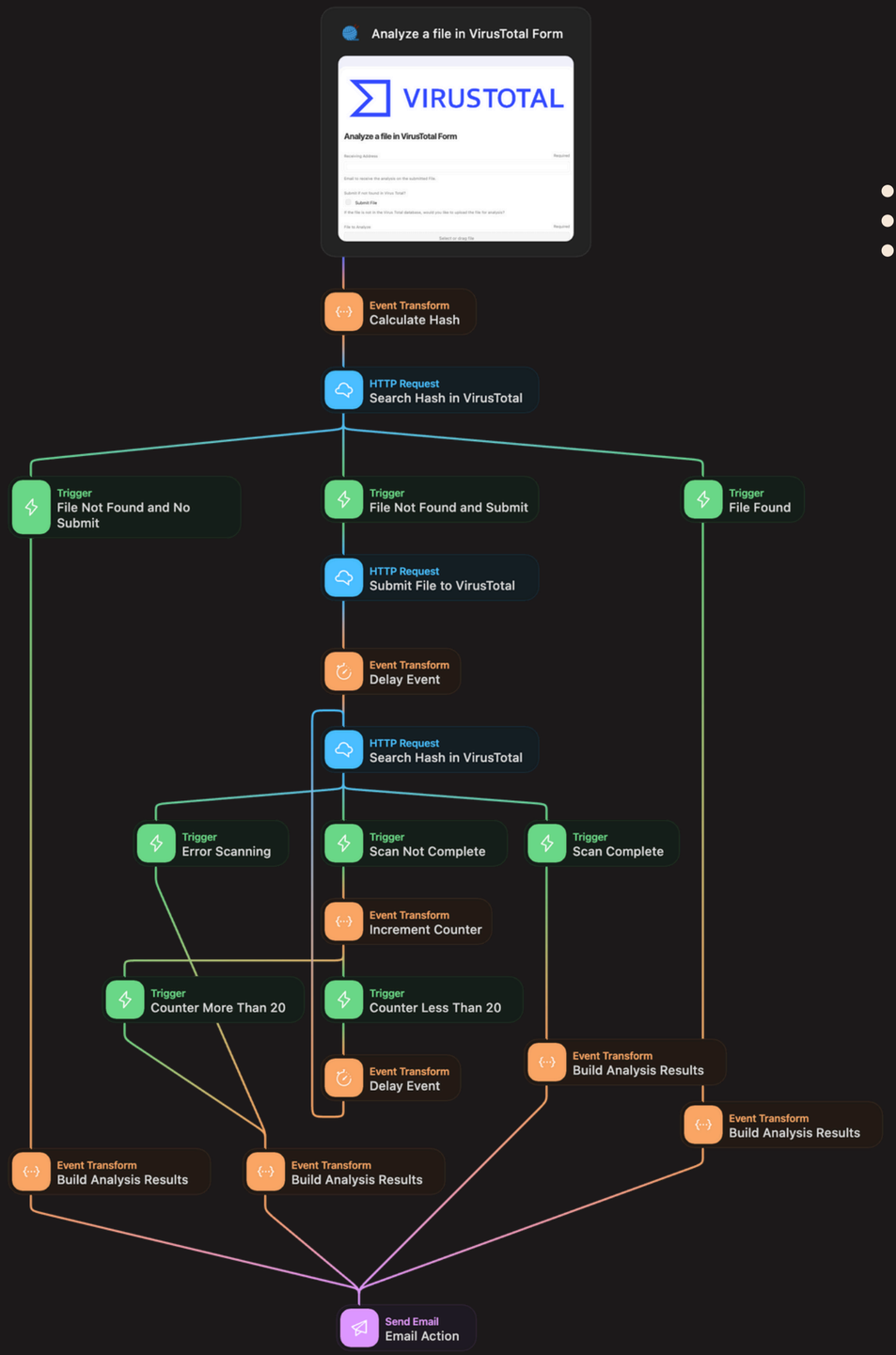
- EVERYTHING ELSE CAN BE TAUGHT
- APPROACH THE PROBLEM IN UNIQUE WAYS
- CREATE REUSABLE, STRUCTURED PLAYBOOKS

PLAYBOOKS

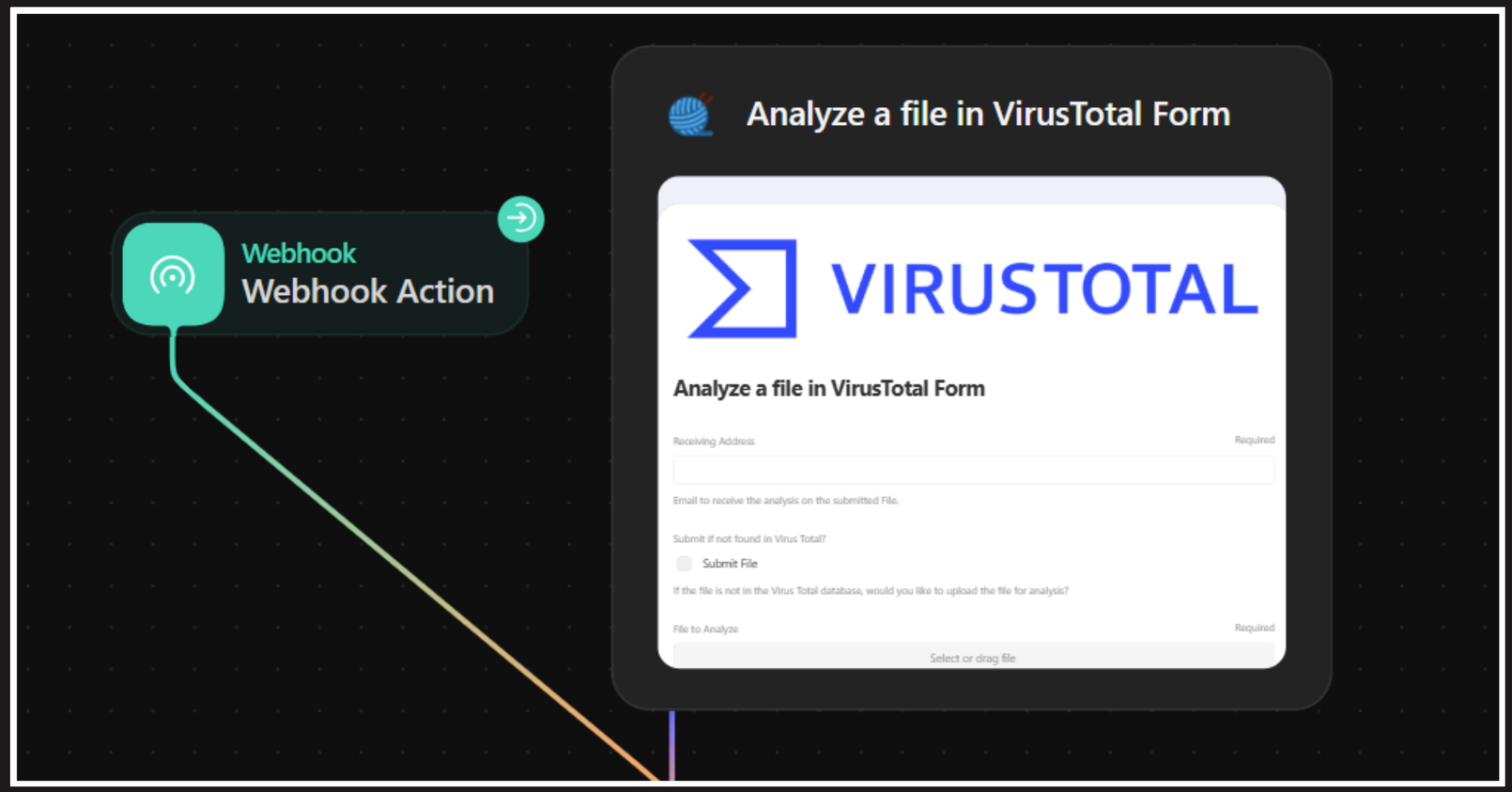
THE BUILDING BLOCKS OF SOAR



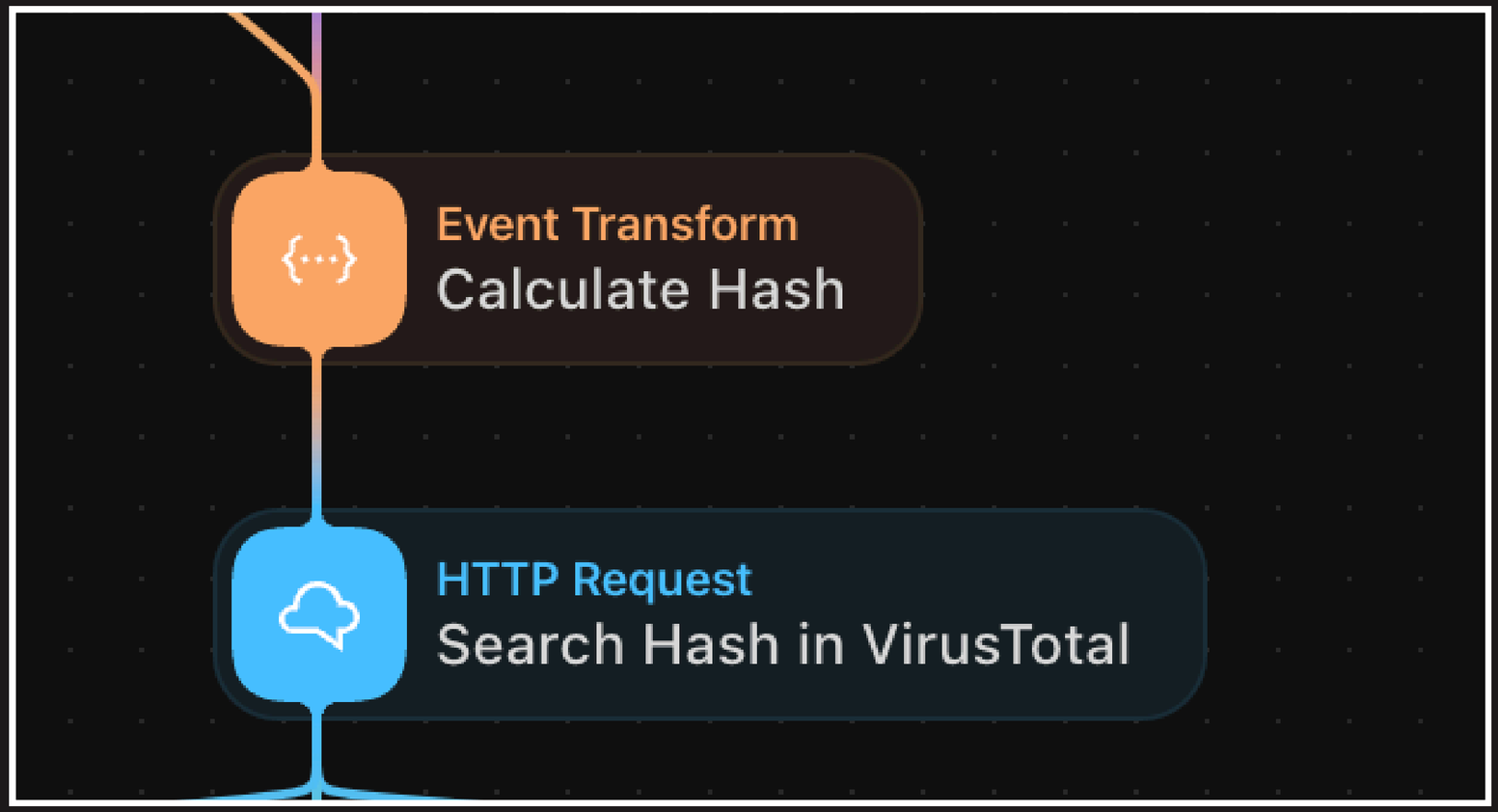
EXAMPLE PLAYBOOK



TRIGGERS, ACTIONS, AND DECISIONS



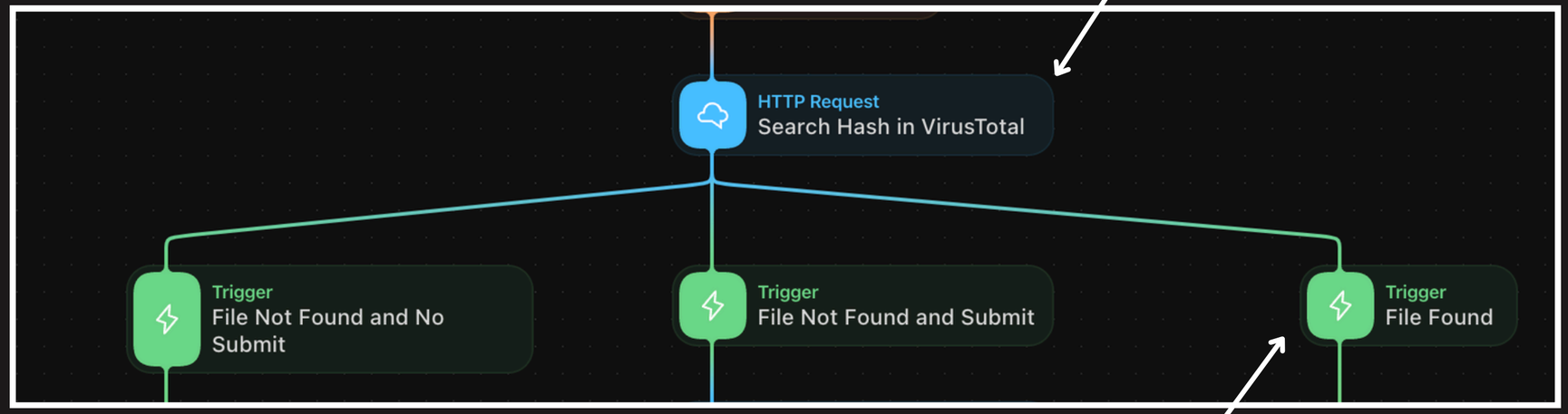
TRIGGERS, ACTIONS, AND DECISIONS



TRIGGERS, ACTIONS, AND DECISIONS

Options

```
{
  "url": "https://www.virustotal.com/api/v3/files/<<calculate_hash.hash>>",
  "content_type": "application_json",
  "method": "get",
  "payload": {},
  "headers": {
    "x-apikey": "<<CREDENTIAL.virustotal>>"
  },
  "retry_on_status": [
    "429"
  ]
}
```



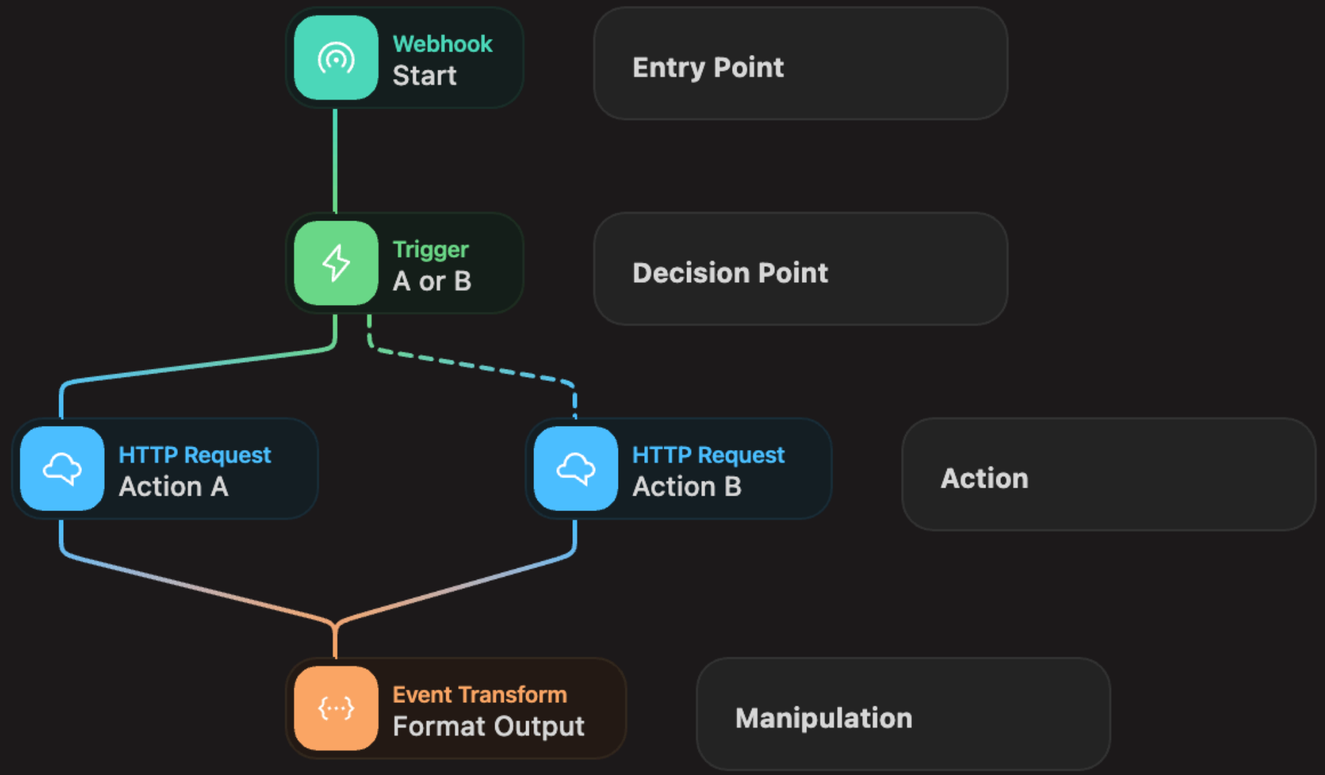
Rules

{} search_hash_in_virustotal.status

is equal to

200

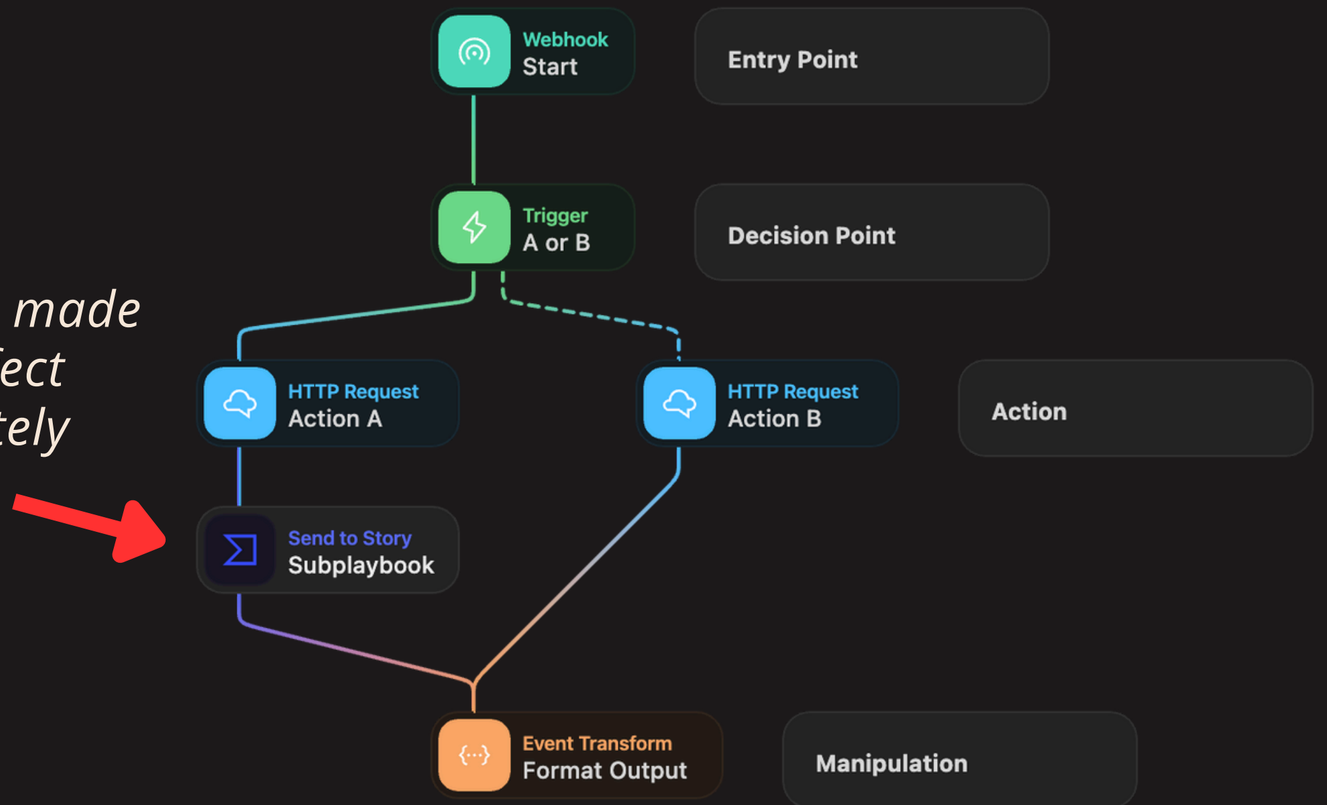
I STRUCTURE


Webhook
Start
Entry Point
Trigger
A or B
Decision Point
HTTP Request
Action A
HTTP Request
Action B
Action
Event Transform
Format Output
Manipulation

SUB-PLAYBOOKS

A PLAYBOOK MEANT TO BE USED BY OTHERS (A FUNCTION)

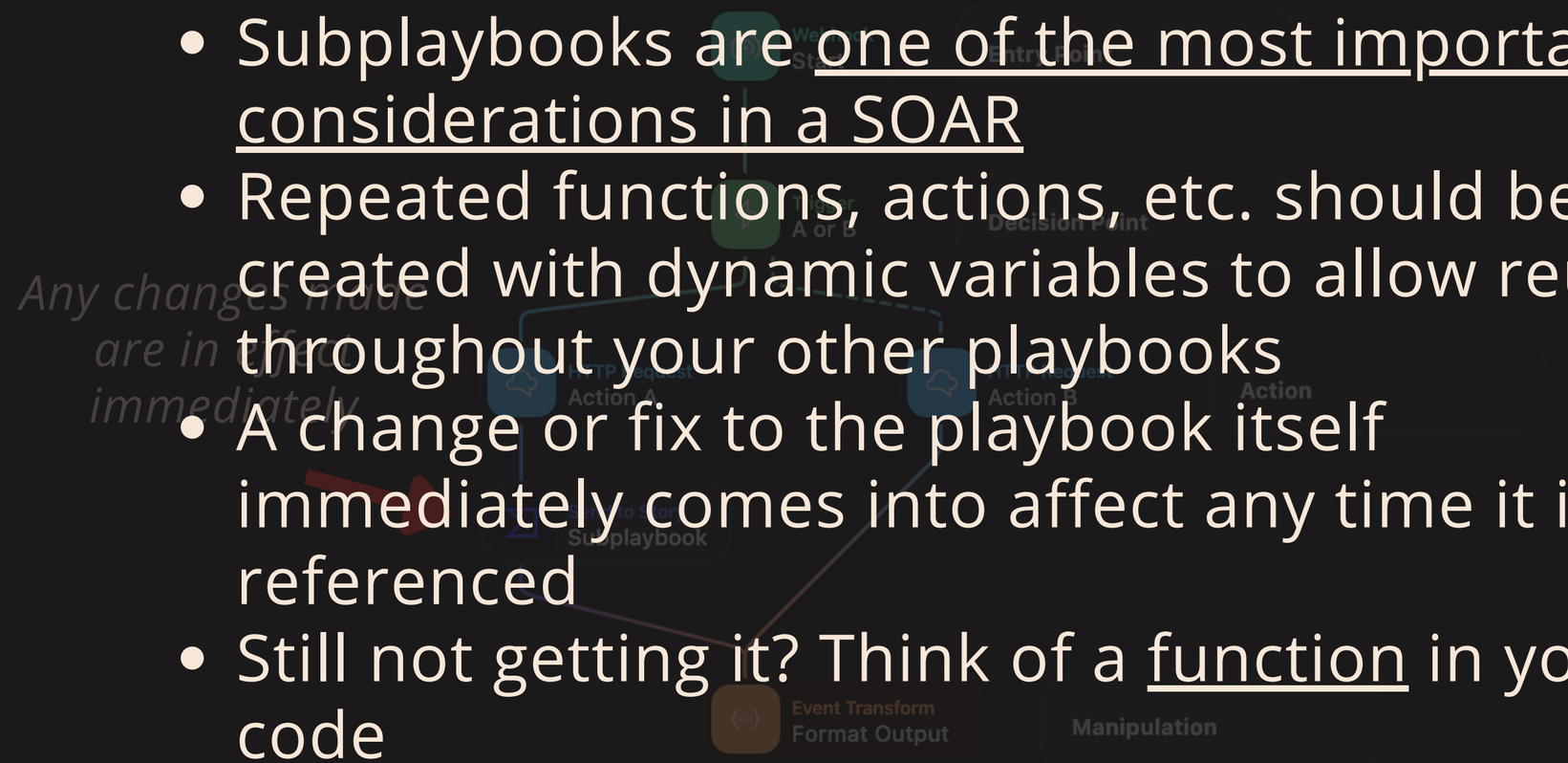
Any changes made are in effect immediately

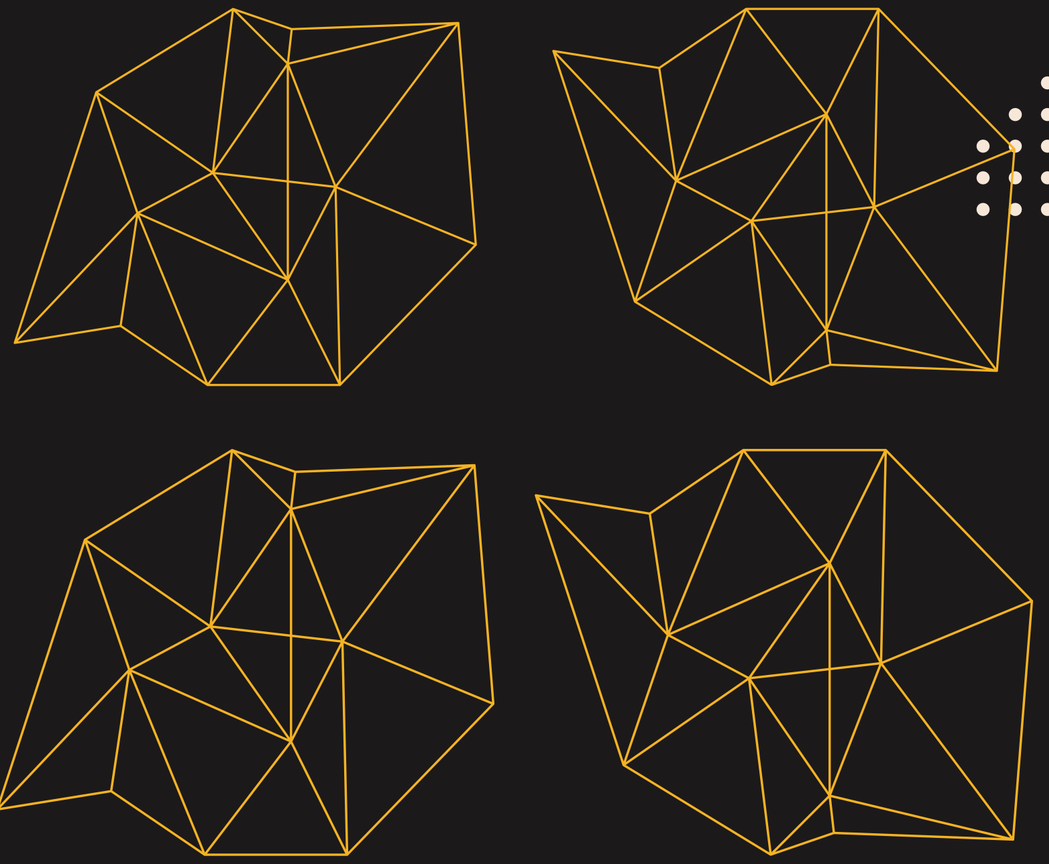


SUB-PLAYBOOKS

A PLAYBOOK MEANT TO BE USED BY OTHERS (A FUNCTION)

- Subplaybooks are one of the most important considerations in a SOAR
- Repeated functions, actions, etc. should be created with dynamic variables to allow reuse throughout your other playbooks
- A change or fix to the playbook itself immediately comes into affect any time it is referenced
- Still not getting it? Think of a function in your code





PLAYBOOK USE CASE

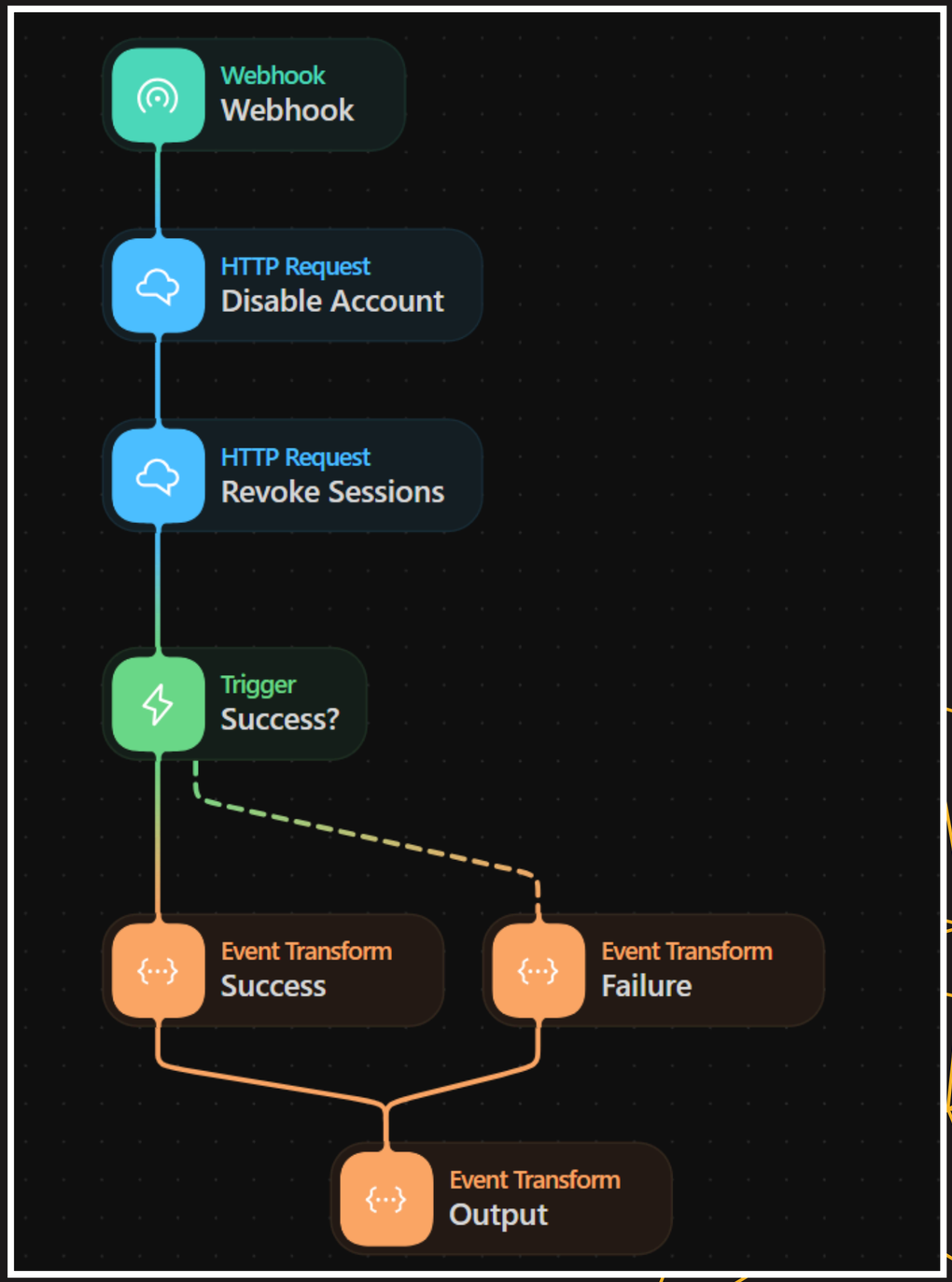
SUSPICIOUS LOGIN REMEDIATION

I USE CASE

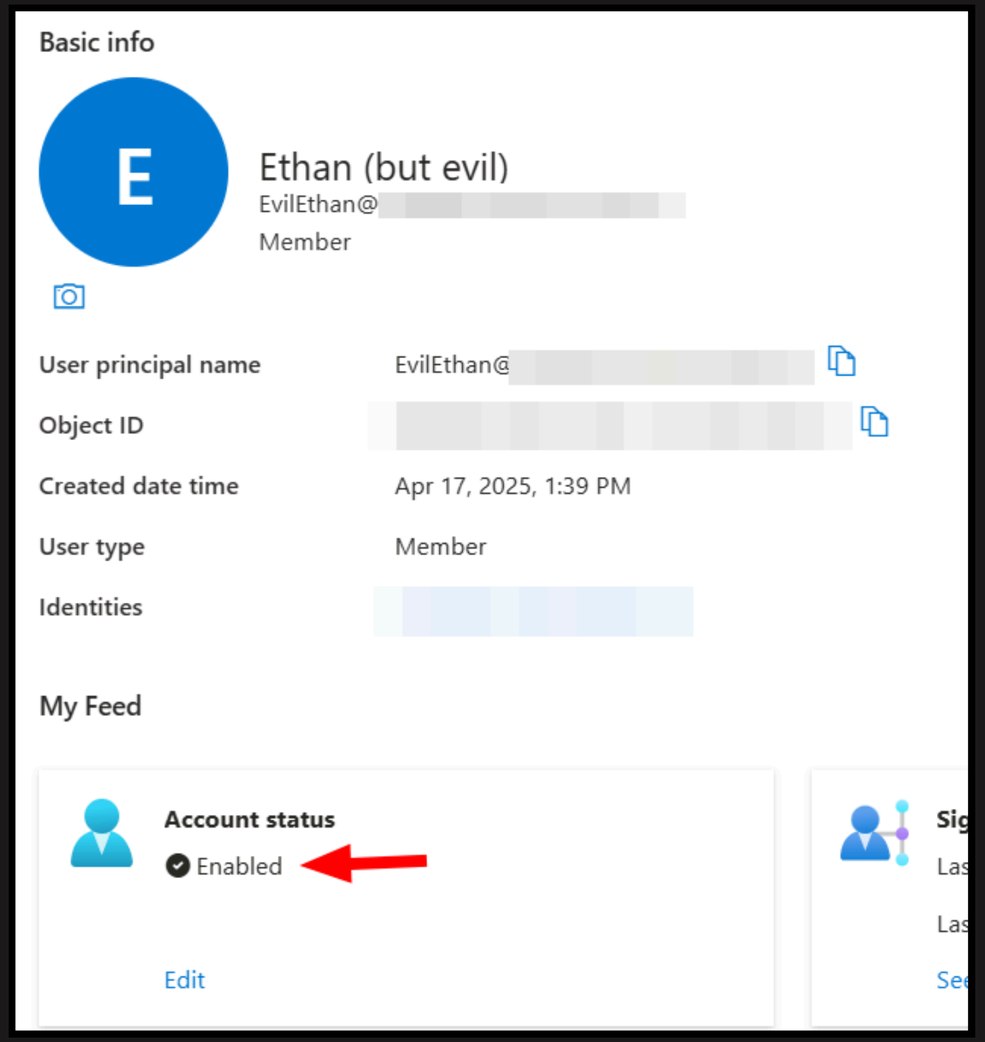
- This would be a *sub-playbook*, fed into by one a cloud triage playbook
- If a cloud detection is a true postitive, could allow immediate reset of a user account

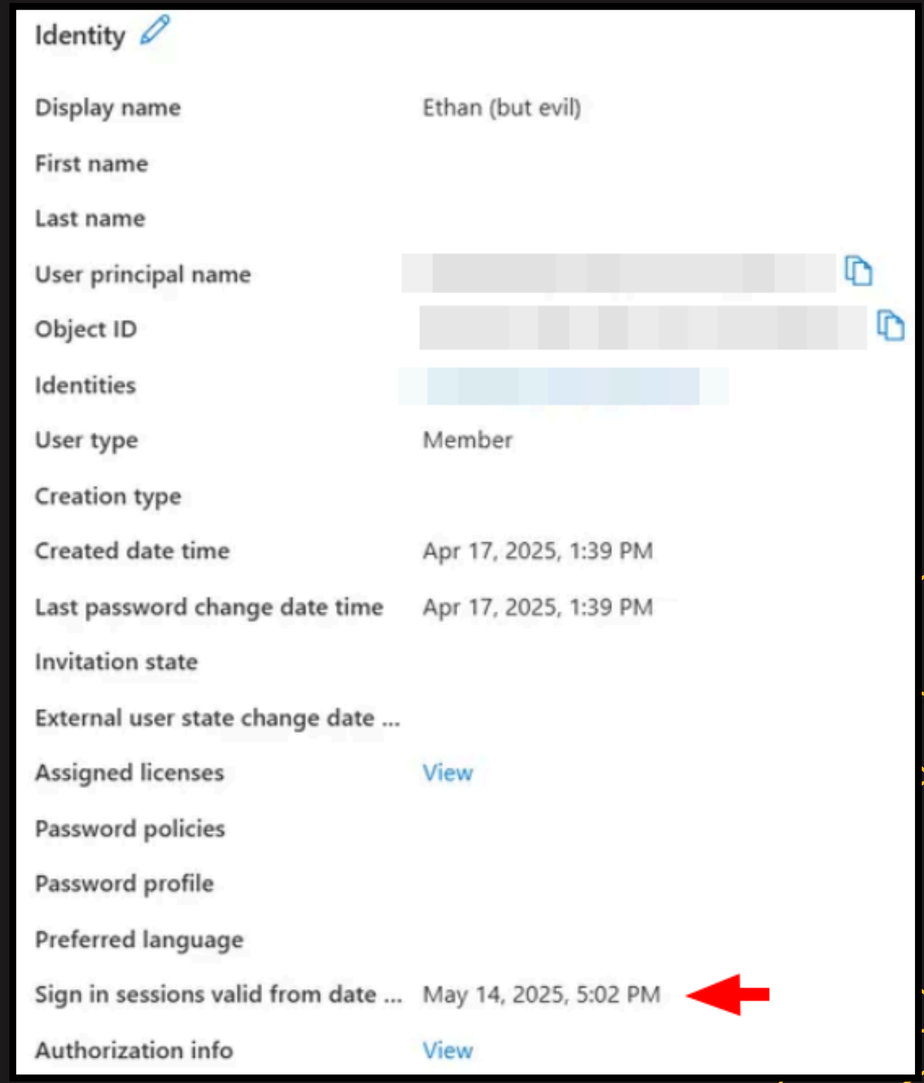
I PLAYBOOK

- Receives input of a user principal
- Straightforward and simple, emphasizes speed and efficiency (and even automation potential)
- Playbook outputs the result and success or failure for handling by the parent playbook calling it

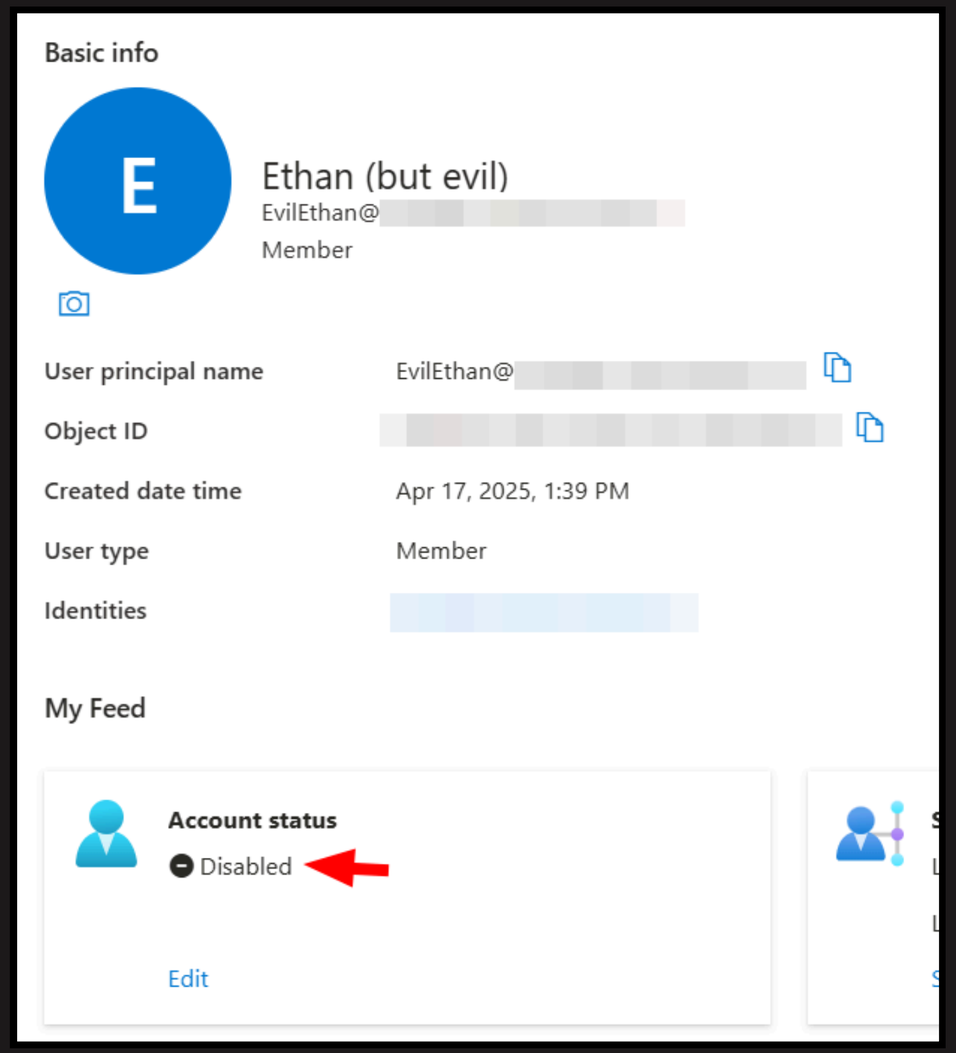


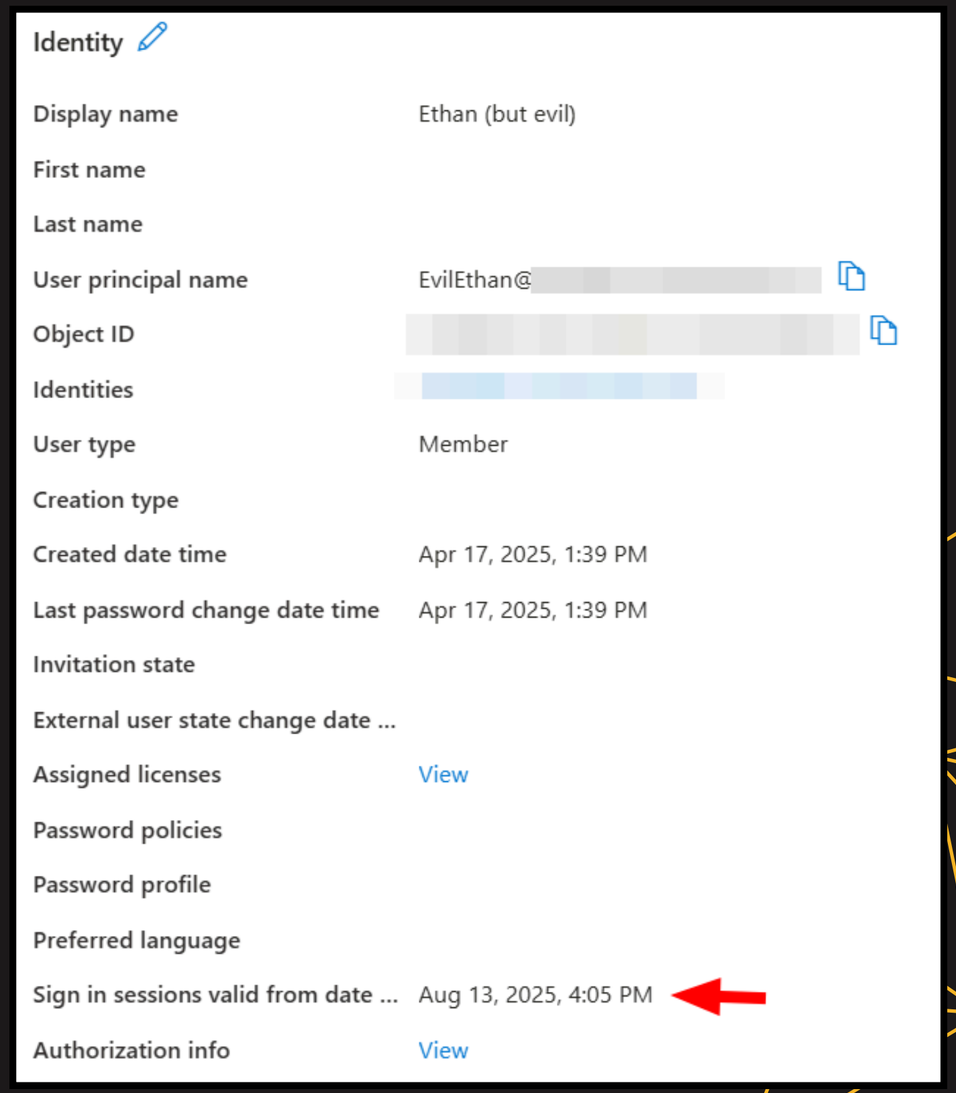
I BEFORE

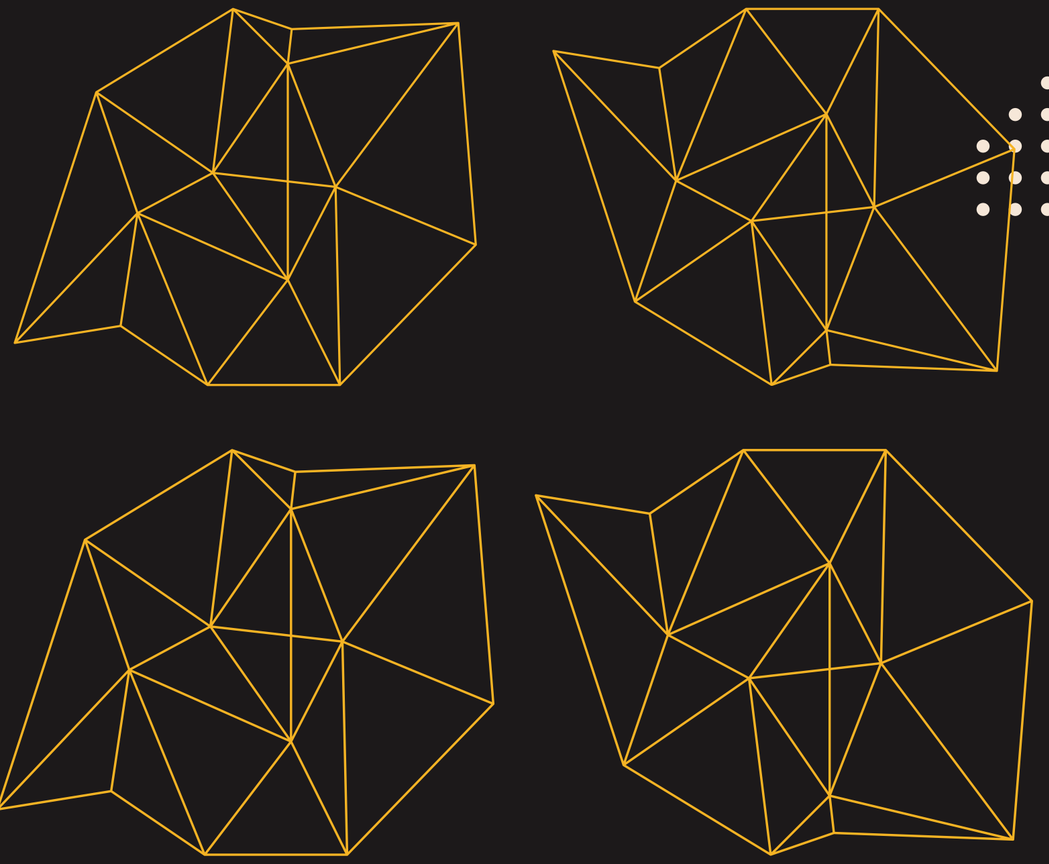

Basic info
E
Ethan (but evil)
EvilEthan@
Member
User principal name
EvilEthan@
Object ID
Created date time
Apr 17, 2025, 1:39 PM
User type
Member
Identities
My Feed
Account status
Enabled
Edit


Identity
Display name
Ethan (but evil)
First name
Last name
User principal name
Object ID
Identities
User type
Member
Creation type
Created date time
Apr 17, 2025, 1:39 PM
Last password change date time
Apr 17, 2025, 1:39 PM
Invitation state
External user state change date ...
Assigned licenses
View
Password policies
Password profile
Preferred language
Sign in sessions valid from date ...
May 14, 2025, 5:02 PM
Authorization info
View

I AFTER


Basic info
E
Ethan (but evil)
EvilEthan@
Member
User principal name
EvilEthan@
Object ID
Created date time
Apr 17, 2025, 1:39 PM
User type
Member
Identities
My Feed
Account status
Disabled
Edit


Identity
Display name
Ethan (but evil)
First name
Last name
User principal name
EvilEthan@
Object ID
Identities
User type
Member
Creation type
Created date time
Apr 17, 2025, 1:39 PM
Last password change date time
Apr 17, 2025, 1:39 PM
Invitation state
External user state change date ...
Assigned licenses
View
Password policies
Password profile
Preferred language
Sign in sessions valid from date ...
Aug 13, 2025, 4:05 PM
Authorization info
View



PLAYBOOK USE CASE

PHISHING EMAIL INVESTIGATION

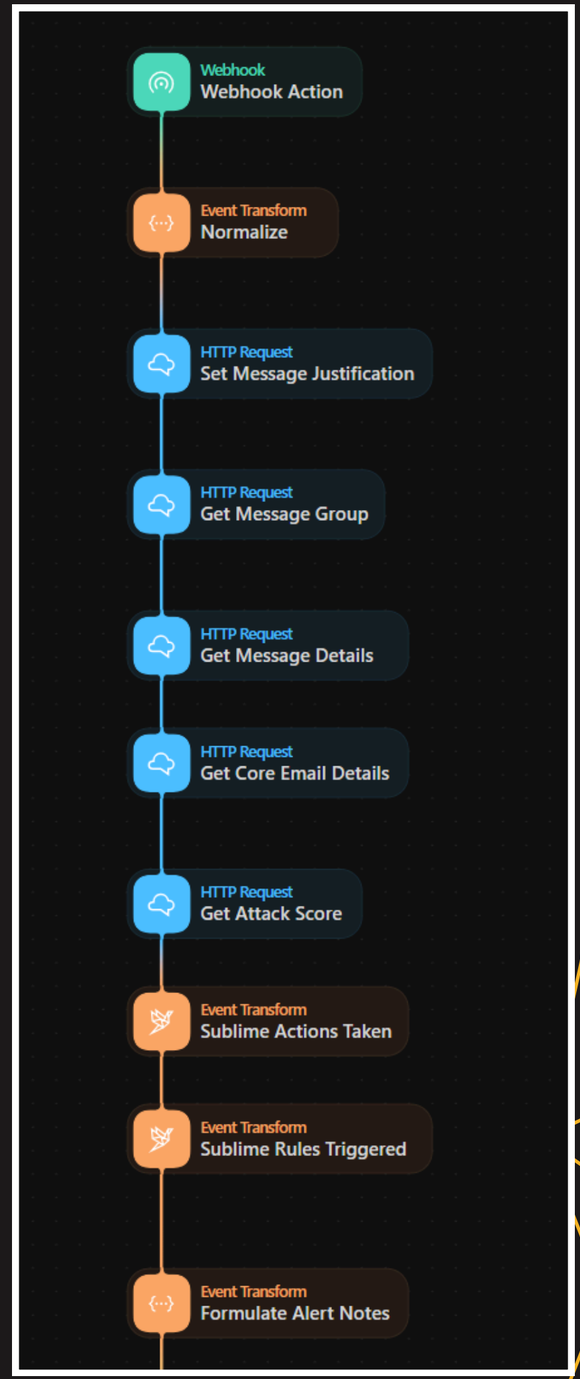
I USE CASE

- Receive alerts via email security tool
- Collect data from those alerts
- Logically assess all data, and determine flow
- Either classify automatically, or create a Case
- Respond to cases without leaving the SOAR

This is an abbreviated version of our playbook

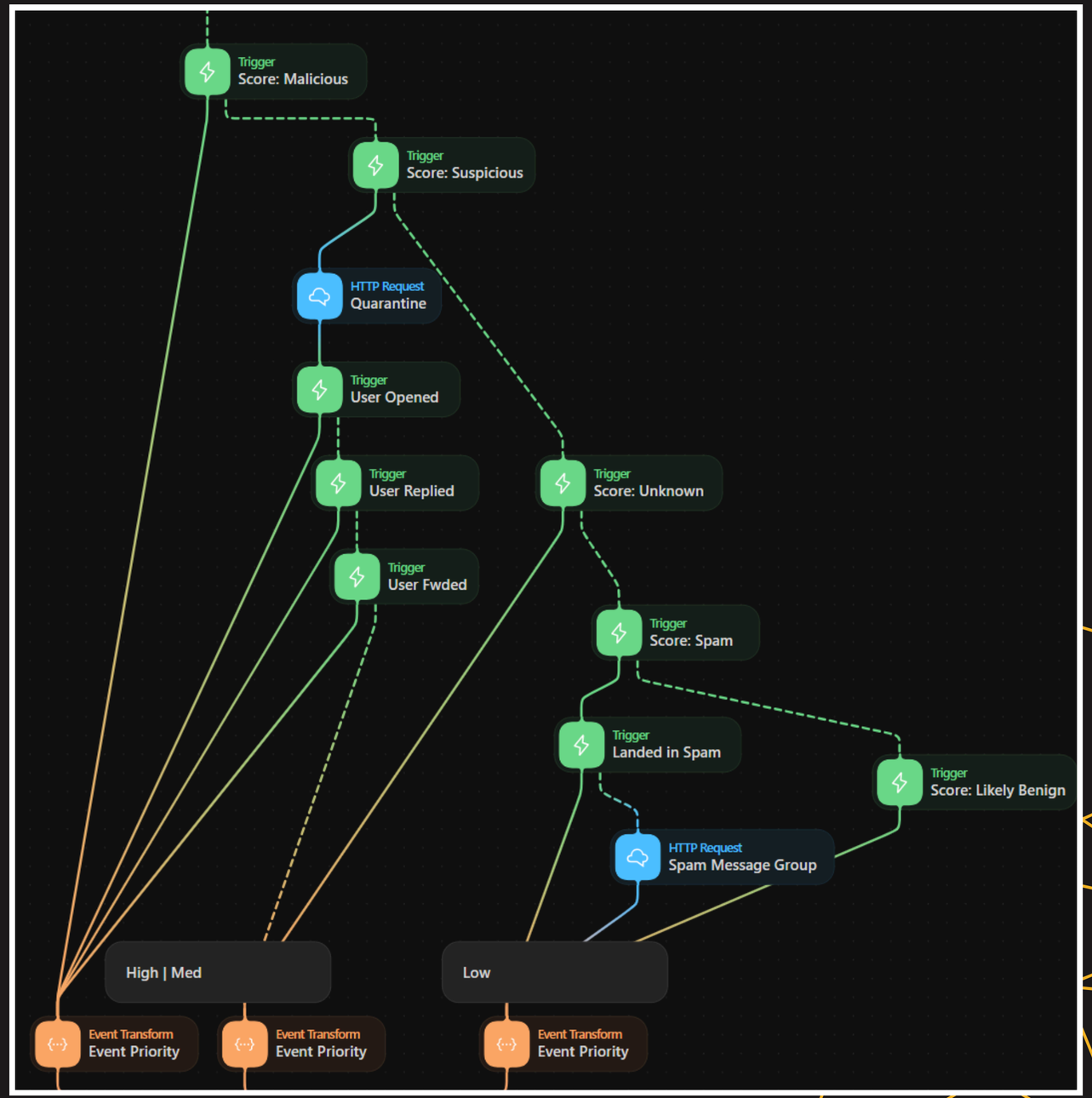
I ENTRY POINT

- Receives alerts
- Normalizes and matches key pieces of data
- Performs a number of API calls to email tool
- Formats data on rules & actions already performed, then starts formulating the alert details



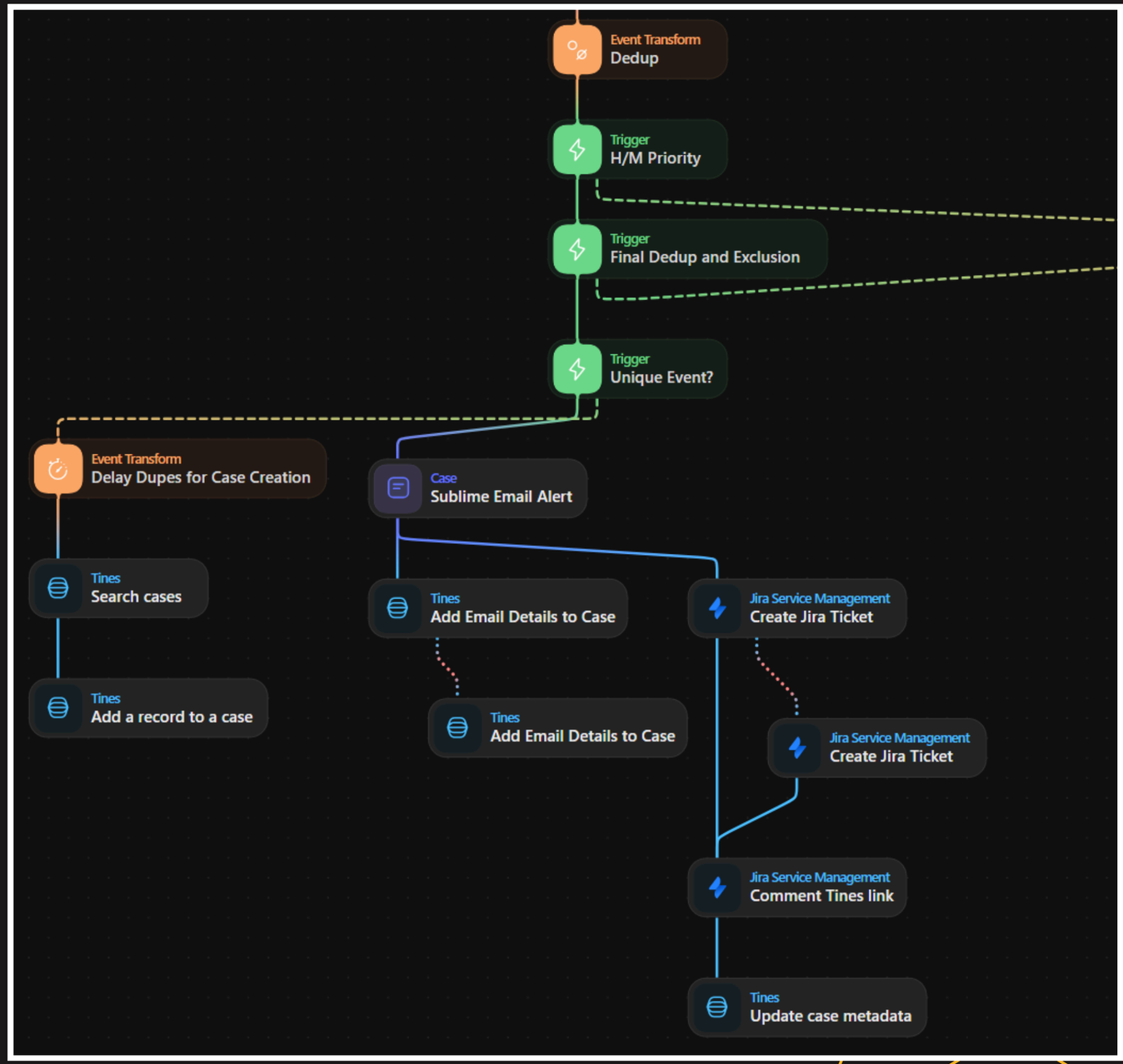
I PRIORITY

- Based on email severity score, and additional details, determine alert severity
- Note how can give higher priority to suspicious emails that have had interaction

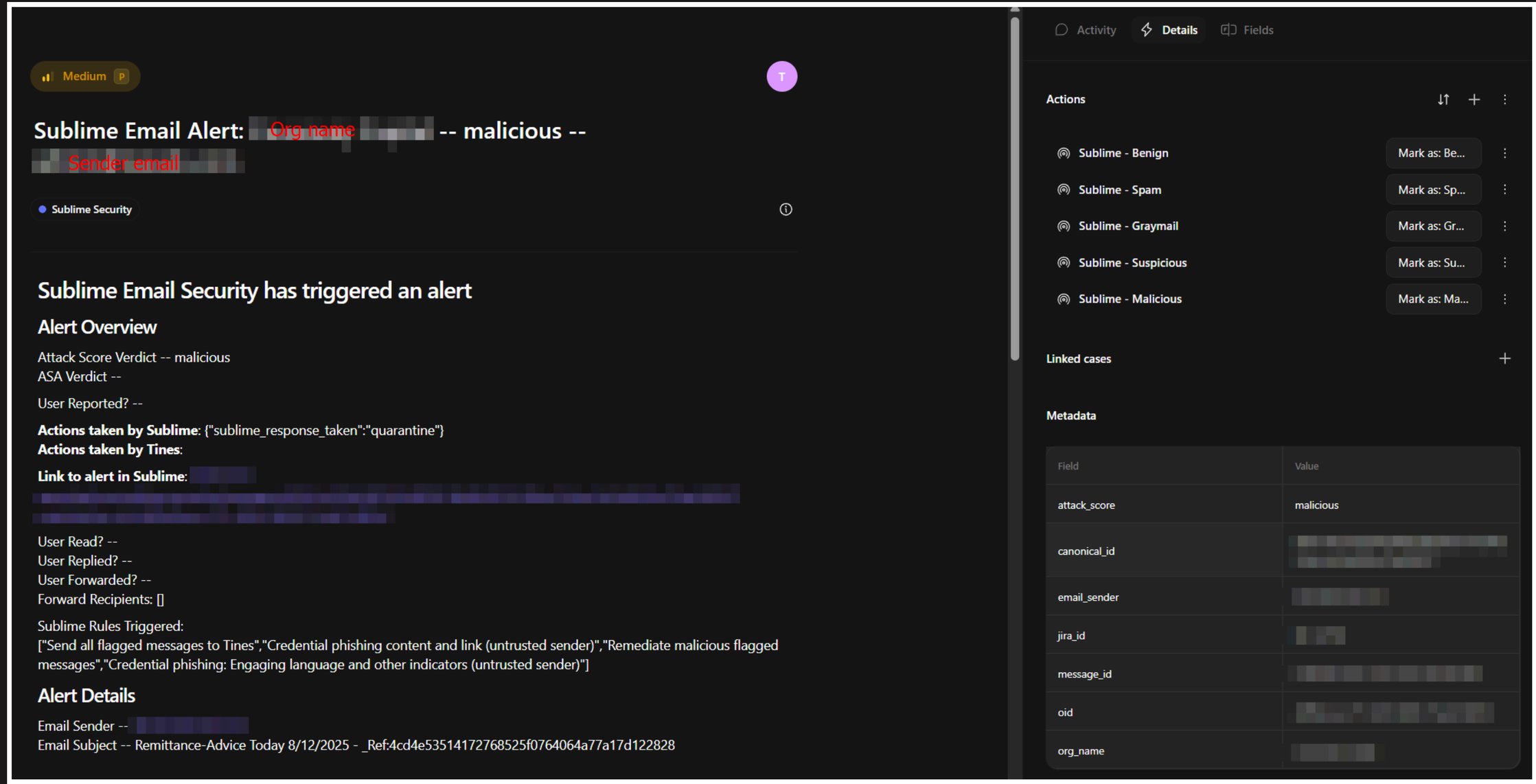


I CASES

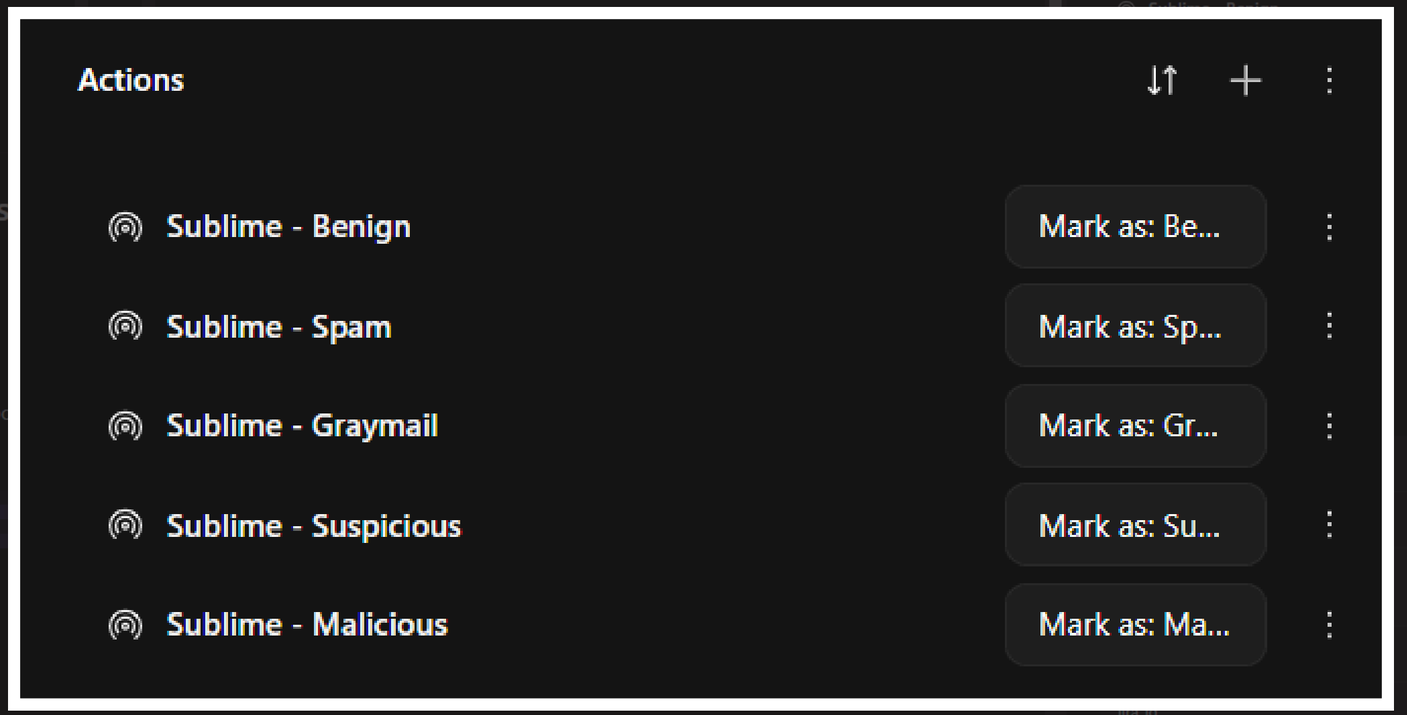
- Deduplicate
- Based on classifications, determine what severity of Case and/or ticket to create
- (Over on the right, Low priority events are handled)



I CASES

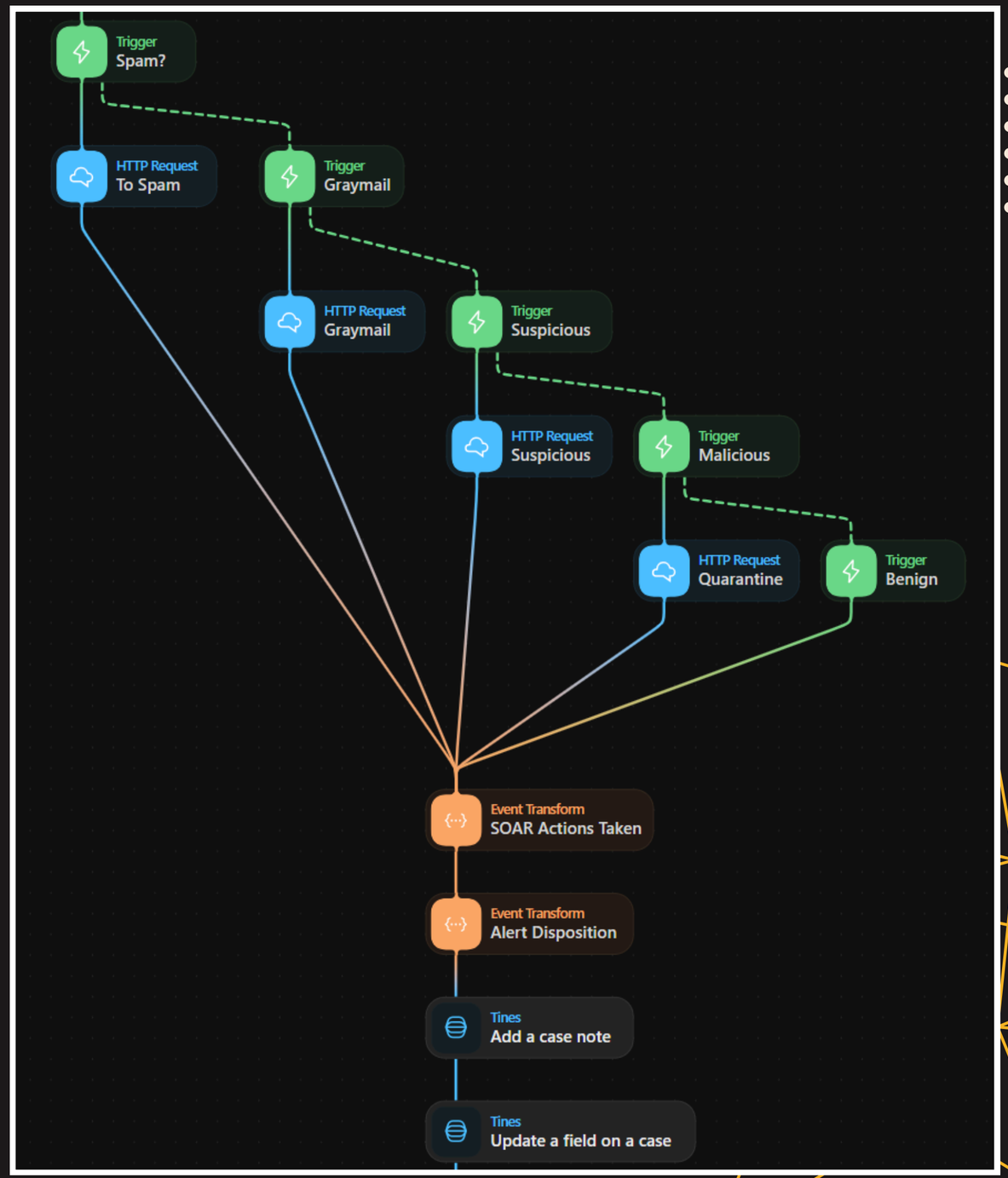

Medium P
T
Sublime Email Alert: Org name -- malicious --
Sender email
Sublime Security
Sublime Email Security has triggered an alert
Alert Overview
Attack Score Verdict -- malicious
ASA Verdict --
User Reported? --
Actions taken by Sublime: {"sublime_response_taken":"quarantine"}
Actions taken by Tines:
Link to alert in Sublime:
User Read? --
User Replied? --
User Forwarded? --
Forward Recipients: []
Sublime Rules Triggered:
["Send all flagged messages to Tines","Credential phishing content and link (untrusted sender)","Remediate malicious flagged messages","Credential phishing: Engaging language and other indicators (untrusted sender)"]
Alert Details
Email Sender --
Email Subject -- Remittance-Advice Today 8/12/2025 - _Ref:4cd4e53514172768525f0764064a77a17d122828
Activity
Details
Fields
Actions
Sublime - Benign
Mark as: Be...
Sublime - Spam
Mark as: Sp...
Sublime - Graymail
Mark as: Gr...
Sublime - Suspicious
Mark as: Su...
Sublime - Malicious
Mark as: Ma...
Linked cases
Metadata
Field
Value
attack_score
malicious
canonical_id
email_sender
jira_id
message_id
oid
org_name

I CASES (ACTIONS)



I RESPONSE

- Allows classification without leaving the SOAR
- Ensures response actions are taken
- Our full playbook has additional verifications based on status
  - i.e. If Benign, but was quarantined, release email from quarantine
- Closes all SOAR & Jira cases associated, fills all necessary fields



HOW TO IMPLEMENT A SOAR RIGHT

IMPLEMENTATION & PITFALLS

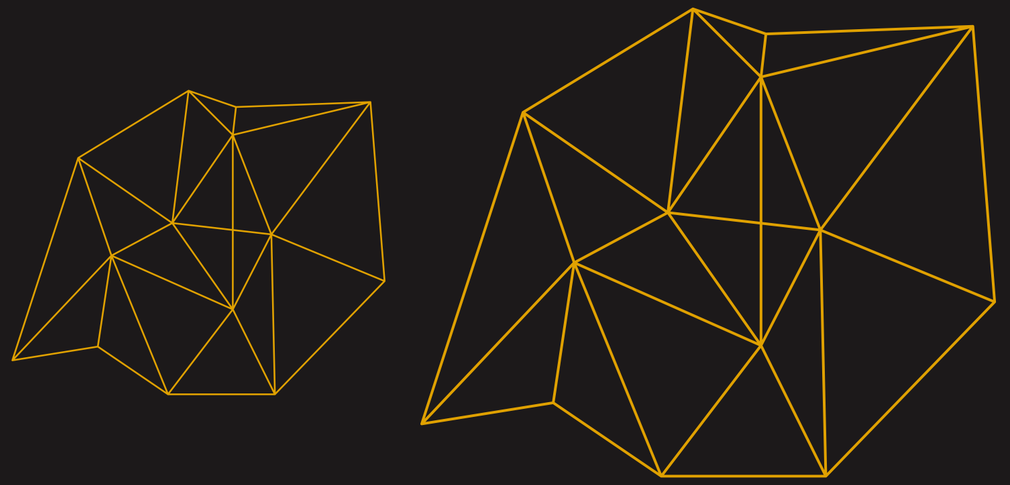
IMPLEMENTATION & PITFALLS

- Lack of direction and advance planning
- Not utilizing subplaybooks
- Making your playbooks too static
- Lack of end user input
- Not using it to the maximum
- “MVP”

FUTURE TRENDS

EVEN SOAR IS RAPIDLY EVOLVING

- ARTIFICIAL INTELLIGENCE
- AGENTIC AI



I ARTIFICIAL INTELLIGENCE

> Updated at 2025-08-06T17:54:52 .946+00:00

> The following is AI generated.

Malicious Behavior Summary

The host ' hostname ' has exhibited concerning behavior, including successful non-RFC1918 authentication and the execution of a known network scanning tool. These activities suggest an attacker may be attempting to gain unauthorized access and gather information about the network.

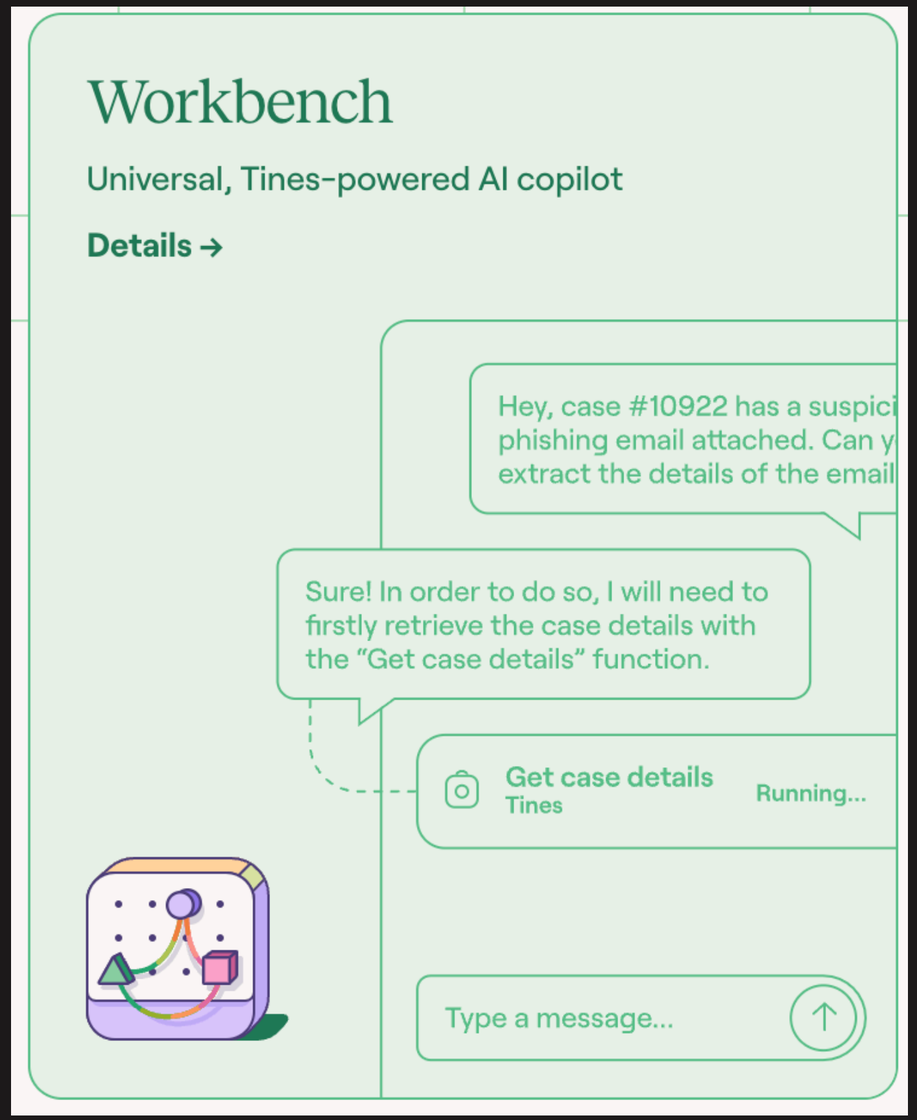
Benign Explanation

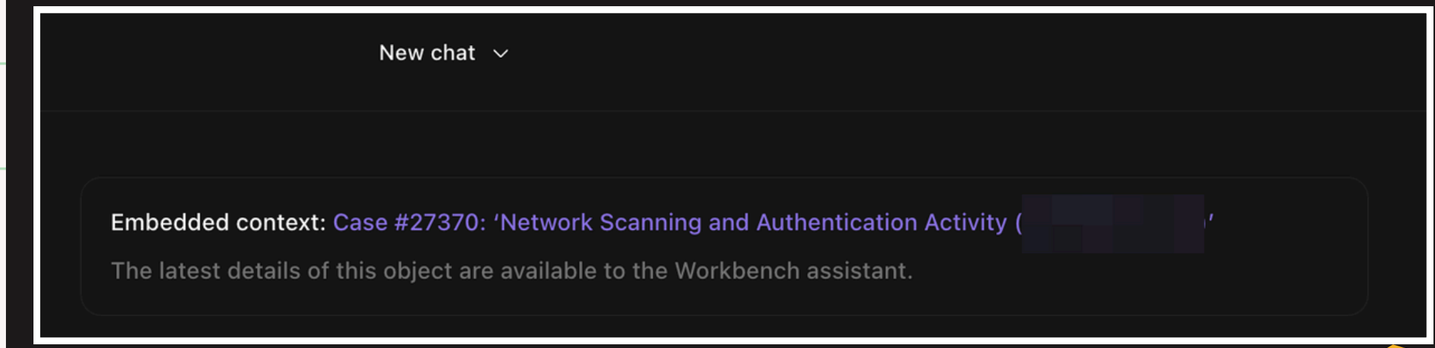
The non-RFC1918 authentication could potentially be legitimate if the user user ' is a remote administrator who needs to access the system from an external network. The scanner process could also be benign if it is being used by a legitimate network administrator for authorized purposes. To confirm this, we should check if ' user ' is a known admin account, and whether the scanner usage is documented and approved.

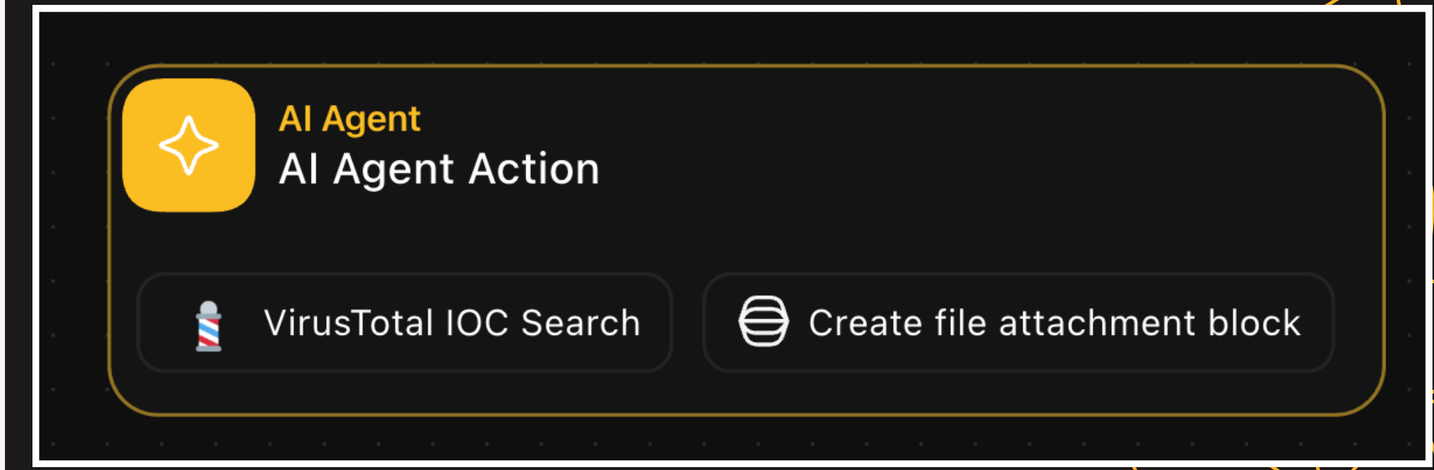
Recommendations

- Verify the identity and authorization of the ' user ' user account
- Determine if the use of scanner is approved and documented
- Review other recent activity on the ' host ' host to identify any other suspicious behavior
- Investigate the source of the non-RFC1918 authentication attempt to assess the risk
- Consider implementing additional security controls to restrict remote access and network scanning

I AGENTIC AI


Workbench
Universal, Tines-powered AI copilot
Details →
Hey, case #10922 has a suspici
phishing email attached. Can y
extract the details of the email
Sure! In order to do so, I will need to firstly retrieve the case details with the "Get case details" function.
Get case details
Tines
Running...
Type a message...


New chat
Embedded context: Case #27370: 'Network Scanning and Authentication Activity (
The latest details of this object are available to the Workbench assistant.


AI Agent
AI Agent Action
VirusTotal IOC Search
Create file attachment block

QUESTIONS?

Twitter: @KilobyteTheDust

LinkedIn: Hayden Covington