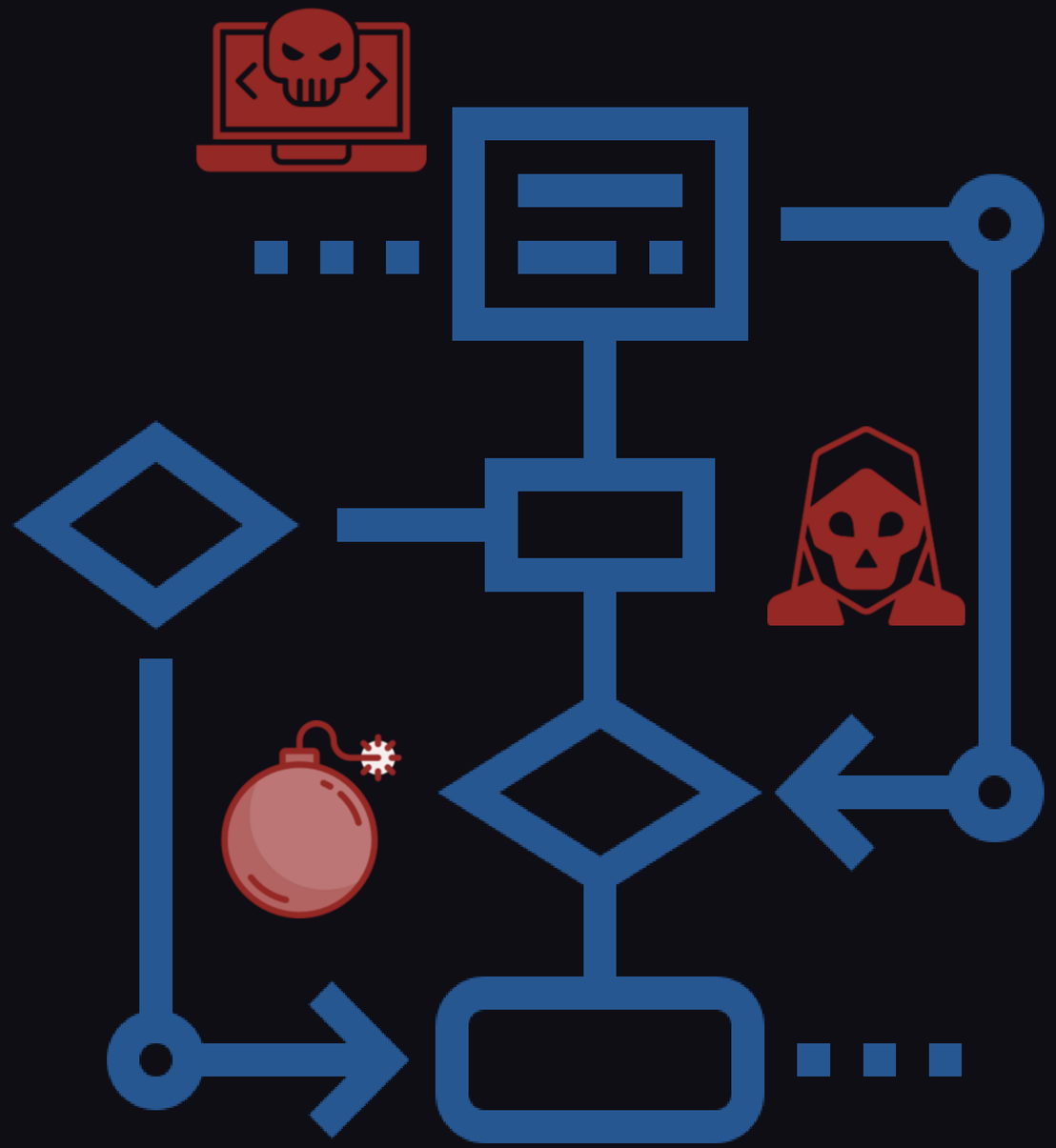
Flowcharts of doom: Mapping adversary behaviour like a threat artist

Jayant (Jay) Kripalani



Agenda

Intro	Attack Flow in action
Before we begin	Attack Flow Components
Problem	Impact Statement
Solution	Outro

About me

- Senior Security Solution Architect – APAC, Splunk a Cisco Company
- Previously worked at – Cisco, Rapid7, McAfee
- Current Specialisation – Threat Detection / Hunting / Intelligence, Security Automation, Machine Learning
- Previous experience – Network Security, Blue Teaming, Malware Engineering
- 20+ years of experience in Security
- Certifications – ISC2, Splunk, Cisco, EC-Council, ISO, etc.
- Publications – IEEE, TechRepublic, Enterprise Executive, US Cybersecurity Magazine, Australian Security Magazine
- Speaking – AISA CyberCon Melbourne & Canberra, CISO Summit, Splunk .confGo, Cisco Live
- Connect with me – share ideas, collaborate on ongoing projects/research, co-authoring opportunities, technical projects

About the project

Problem

Defenders often track adversary behaviours atomically, focusing on one specific action at a time. This makes it harder to understand adversary attacks and to build effective defences against those attacks

Example - Cryptojacking

Tesla cloud systems exploited by hackers to mine cryptocurrency

Updated: Researchers have discovered that Tesla's AWS cloud systems were compromised for the purpose of cryptojacking.

Written by **Charlie Osborne,** Contributing Writer

Feb. 20, 2018 at 6:00 a.m. PT

Tesla

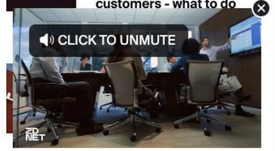
Tesla's cloud environment has been exploited by threat actors to mine cryptocurrencies, researchers have discovered.

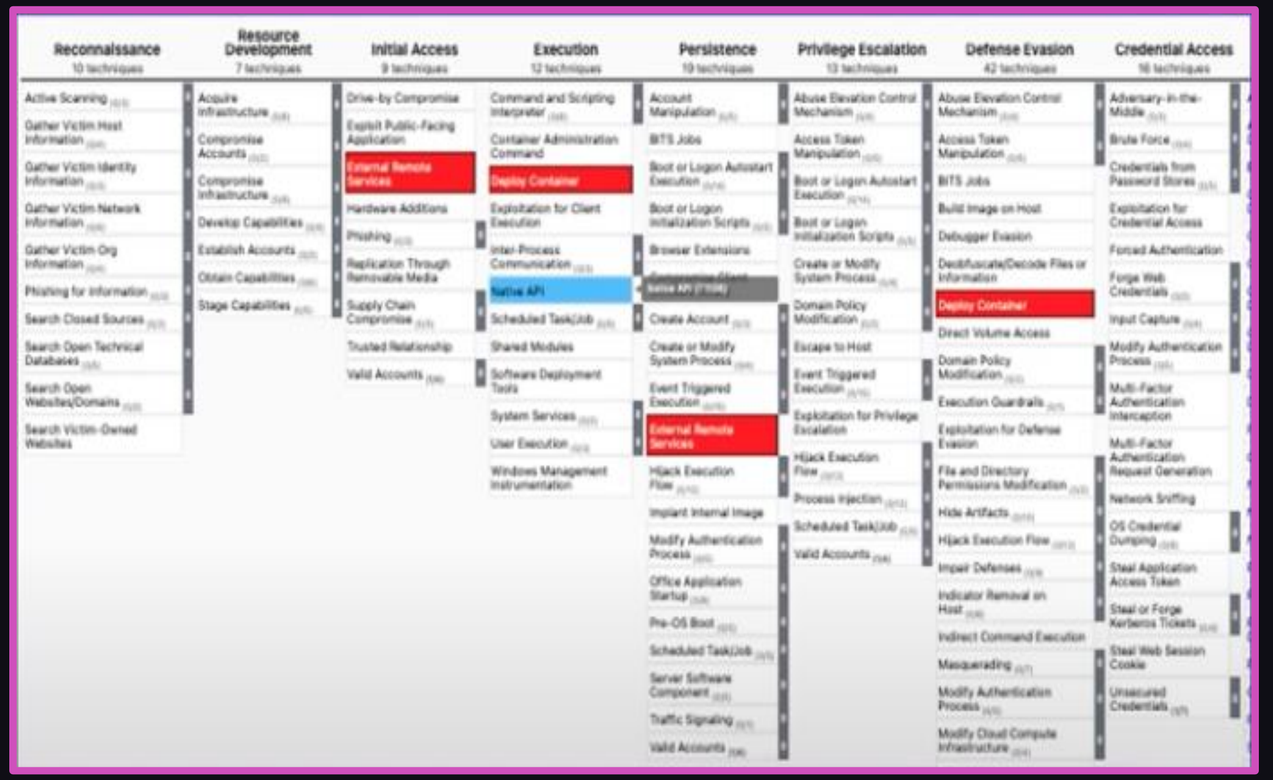
On Tuesday, cloud security firm RedLock released the firm's 2018 Cloud Security Trends report which

/ security

/ related

Massive TransUnion breach leaks personal data of 4.4 million customers - what to do





Atomic attacks & mitigation

```
`sysmon` EventCode=10 TargetImage=*lsass.exe (GrantedAccess=0x1010 OR GrantedAccess=0x1410)
| stats count min(_time) as firstTime max(_time) as lastTime by CallTrace EventID GrantedAccess Guid
Opcode ProcessID SecurityID SourceImage SourceProcessGUID SourceProcessId TargetImage TargetProcessGUID
TargetProcessId UserID dest granted_access parent_process_exec parent_process_guid parent_process_id
parent_process_name parent_process_path process_exec process_guid process_id process_name process_path
signature signature_id user_id vendor_product
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `detect_credential_dumping_through_lsass_access_filter`
```


```
index=windows OR index=wineventlog  sourcetype=wineventlog
|dedup EventCode
|rex field=EventCodeDescription (?<account_desc>account)
|where EventCodeDescription NOT null AND account_desc NOT null
|table _time dest_nt_domain dest_nt_host src_user EventCode
EventCodeDescription
|rename dest_nt_domain AS Domain dest_nt_host AS Host src_user AS User
```

Realism – Why Attack Flows are important

A single block **IS NOT** a stopped attack

Attackers persist and try to find other avenues of attack

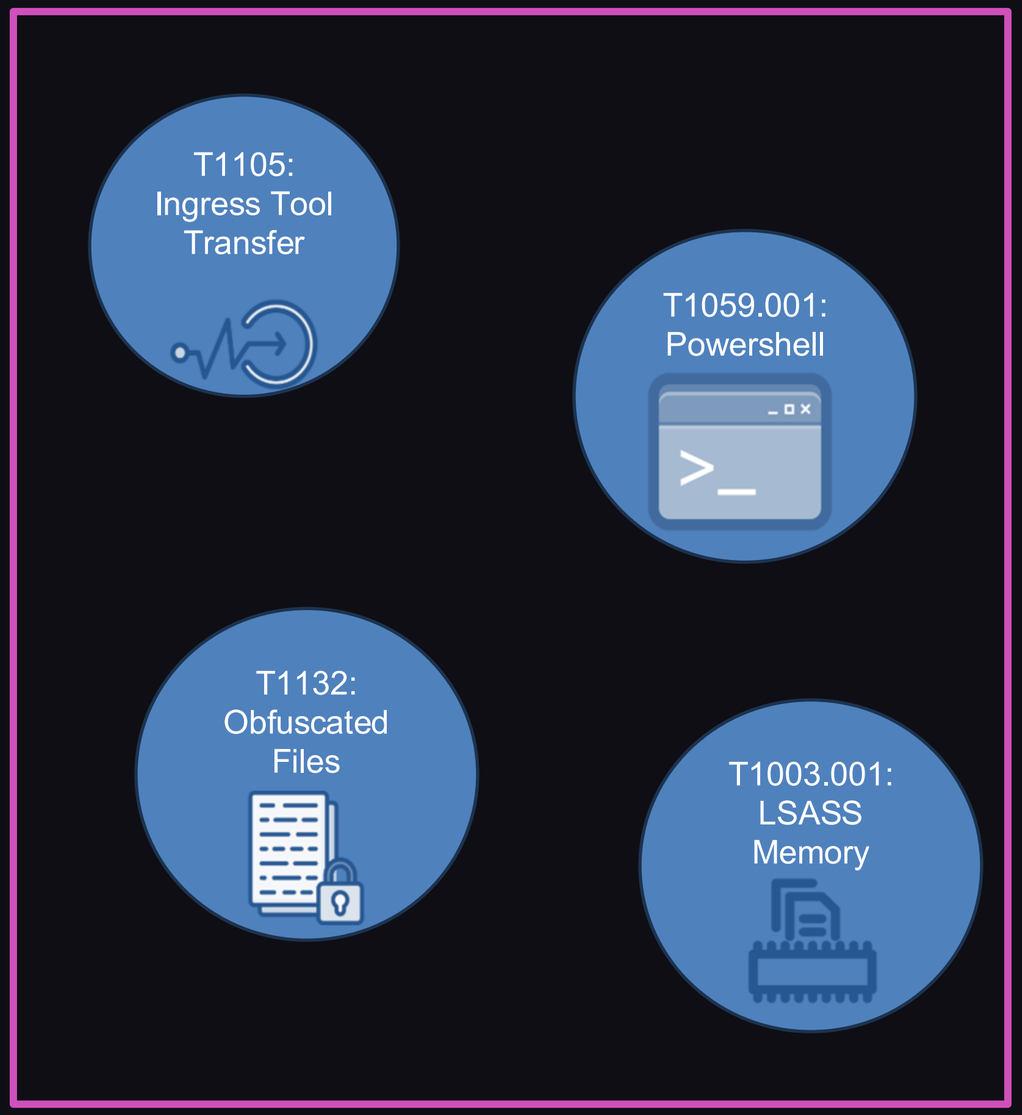
Alert Fatigue

Too many alerts = alert fatigue

Too many alerts = too much information to parse through

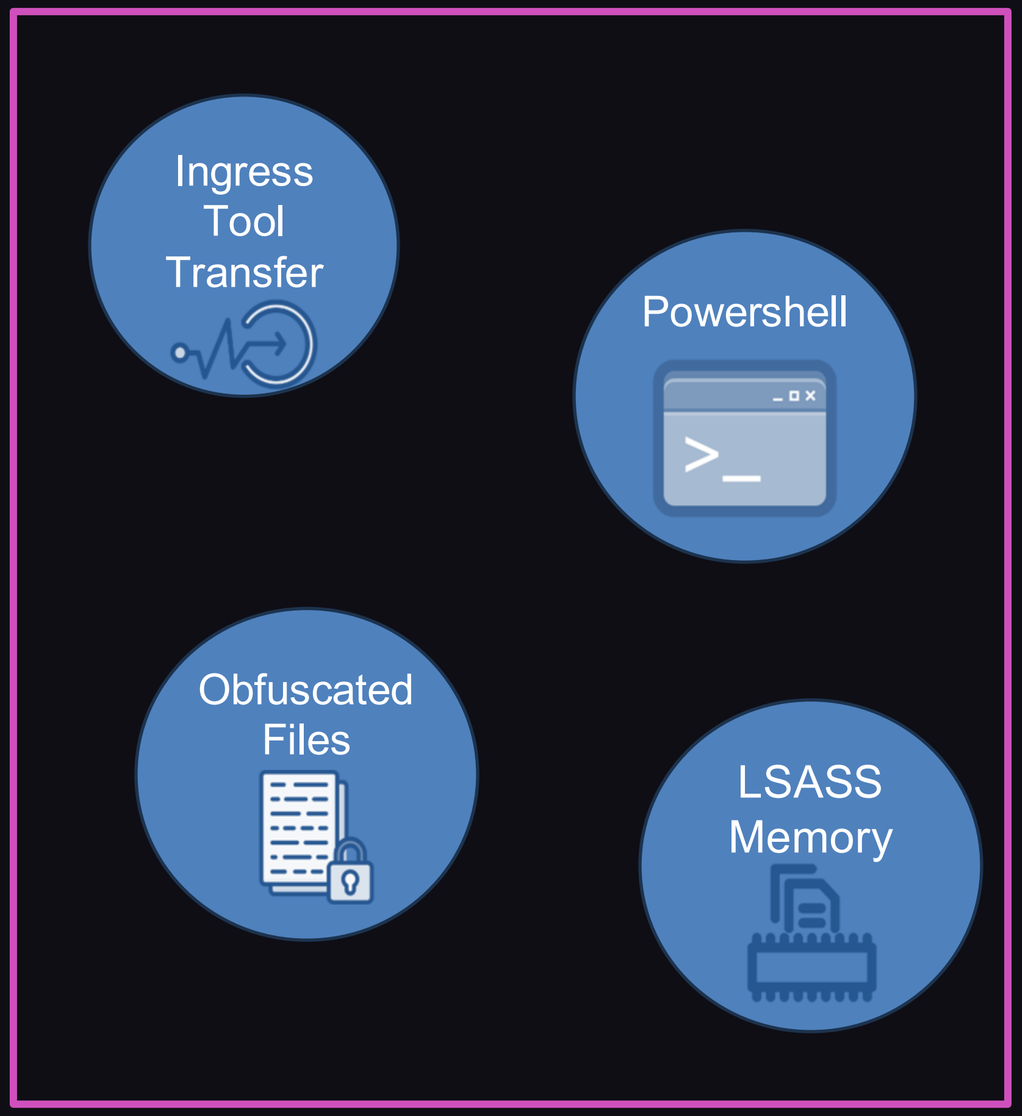
Alert fatigue = relevant information gets ignored

Describing/Mapping adversary behaviour

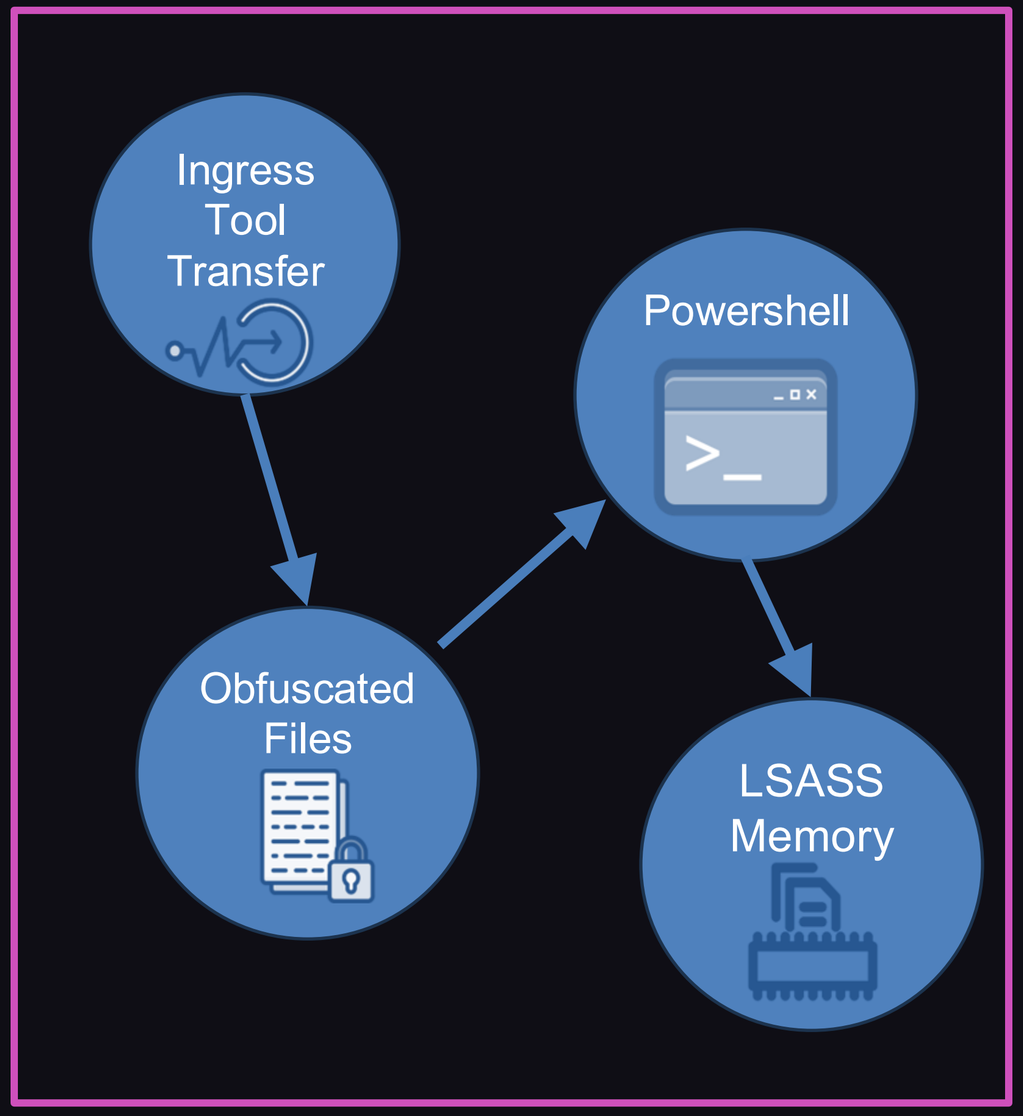


Atomic Behaviours

Describing/Mapping adversary behaviour



Atomic Behaviours



Sequenced Behaviours

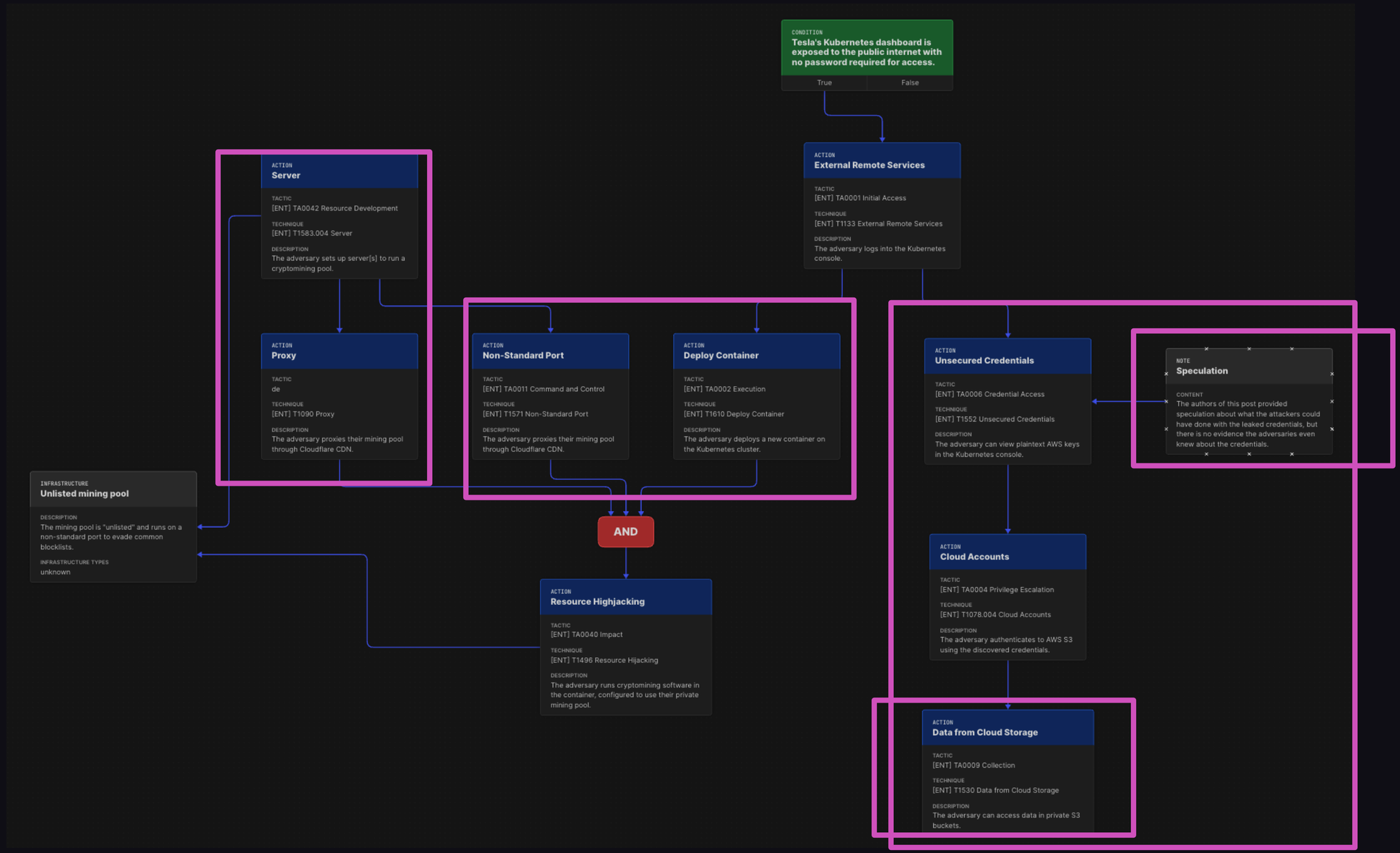
Solution

Create a language, and associated tooling, to describe flows of ATT&CK techniques and combine those flows into patterns of behaviour.

Attack Flow

What it is?

Attack Flow – Tesla Kubernetes Breach

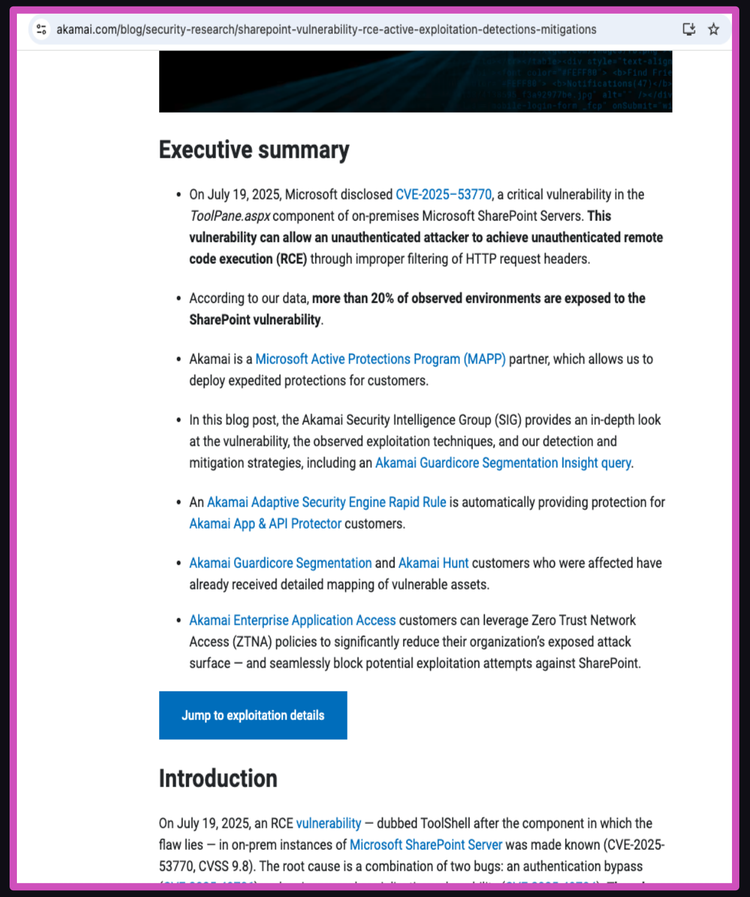


Approach to Flow Building

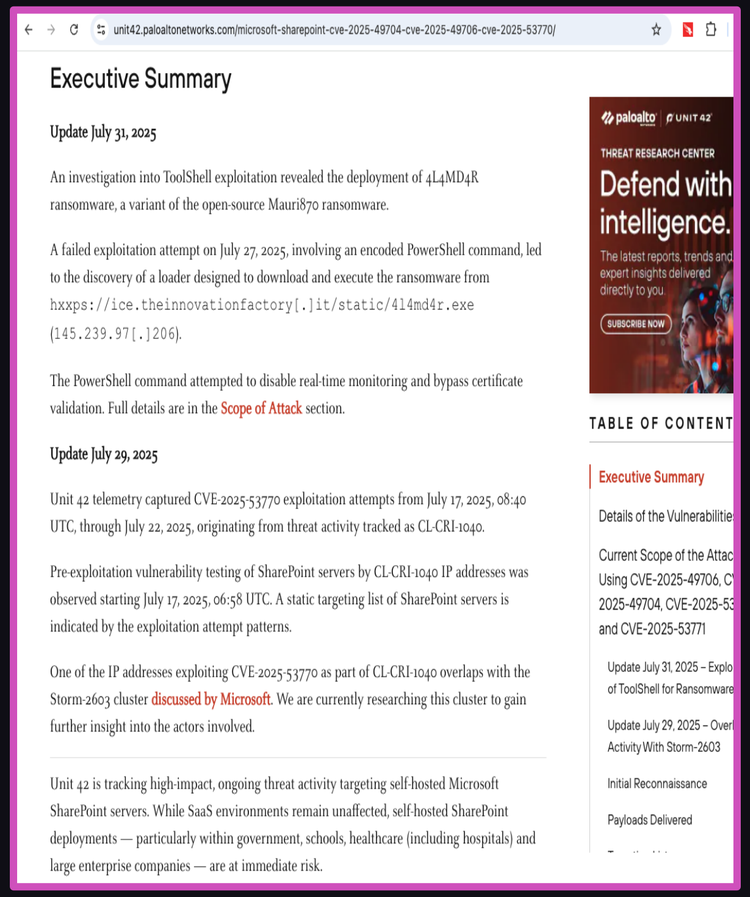
1. Find appropriate CTI reporting.
2. Annotate the report with TTPs.
3. Create the actions in the flow based on the TTPs.
4. Add additional items for context: IOCs, Assets, etc.

Using Attack Flow for CTI

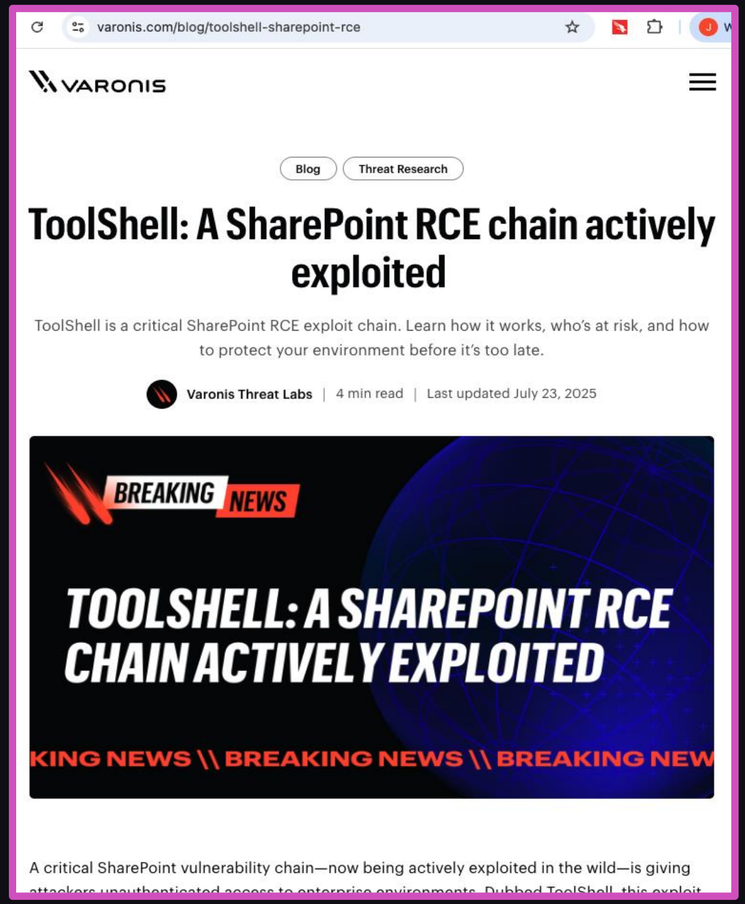
Explaining the ToolShell Vulnerability (Timeline: July 2025) using Attack Flow



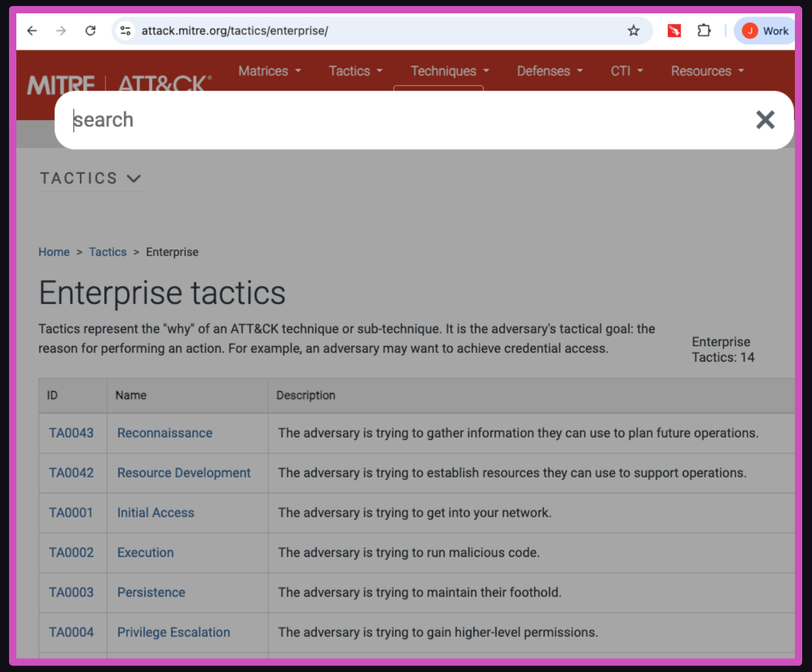
akamai.com/blog/security-research/..

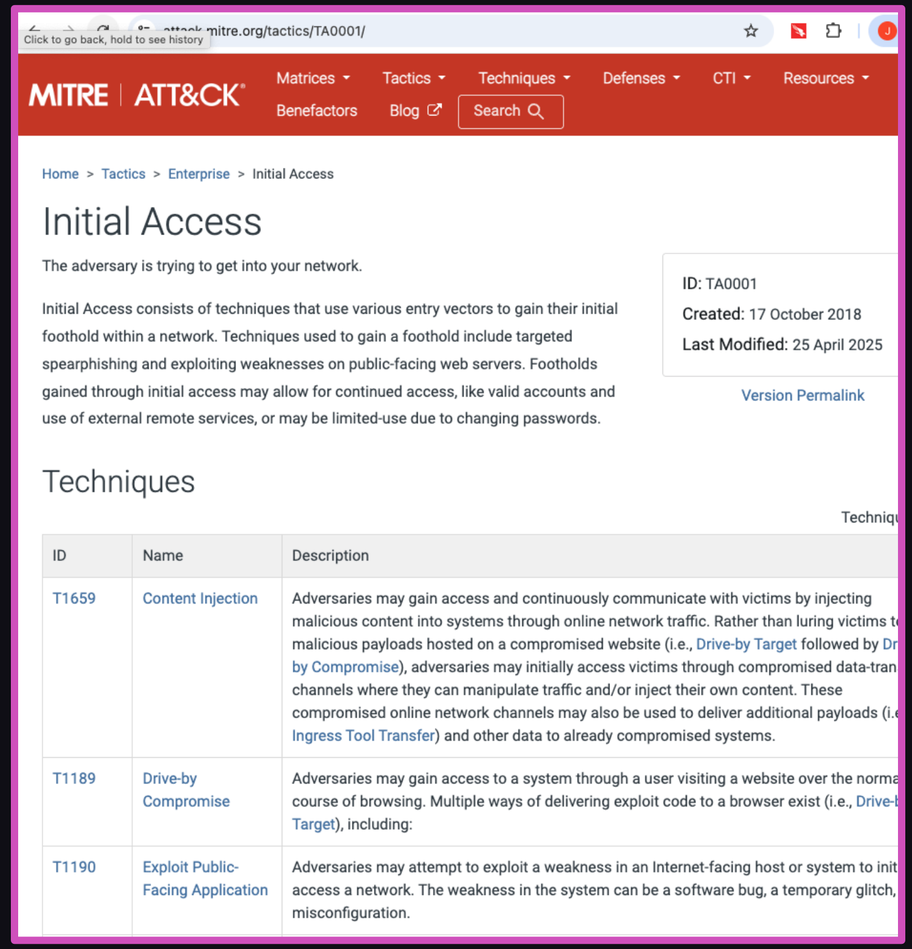


unit42.paloaltonetworks.com/..



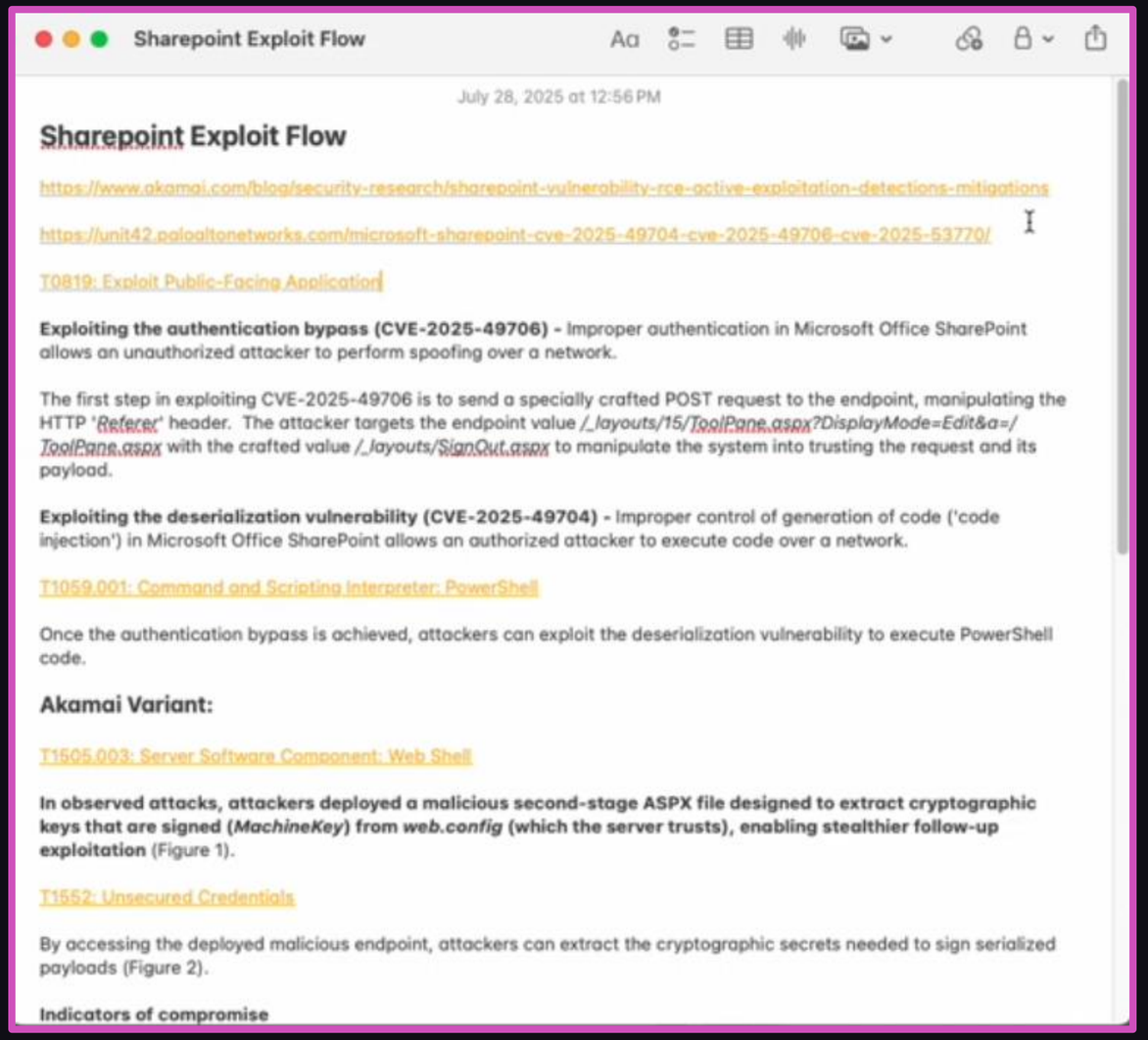
varonis.com/blog/..

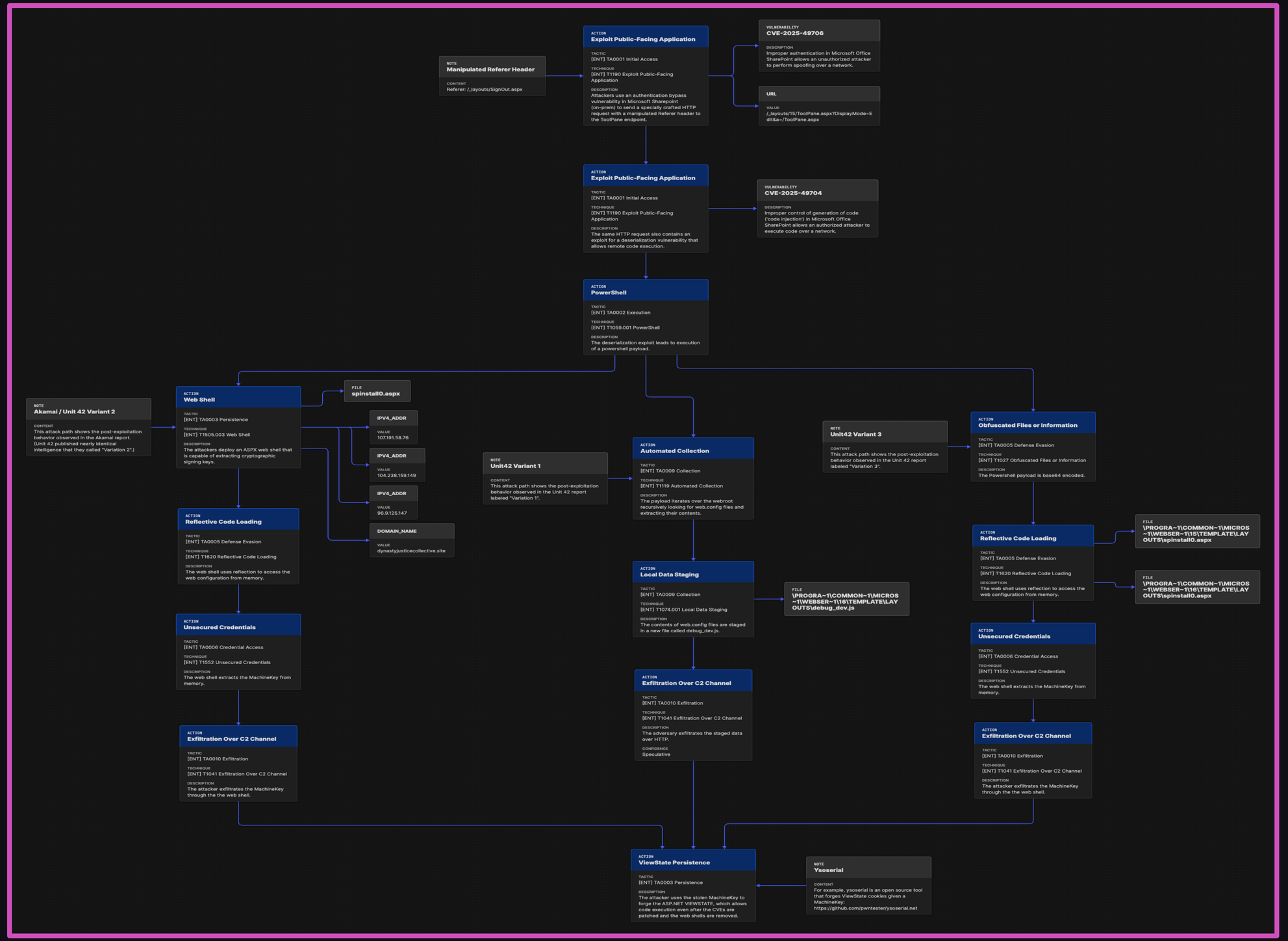




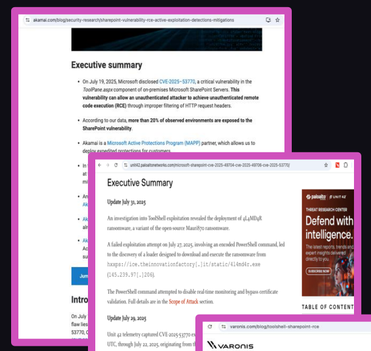
Browser Extension

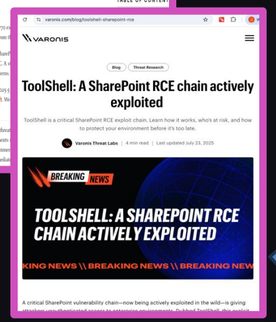
attack.mitre.org/tactics/..


Sharepoint Exploit Flow
Aa
July 28, 2025 at 12:56 PM
Sharepoint Exploit Flow
https://www.akamai.com/blog/security-research/sharepoint-vulnerability-rce-active-exploitation-detections-mitigations
https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/
T0819: Exploit Public-Facing Application
Exploiting the authentication bypass (CVE-2025-49706) - Improper authentication in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.
The first step in exploiting CVE-2025-49706 is to send a specially crafted POST request to the endpoint, manipulating the HTTP 'Referer' header. The attacker targets the endpoint value /_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx with the crafted value /_layouts/SignOut.aspx to manipulate the system into trusting the request and its payload.
Exploiting the deserialization vulnerability (CVE-2025-49704) - Improper control of generation of code ('code injection') in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.
T1059.001: Command and Scripting Interpreter: PowerShell
Once the authentication bypass is achieved, attackers can exploit the deserialization vulnerability to execute PowerShell code.
Akamai Variant:
T1505.003: Server Software Component: Web Shell
In observed attacks, attackers deployed a malicious second-stage ASPX file designed to extract cryptographic keys that are signed (MachineKey) from web.config (which the server trusts), enabling stealthier follow-up exploitation (Figure 1).
T1552: Unsecured Credentials
By accessing the deployed malicious endpoint, attackers can extract the cryptographic secrets needed to sign serialized payloads (Figure 2).
Indicators of compromise


NOTE
Manipulated Referer Header
CONTENT
Referer: /_layouts/SignOut.aspx
ACTION
Exploit Public-Facing Application
TACTIC
[ENT] TA0001 Initial Access
TECHNIQUE
[ENT] T1190 Exploit Public-Facing Application
DESCRIPTION
Attackers use an authentication bypass vulnerability in Microsoft Sharepoint (on-prem) to send a specially crafted HTTP request with a manipulated Referer header to the ToolPane endpoint.
VULNERABILITY
CVE-2025-49706
DESCRIPTION
Improper authentication in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.
URL
VALUE
/_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx
ACTION
Exploit Public-Facing Application
TACTIC
[ENT] TA0001 Initial Access
TECHNIQUE
[ENT] T1190 Exploit Public-Facing Application
DESCRIPTION
The same HTTP request also contains an exploit for a deserialization vulnerability that allows remote code execution.
VULNERABILITY
CVE-2025-49704
DESCRIPTION
Improper control of generation of code ('code injection') in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.
ACTION
PowerShell
TACTIC
[ENT] TA0002 Execution
TECHNIQUE
[ENT] T1059.001 PowerShell
DESCRIPTION
The deserialization exploit leads to execution of a powershell payload.
NOTE
Akamai / Unit 42 Variant 2
CONTENT
This attack path shows the post-exploitation behavior observed in the Akamai report. (Unit 42 published nearly identical intelligence that they called "Variation 2".)
ACTION
Web Shell
TACTIC
[ENT] TA0003 Persistence
TECHNIQUE
[ENT] T1505.003 Web Shell
DESCRIPTION
The attackers deploy an ASPX web shell that is capable of extracting cryptographic signing keys.
FILE
spinstall0.aspx
IPV4_ADDR
VALUE
107.191.58.76
IPV4_ADDR
VALUE
104.238.159.149
IPV4_ADDR
VALUE
96.9.125.147
DOMAIN_NAME
VALUE
dynastyjusticecollective.site
NOTE
Unit42 Variant 1
CONTENT
This attack path shows the post-exploitation behavior observed in the Unit 42 report labeled "Variation 1".
ACTION
Automated Collection
TACTIC
[ENT] TA0009 Collection
TECHNIQUE
[ENT] T1119 Automated Collection
DESCRIPTION
The payload iterates over the webroot recursively looking for web.config files and extracting their contents.
NOTE
Unit42 Variant 3
CONTENT
This attack path shows the post-exploitation behavior observed in the Unit 42 report labeled "Variation 3".
ACTION
Obfuscated Files or Information
TACTIC
[ENT] TA0005 Defense Evasion
TECHNIQUE
[ENT] T1027 Obfuscated Files or Information
DESCRIPTION
The Powershell payload is base64 encoded.
ACTION
Reflective Code Loading
TACTIC
[ENT] TA0005 Defense Evasion
TECHNIQUE
[ENT] T1620 Reflective Code Loading
DESCRIPTION
The web shell uses reflection to access the web configuration from memory.
ACTION
Reflective Code Loading
TACTIC
[ENT] TA0005 Defense Evasion
TECHNIQUE
[ENT] T1620 Reflective Code Loading
DESCRIPTION
The web shell uses reflection to access the web configuration from memory.
FILE
\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS\spinstall0.aspx
FILE
\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS\spinstall0.aspx
ACTION
Local Data Staging
TACTIC
[ENT] TA0009 Collection
TECHNIQUE
[ENT] T1074.001 Local Data Staging
DESCRIPTION
The contents of web.config files are staged in a new file called debug_dev.js.
FILE
\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS\debug_dev.js
ACTION
Unsecured Credentials
TACTIC
[ENT] TA0006 Credential Access
TECHNIQUE
[ENT] T1552 Unsecured Credentials
DESCRIPTION
The web shell extracts the MachineKey from memory.
ACTION
Unsecured Credentials
TACTIC
[ENT] TA0006 Credential Access
TECHNIQUE
[ENT] T1552 Unsecured Credentials
DESCRIPTION
The web shell extracts the MachineKey from memory.
ACTION
Exfiltration Over C2 Channel
TACTIC
[ENT] TA0010 Exfiltration
TECHNIQUE
[ENT] T1041 Exfiltration Over C2 Channel
DESCRIPTION
The adversary exfiltrates the staged data over HTTP.
CONFIDENCE
Speculative
ACTION
Exfiltration Over C2 Channel
TACTIC
[ENT] TA0010 Exfiltration
TECHNIQUE
[ENT] T1041 Exfiltration Over C2 Channel
DESCRIPTION
The attacker exfiltrates the MachineKey through the the web shell.
ACTION
Exfiltration Over C2 Channel
TACTIC
[ENT] TA0010 Exfiltration
TECHNIQUE
[ENT] T1041 Exfiltration Over C2 Channel
DESCRIPTION
The attacker exfiltrates the MachineKey through the the web shell.
ACTION
ViewState Persistence
TACTIC
[ENT] TA0003 Persistence
DESCRIPTION
The attacker uses the stolen MachineKey to forge the ASP.NET VIEWSTATE, which allows code execution even after the CVEs are patched and the web shells are removed.
NOTE
Ysoserial
CONTENT
For example, ysoserial is an open source tool that forges ViewState cookies given a MachineKey:
https://github.com/pwntester/ysoserial.net

Detection Pipelines





CTI

Create Flow

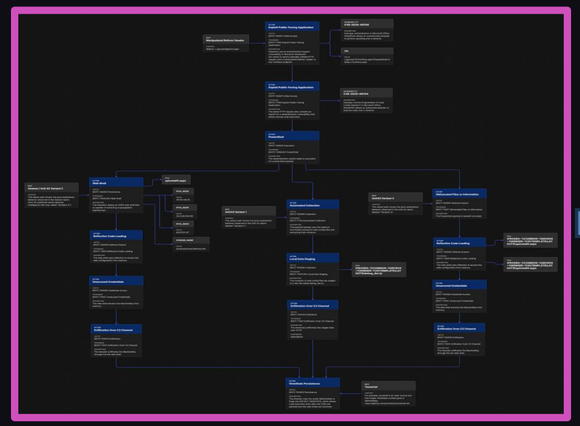
JSON

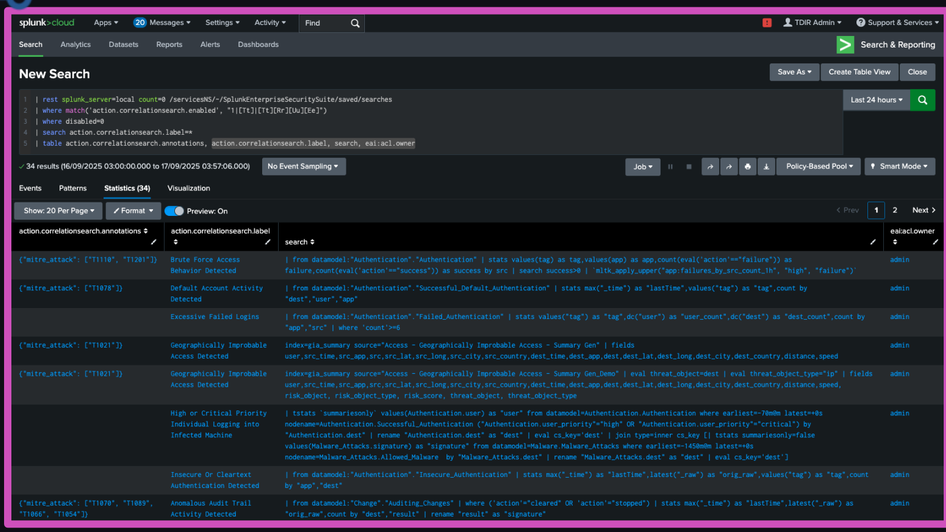
- Ingest
- Parse

Check Detection Coverage

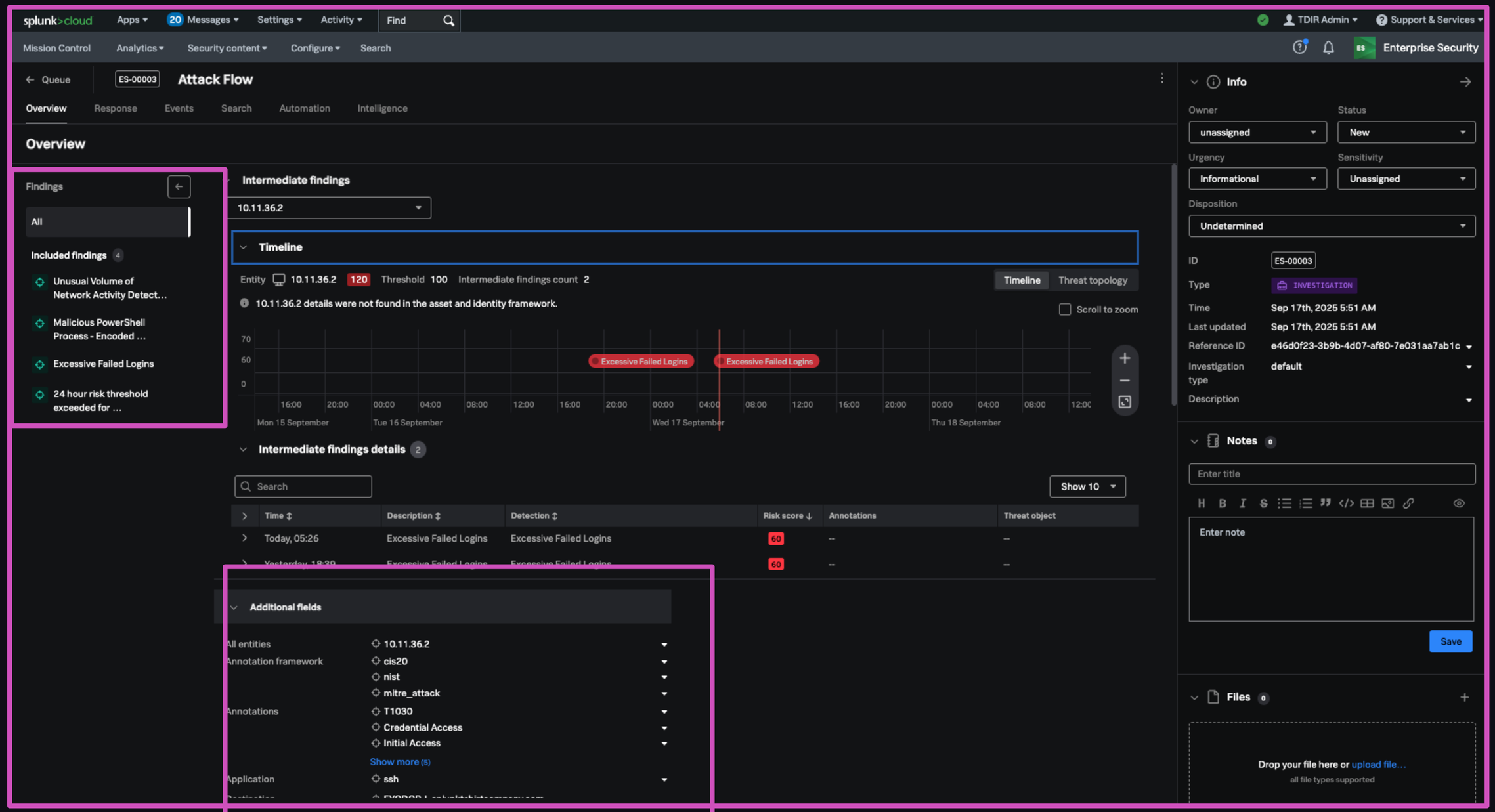
Deploy missing Detections

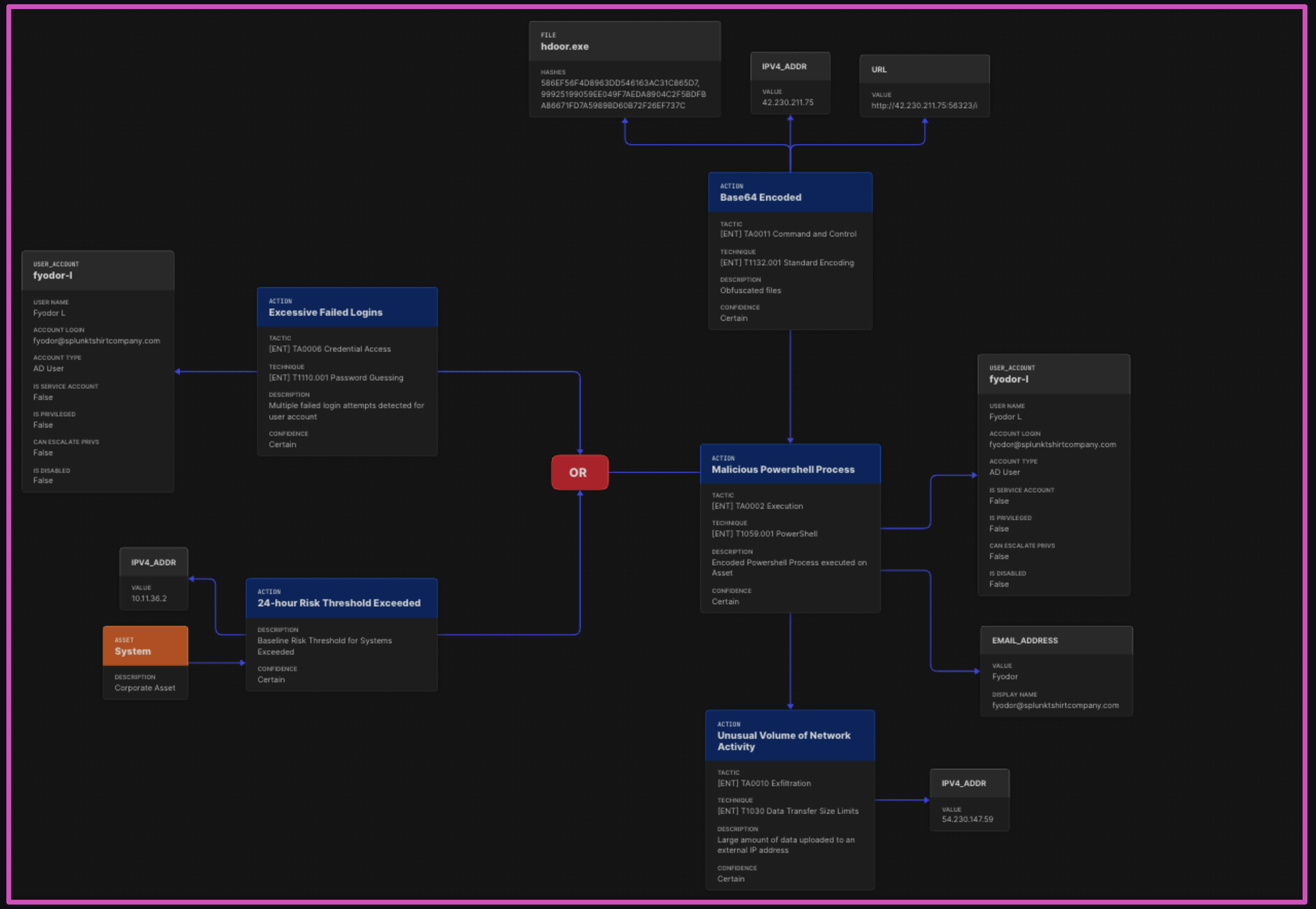
Test



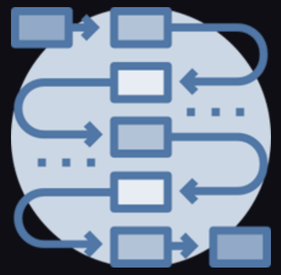


Using Attack Flow for Investigations


splunk>cloud
Apps
20 Messages
Settings
Activity
Find
TDIR Admin
Support & Services
Mission Control
Analytics
Security content
Configure
Search
Enterprise Security
Queue
ES-00003
Attack Flow
Overview
Response
Events
Search
Automation
Intelligence
Overview
Findings
All
Included findings 4
Unusual Volume of Network Activity Detect...
Malicious PowerShell Process - Encoded ...
Excessive Failed Logins
24 hour risk threshold exceeded for ...
Intermediate findings
10.11.36.2
Timeline
Entity 10.11.36.2 120 Threshold 100 Intermediate findings count 2
Timeline
Threat topology
10.11.36.2 details were not found in the asset and identity framework.
Scroll to zoom
70
60
0
Excessive Failed Logins
Excessive Failed Logins
16:00 20:00 00:00 04:00 08:00 12:00 16:00 20:00 00:00 04:00 08:00 12:00 16:00 20:00 00:00 04:00 08:00 12:00
Mon 15 September
Tue 16 September
Wed 17 September
Thu 18 September
Intermediate findings details 2
Search
Show 10
Time
Description
Detection
Risk score
Annotations
Threat object
Today, 05:26
Excessive Failed Logins
Excessive Failed Logins
60
--
--
Additional fields
All entities
10.11.36.2
Annotation framework
cis20
nist
mitre_attack
Annotations
T1030
Credential Access
Initial Access
Show more (5)
Application
ssh
Info
Owner
unassigned
Status
New
Urgency
Informational
Sensitivity
Unassigned
Disposition
Undetermined
ID
ES-00003
Type
INVESTIGATION
Time
Sep 17th, 2025 5:51 AM
Last updated
Sep 17th, 2025 5:51 AM
Reference ID
e46d0f23-3b9b-4d07-af80-7e031aa7ab1c
Investigation type
default
Description
Notes 0
Enter title
Enter note
Save
Files 0
Drop your file here or upload file...
all file types supported


FILE
hdoor.exe
HASHES
586EF56F4D8963DD546163AC31C865D7,
99925199059EE049F7AEDA8904C2F5BDFB
A86671FD7A5989BD60B72F26EF737C
IPV4_ADDR
VALUE
42.230.211.75
URL
VALUE
http://42.230.211.75:56323/i
ACTION
Base64 Encoded
TACTIC
[ENT] TA0011 Command and Control
TECHNIQUE
[ENT] T1132.001 Standard Encoding
DESCRIPTION
Obfuscated files
CONFIDENCE
Certain
USER_ACCOUNT
fyodor-l
USER NAME
Fyodor L
ACCOUNT LOGIN
fyodor@splunktshirtcompany.com
ACCOUNT TYPE
AD User
IS SERVICE ACCOUNT
False
IS PRIVILEGED
False
CAN ESCALATE PRIVS
False
IS DISABLED
False
ACTION
Excessive Failed Logins
TACTIC
[ENT] TA0006 Credential Access
TECHNIQUE
[ENT] T1110.001 Password Guessing
DESCRIPTION
Multiple failed login attempts detected for user account
CONFIDENCE
Certain
OR
ACTION
Malicious Powershell Process
TACTIC
[ENT] TA0002 Execution
TECHNIQUE
[ENT] T1059.001 PowerShell
DESCRIPTION
Encoded Powershell Process executed on Asset
CONFIDENCE
Certain
USER_ACCOUNT
fyodor-l
USER NAME
Fyodor L
ACCOUNT LOGIN
fyodor@splunktshirtcompany.com
ACCOUNT TYPE
AD User
IS SERVICE ACCOUNT
False
IS PRIVILEGED
False
CAN ESCALATE PRIVS
False
IS DISABLED
False
IPV4_ADDR
VALUE
10.11.36.2
ASSET
System
DESCRIPTION
Corporate Asset
ACTION
24-hour Risk Threshold Exceeded
DESCRIPTION
Baseline Risk Threshold for Systems Exceeded
CONFIDENCE
Certain
EMAIL_ADDRESS
VALUE
Fyodor
DISPLAY NAME
fyodor@splunktshirtcompany.com
ACTION
Unusual Volume of Network Activity
TACTIC
[ENT] TA0010 Exfiltration
TECHNIQUE
[ENT] T1030 Data Transfer Size Limits
DESCRIPTION
Large amount of data uploaded to an external IP address
CONFIDENCE
Certain
IPV4_ADDR
VALUE
54.230.147.59

Components of Attack Flow



Attack Flow Builder Tool

- Web-based tool for creating, editing and presenting flows
- Easily publish & share

Attack Flow Library

- A collection of example flows
- Used for learning about attacks and/or data mining

Machine-Readable Format

- Based on STIX 2.1
- Interoperability between vendors

Visualisation

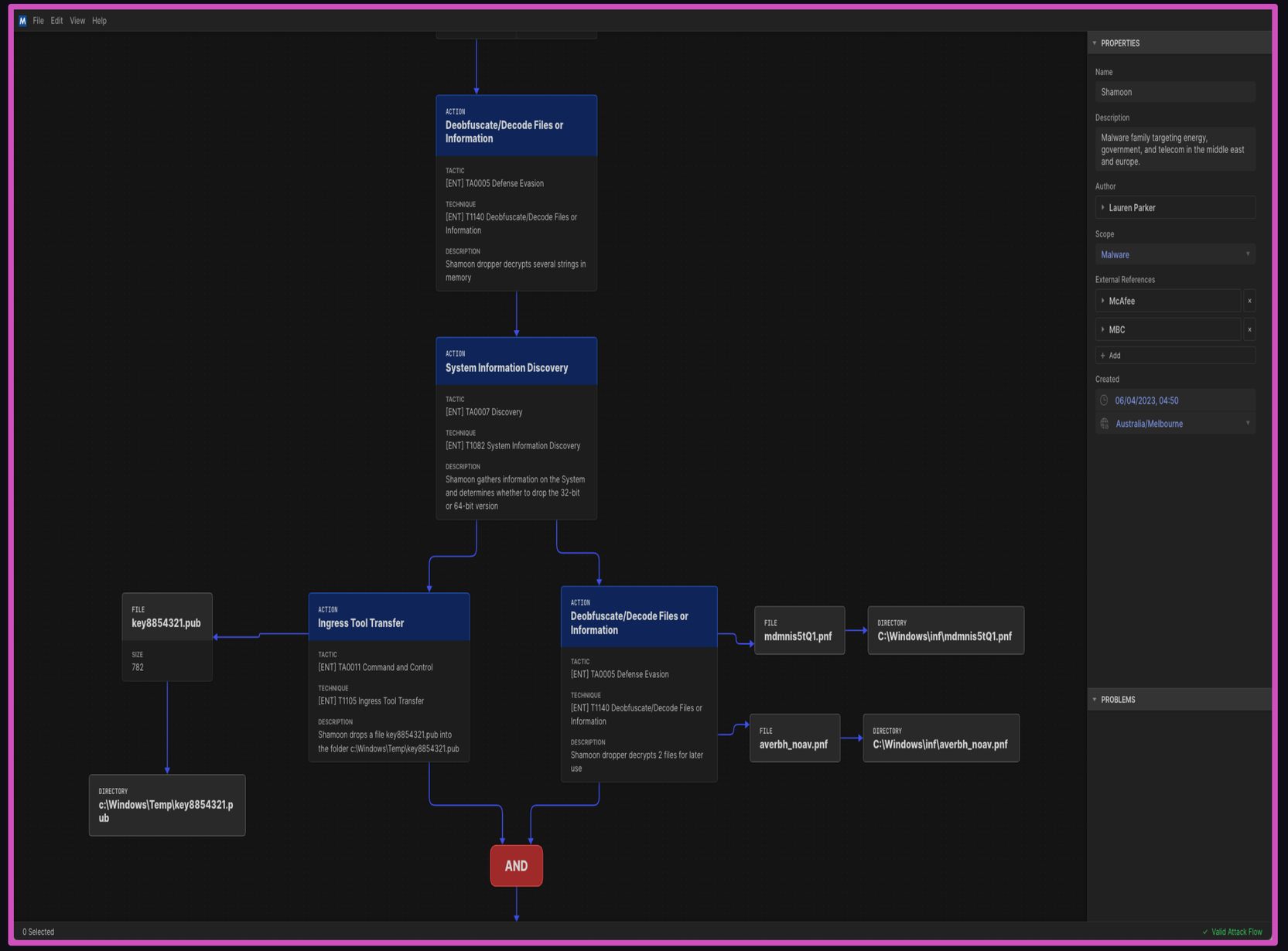
- Tools for visualising flows for different audiences and purposes

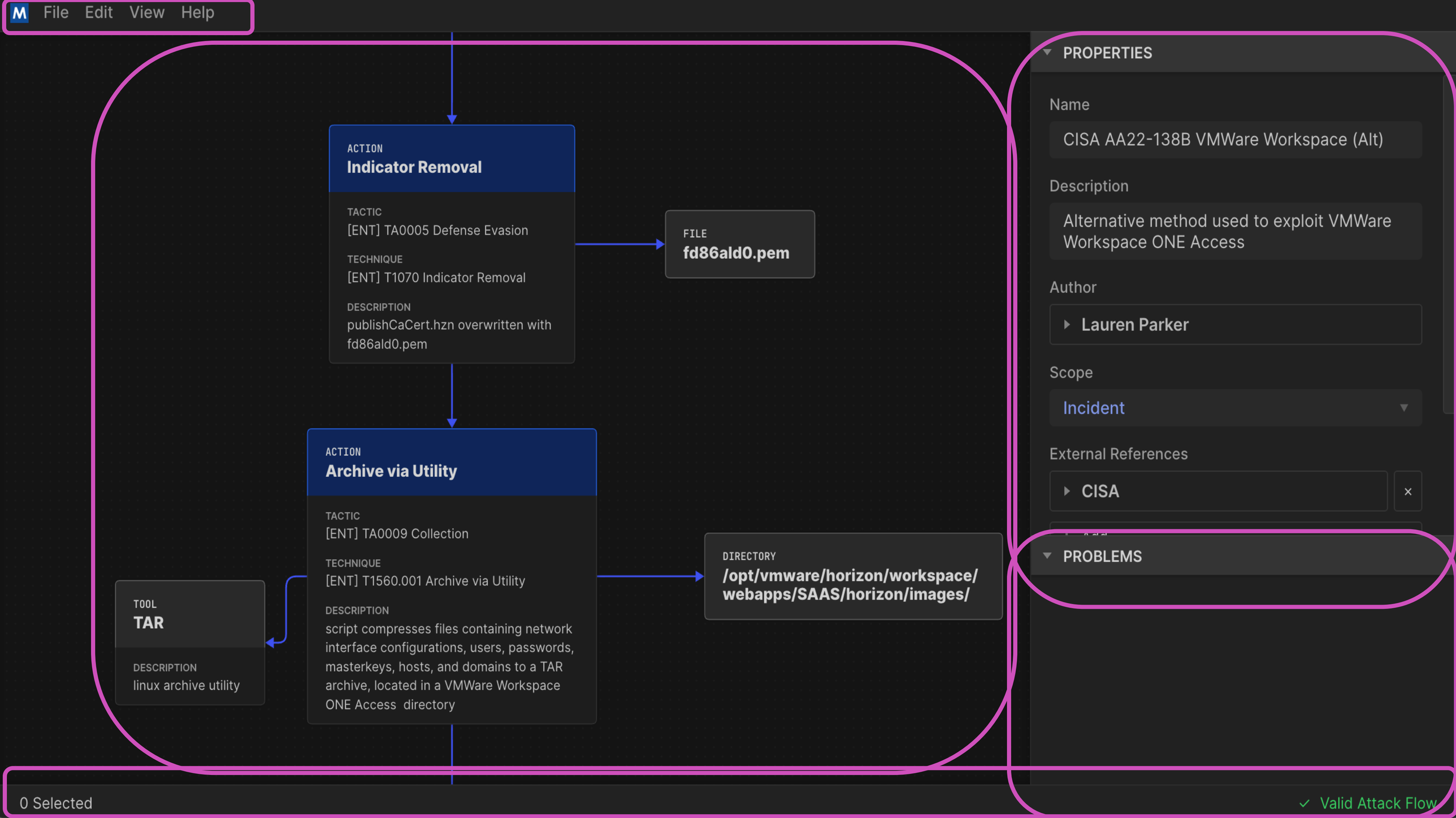
Documentation

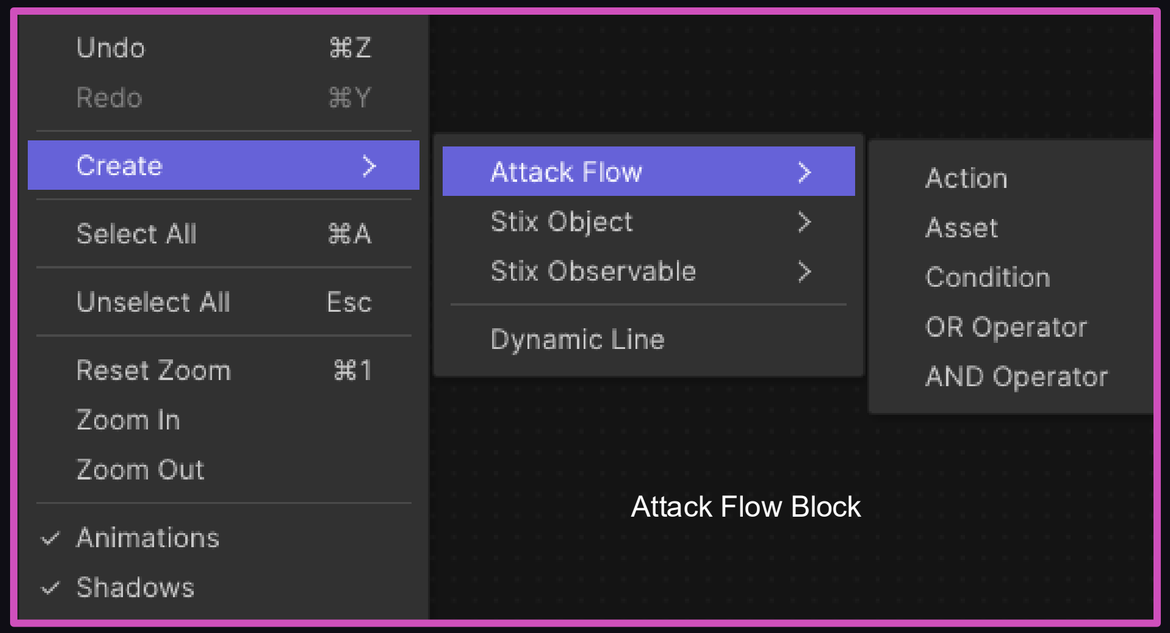
- User-friendly learning curve
- Easy access to the builder & flow library

Component 1 - Attack Flow Builder Tool

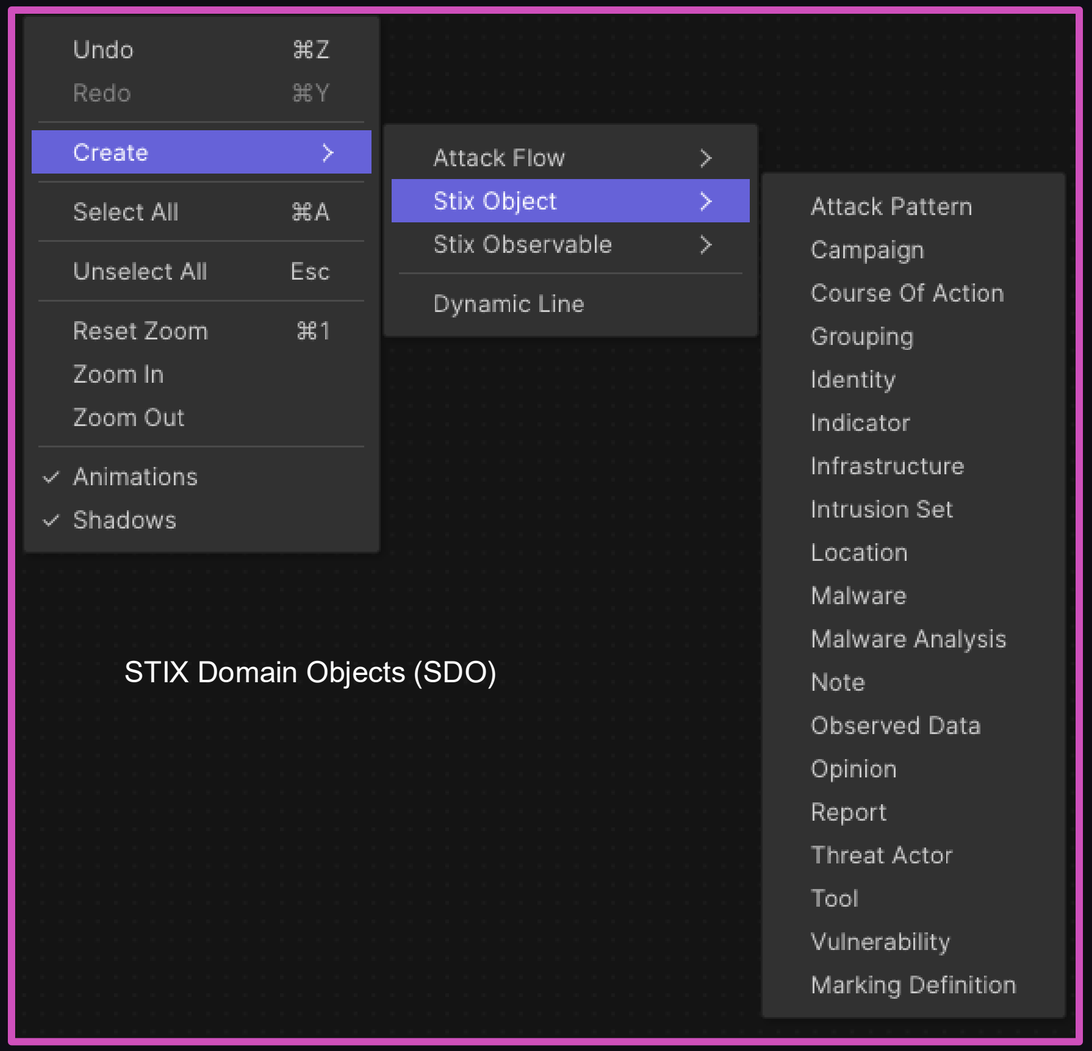
- Open-source, web-based tool.
- Similar to Visio: create nodes (boxes) and connect with edges (lines).
- Create, edit, export and present flows.
- Private: flow data stays in the browser. CTID does not collect or share it.
- Can be hosted on-premise for additional privacy & assurance.



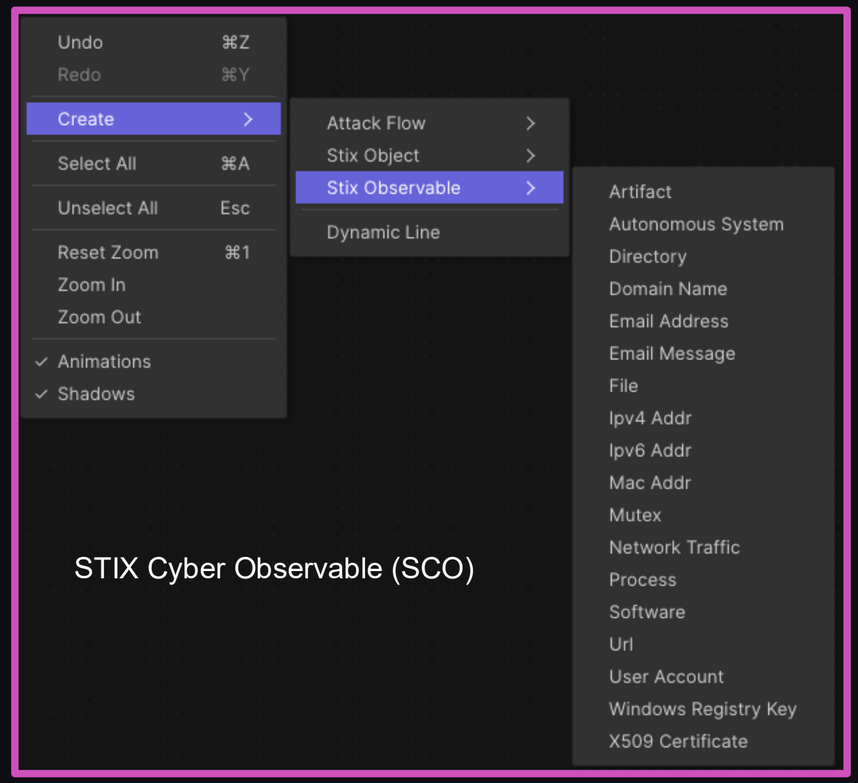

File Edit View Help
ACTION
Indicator Removal
TACTIC
[ENT] TA0005 Defense Evasion
TECHNIQUE
[ENT] T1070 Indicator Removal
DESCRIPTION
publishCaCert.hzn overwritten with fd86ald0.pem
FILE
fd86ald0.pem
ACTION
Archive via Utility
TACTIC
[ENT] TA0009 Collection
TECHNIQUE
[ENT] T1560.001 Archive via Utility
DESCRIPTION
script compresses files containing network interface configurations, users, passwords, masterkeys, hosts, and domains to a TAR archive, located in a VMWare Workspace ONE Access directory
TOOL
TAR
DESCRIPTION
linux archive utility
DIRECTORY
/opt/vmware/horizon/workspace/webapps/SAAS/horizon/images/
PROPERTIES
Name
CISA AA22-138B VMWare Workspace (Alt)
Description
Alternative method used to exploit VMWare Workspace ONE Access
Author
Lauren Parker
Scope
Incident
External References
CISA
PROBLEMS
0 Selected
Valid Attack Flow



Attack Flow Block



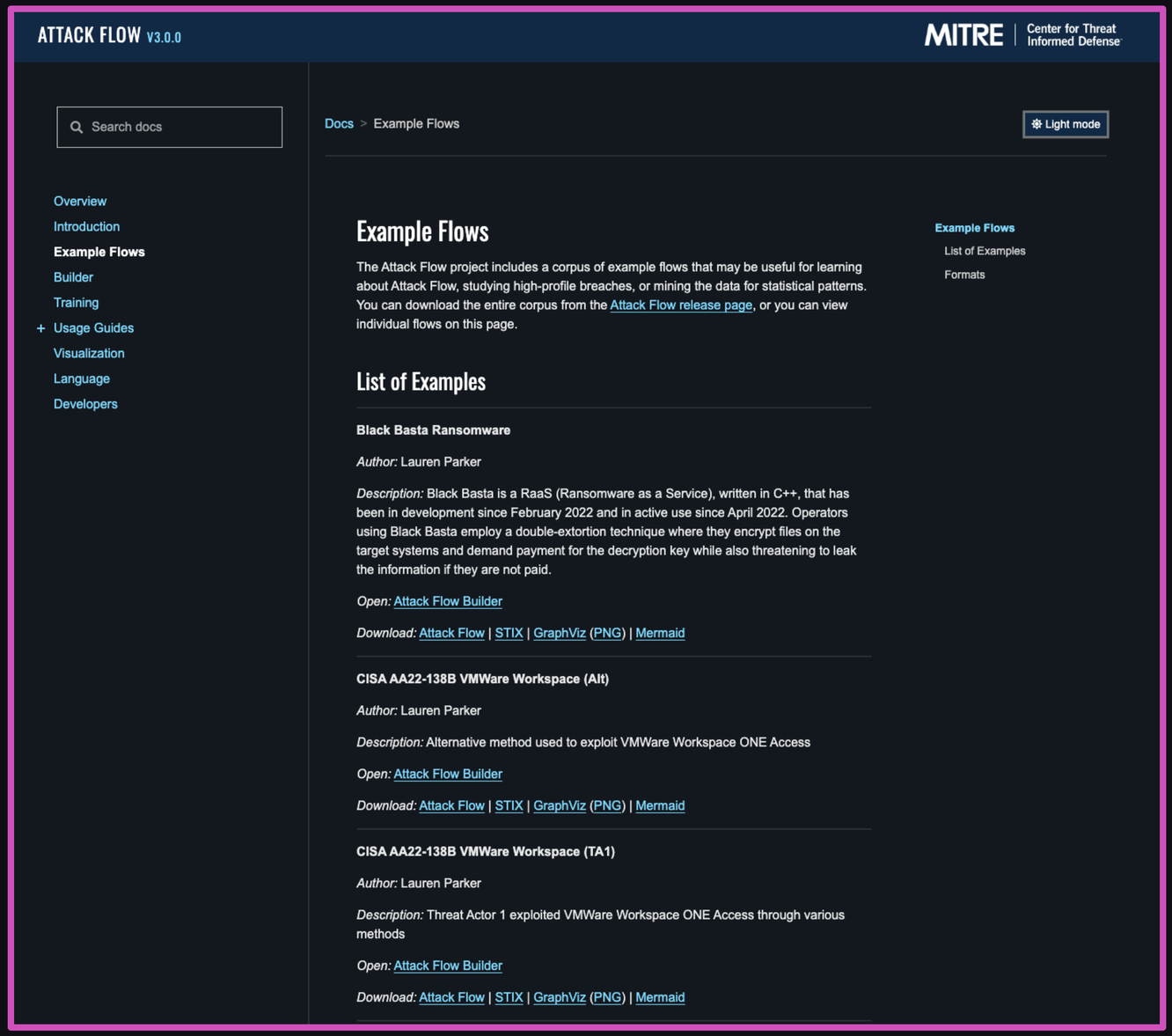
STIX Domain Objects (SDO)



STIX Cyber Observable (SCO)

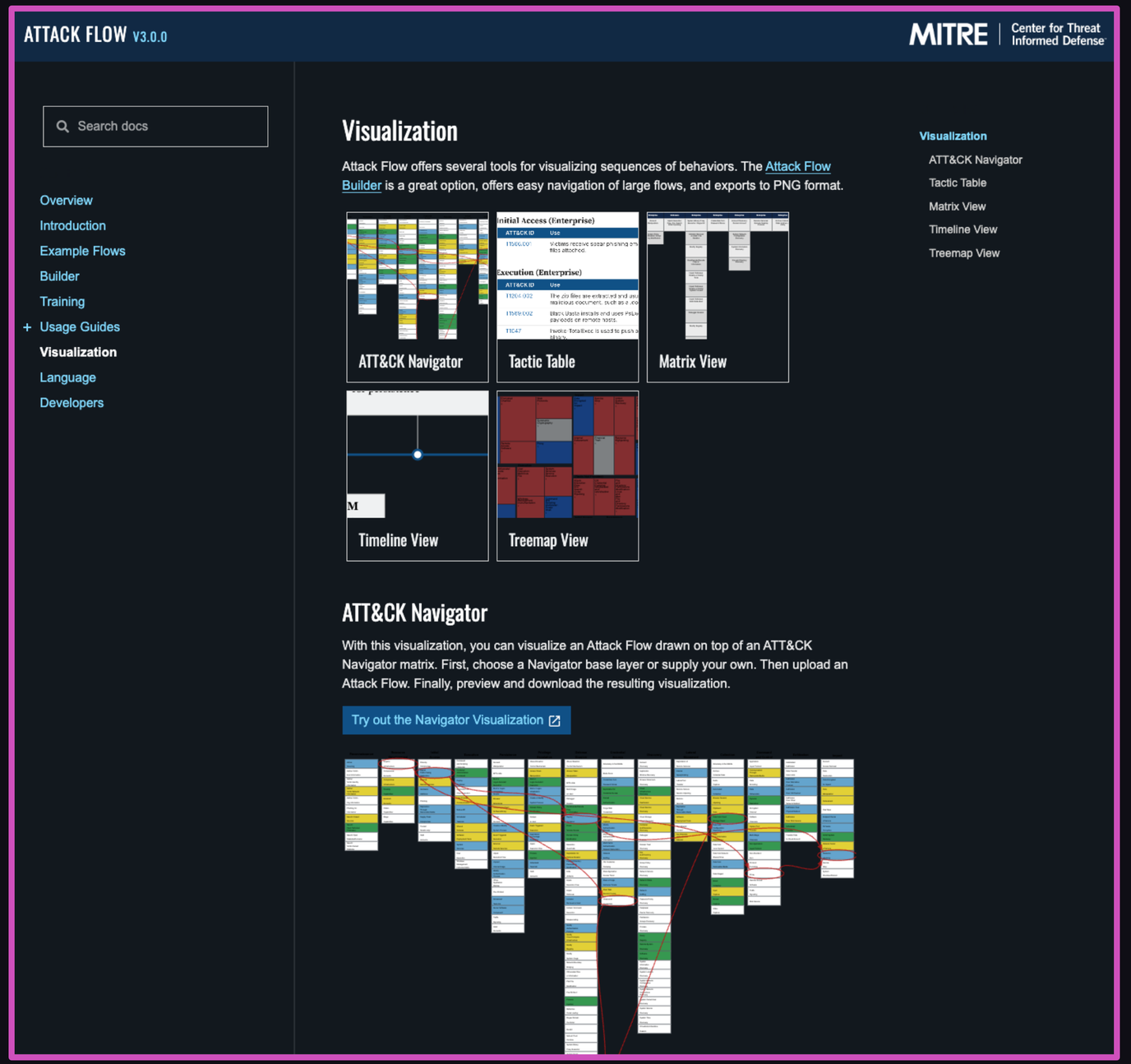
Component 2 - Attack Flow Library

- A collection of example flows, based mostly on real-world CTI.
- Each example contains references to source material
- Open each example in Attack Flow Builder (.afb) or download as image (.png)

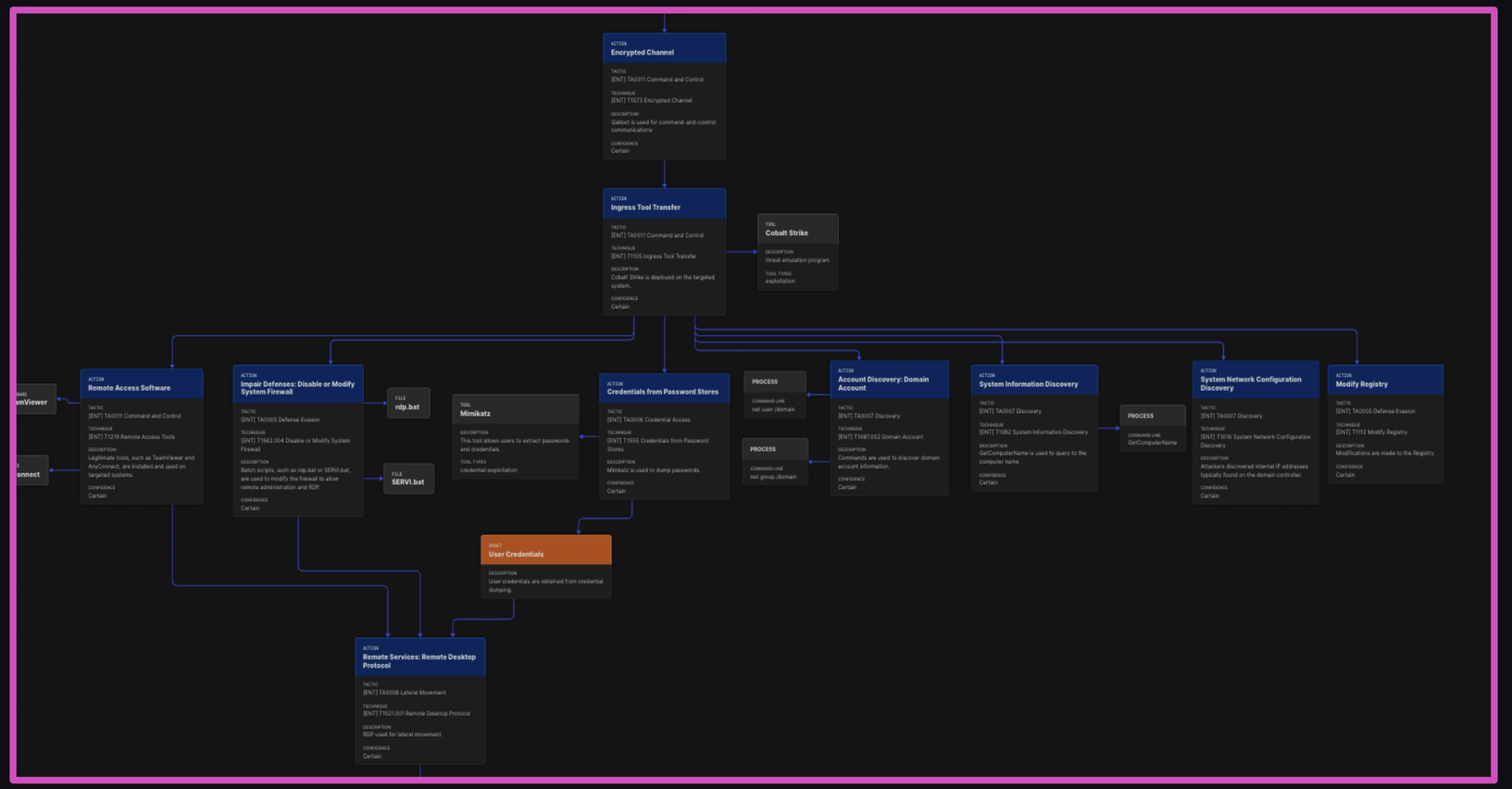


Component 3 – Visualisation

- Extract data from an Attack Flow and generate insight by visualising it in new ways
- Automatically generate TTP tables or timeline views – a huge time saver.



Visualisation



.afb — Attack Flow

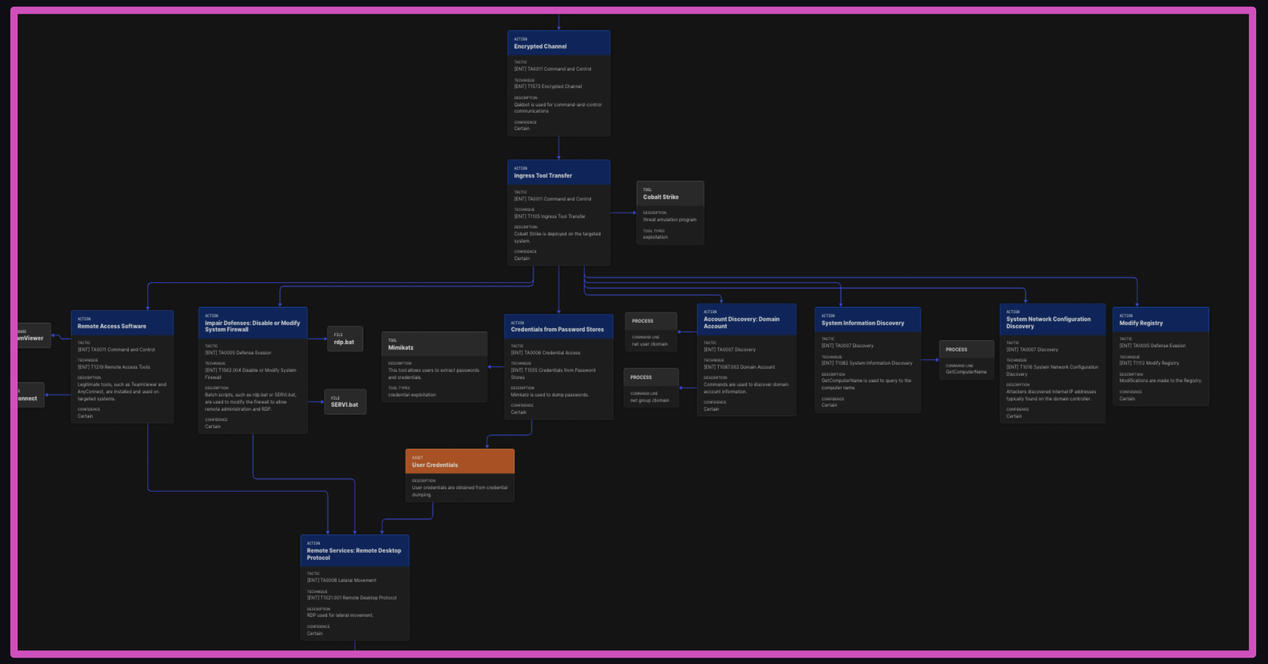
.json — STIX

.png — Portable Network Graphic

.dot — GraphViz

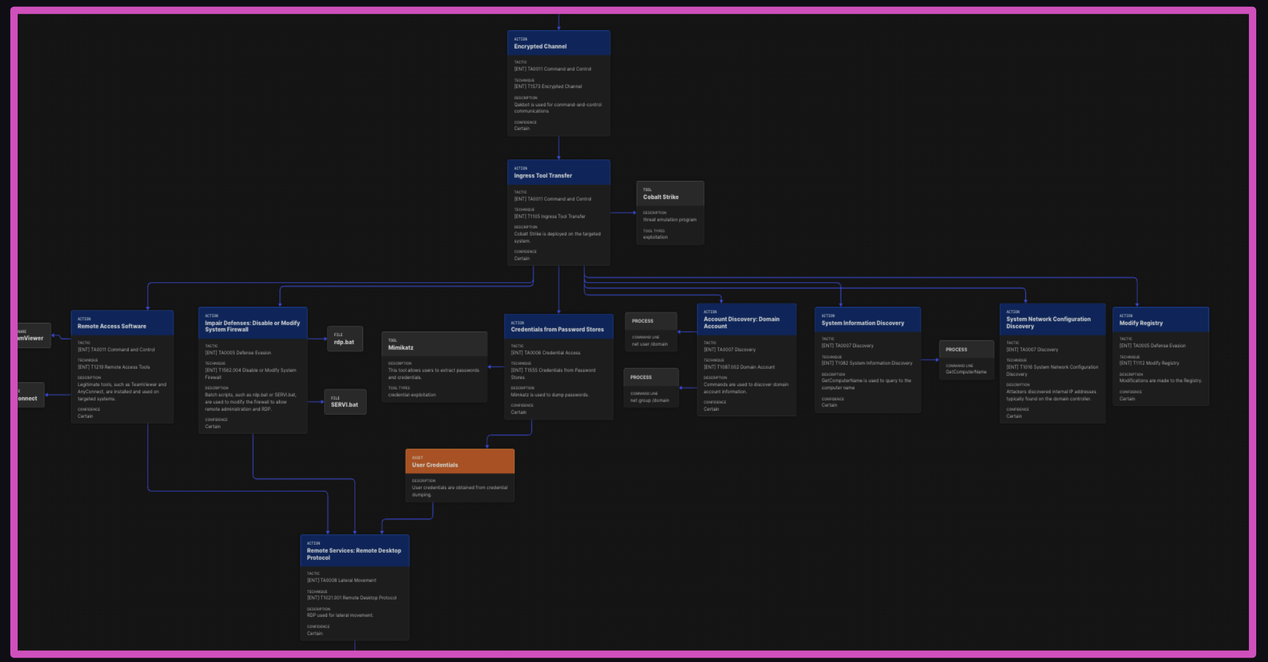
.mmd — Mermaid.js

Visualisation



- Attack Flow is inherently visual – but it is a single mode of visualisation.
  - This might be limiting for certain audiences or purposes.
- Flow Visualisation means to represent existing flows in new ways

Visualisation

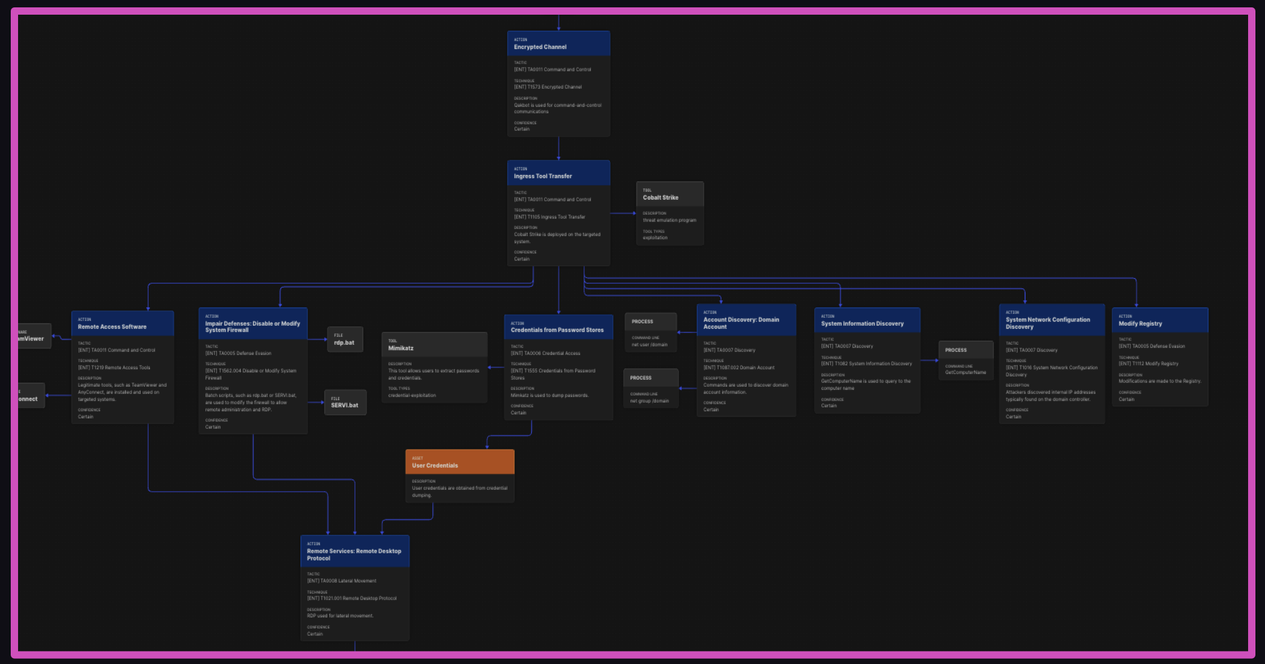


Save time through Automation

- Automate artifacts that are currently made by hand (or not at all)

Generate insights

- View data in new ways, or mashed up with other data sources
- Derive new insights



ATT&CK Navigator

Table 1: TA0001 - Initial Access (Enterprise)

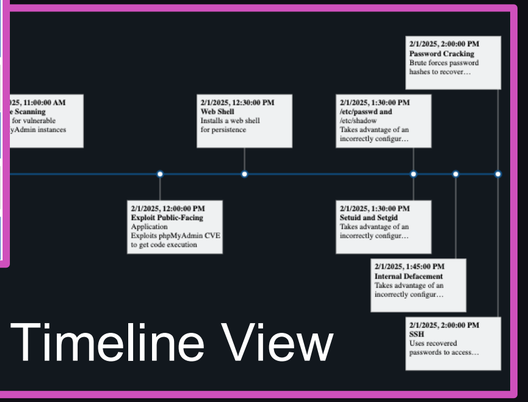
Technique Name	ATT&CK ID	Use
Phishing: Spearphishing Attachment	T1566.001	Victims receive spear phishing emails with malicious zip files attached.

Table 2: TA0002 - Execution (Enterprise)

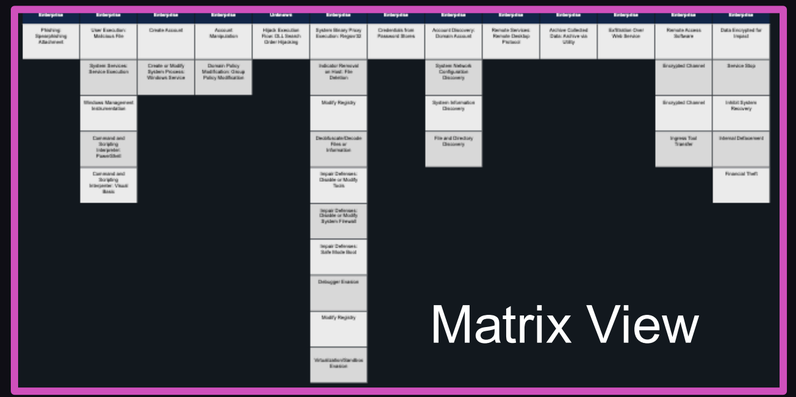
Technique Name	ATT&CK ID	Use
User Execution: Malicious File	T1204.002	The zip files are extracted and usually contain a malicious document, such as a .doc, .pdf, or .xls.
System Services: Service Execution	T1569.002	Black Basta installs and uses PsExec to execute payloads on remote hosts.
Windows Management Instrumentation	T1047	Invoke-TotalExec is used to push out the ransomware binary.
Command and Scripting Interpreter: PowerShell	T1059.001	Within the malicious files, encoded PowerShell scripts are used to download additional malicious scripts.
Command and Scripting Interpreter: Visual Basic	T1059.005	The extracted files contain malicious macros.

Tactic Table

Treemap View



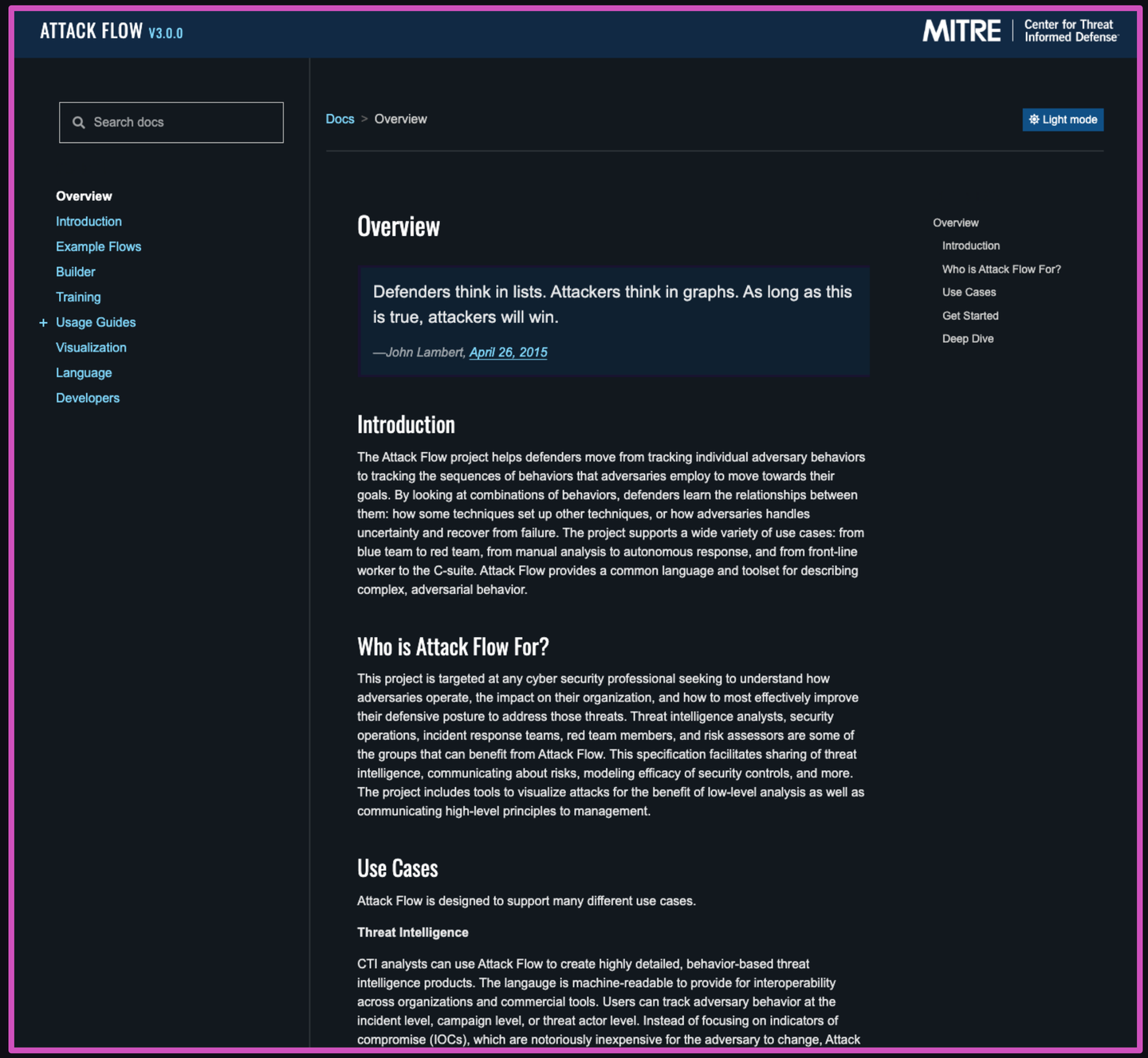
Timeline View



Matrix View

Component 4 – Documentation

- A complete guide to learning Attack Flow, starting from the ground up
- Links to builder tool and visualisations
- Usage guides for applying Attack Flow to specific job roles



Impact

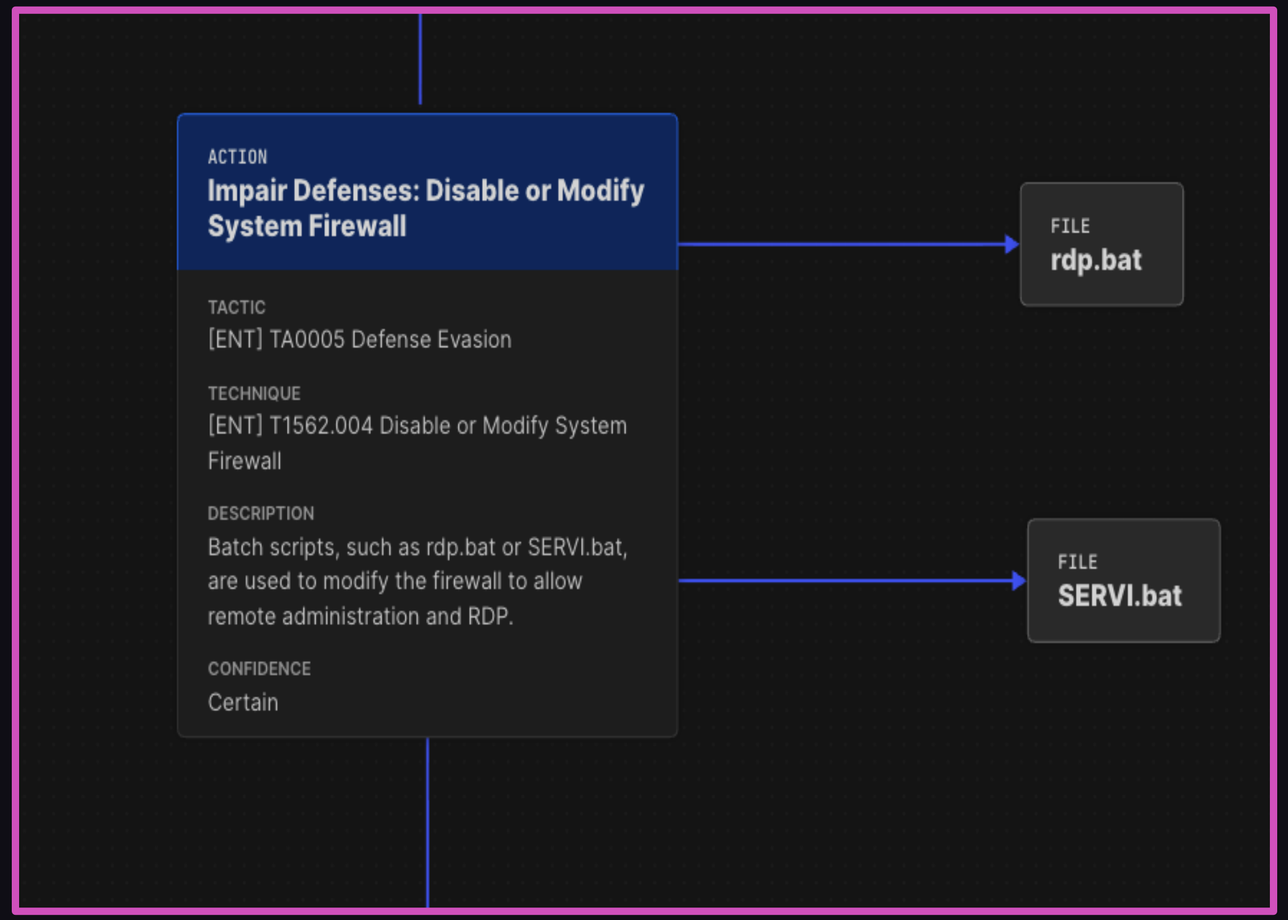
Help defenders and leaders understand how adversaries operate and compose atomic techniques into attacks to better understand defensive posture

Attack Flow

Why it matters?

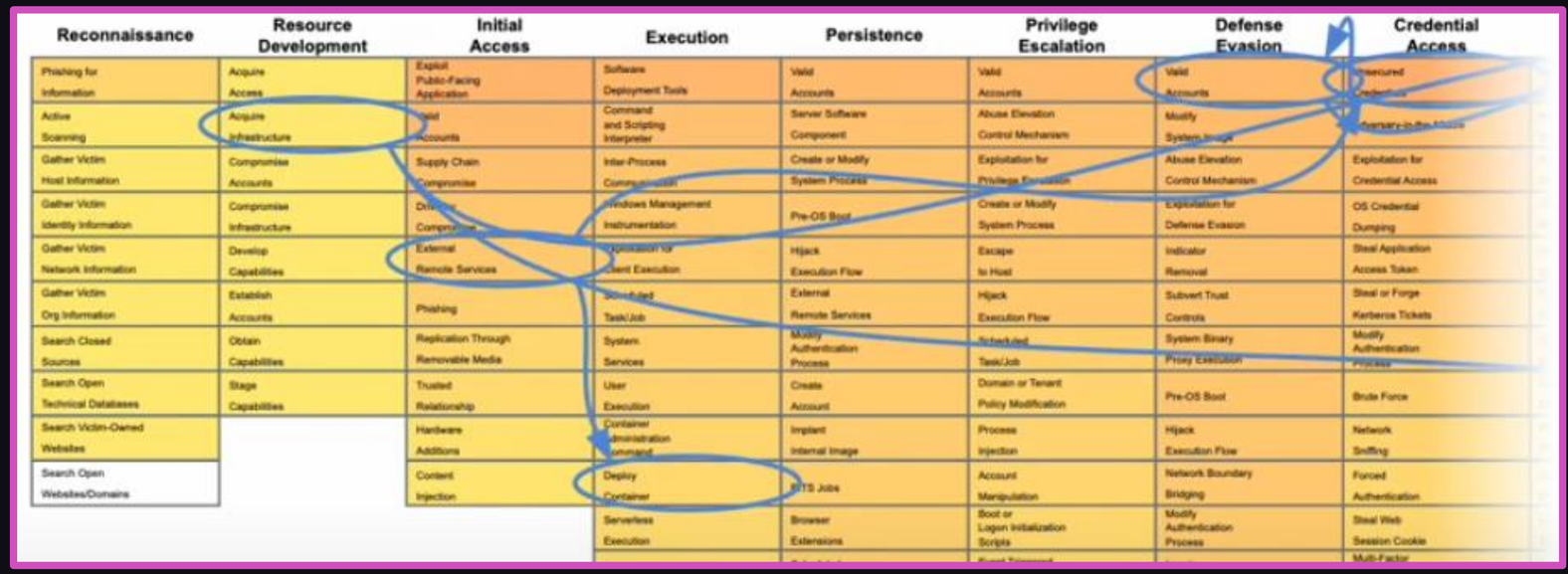
Less Ambiguous

- Prose reports contain significant ambiguity, especially around the order of events, dependencies and confidence levels.
- Attack Flow clarifies how an adversary works through a sequence of behaviours to reach their desired impact.
- Models how adversaries handle failure and recovery.



Visualise & Present

- Visualise attack paths and chokepoints.
- High quality presentations for a variety of audiences, including execs.
- Combine with other data to generate insights.



Increase Automation

- Machine readable format is compatible with STIX; import & export IOCs easily
- Visualisation tools automatically create artifacts such as TTP tables or attack timelines
- Open source: coders can build custom tooling


```
{
  "type": "bundle",
  "id": "bundle--bd17b78b-2ffd-45db-a4b0-d1104b95c2db",
  "spec_version": "2.1",
  "created": "2025-07-30T19:47:12.605Z",
  "modified": "2025-07-30T19:47:12.605Z",
  "objects": [
    {
      "type": "extension-definition",
      "id": "extension-definition--fb9c968a-745b-4ade-9b25-c324172197f4",
      "spec_version": "2.1",
      "created": "2022-08-02T19:34:35.143Z",
      "modified": "2022-08-02T19:34:35.143Z",
      "name": "Attack Flow",
      "description": "Extends STIX 2.1 with features to create Attack Flows.",
      "created_by_ref": "identity--fb9c968a-745b-4ade-9b25-c324172197f4",
      "schema": "https://center-for-threat-informed-defense.github.io/attack-flow/stix/attack-flow-schema-2.0.0.json",
      "version": "2.0.0",
      "extension_types": [
        "new-sdo"
      ],
      "external_references": [
        {
          "source_name": "Documentation",
          "description": "Documentation for Attack Flow",
          "url": "https://center-for-threat-informed-defense.github.io/attack-flow"
        },
        {
          "source_name": "GitHub",
          "description": "Source code repository for Attack Flow",
          "url": "https://github.com/center-for-threat-informed-defense/attack-flow"
        }
      ]
    },
    {
      "type": "identity",
      "id": "identity--fb9c968a-745b-4ade-9b25-c324172197f4",
      "spec_version": "2.1",
      "created": "2022-08-02T19:34:35.143Z",
      "modified": "2022-08-02T19:34:35.143Z",
      "created_by_ref": "identity--fb9c968a-745b-4ade-9b25-c324172197f4",
      "name": "MITRE Center for Threat-Informed Defense",
      "identity_class": "organization"
    },
    {
      "type": "attack-flow",
      "id": "attack-flow--042142d6-2080-4c1d-8ef2-bad02c39db3b",
      "spec_version": "2.1",
      "created": "2024-06-19T15:45:49.090Z",
      "modified": "2025-07-30T19:47:12.606Z",
      "extensions": {
        "extension-definition--fb9c968a-745b-4ade-9b25-c324172197f4": {
          "extension_type": "new-sdo"
        }
      },
      "created_by_ref": "identity--0b55fa9f-cd34-442f-a59e-8dae3ff9c0a7",
      "start_refs": [
        "attack-action--a3679838-b02f-4c2b-a0b6-d3450ca2e1dd"
      ]
```


Line 1, Column 1 — 1375 Lines

Who is it for?

- **Cyber Threat Intelligence Analysts**
  - Use Attack Flow to augment CTI reporting.
  - Automatically generate generating artifacts, example – export STIX IOCs, generate timeline view, create TTP table, etc.

- **Incident Response**
  - Use Attack Flow to document incident investigations as they develop.
  - Confidence and notes feature to highlight what's known vs. unknown and where to focus next.

- **Red Team**
  - Plan Red Team scenarios based on known threat actors; start at high level and work down to procedure level.
  - Record execution notes and use the flow to debrief Blue Team.

Resources

- Learn more about MITRE –
  - https://www.mitre.org/focus-areas/cybersecurity
- MITRE ATT&CK® Framework –
  - https://attack.mitre.org
- Know more about MITRE CTID –
  - https://ctid.mitre.org
- Project Website -
  - https://center-for-threat-informed-defense.github.io/attack-flow/

Next Steps

- Visit the Project Website –
  - https://center-for-threat-informed-defense.github.io/attack-flow/
  - Shortlink -> ctid.io/flow

- Open an existing flow and learn about a published breach

- Find an open-source CTI report and try build your own flow for it
  - https://github.com/center-for-threat-informed-defense/attack-flow

Questions?

Thank You