Context is all you need

What alerts, events & logs are relevant to each other?

Agenda

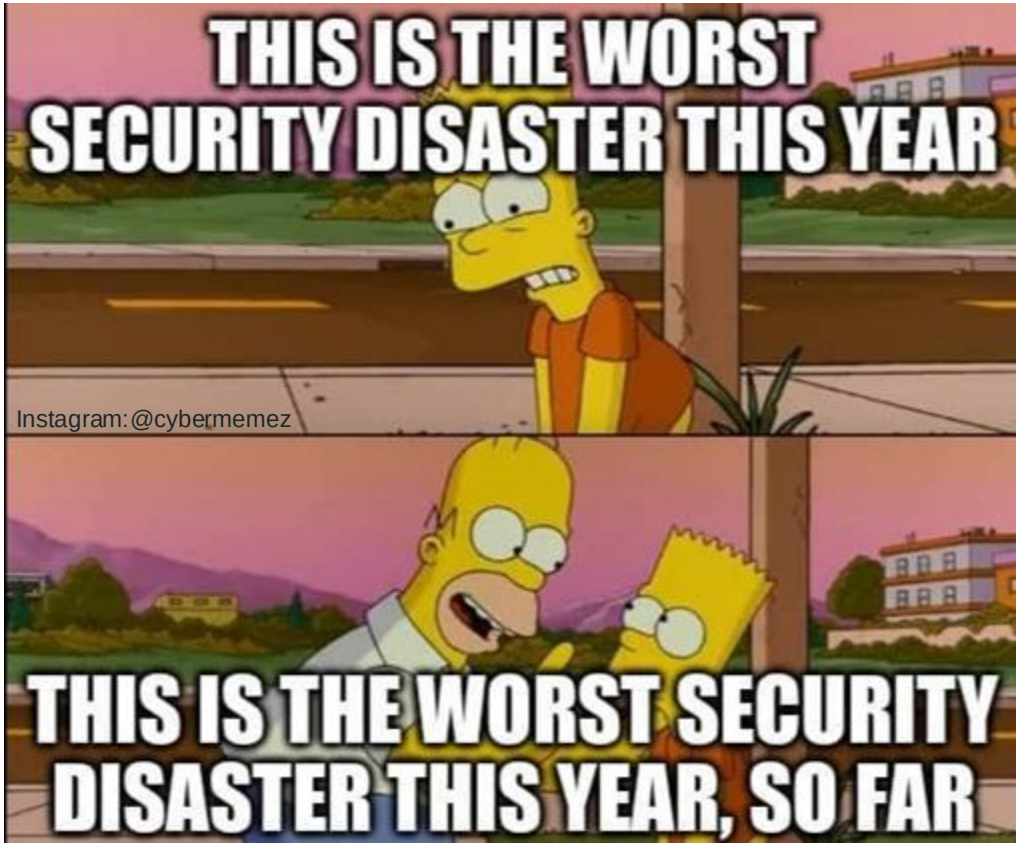
1. Whoami
2. Macro Challenges
   a. Attack Complexity
   b. Data Volume
3. Analysis Challenges
   a. False Positives
   b. Coordinated Attacks
4. ATT&CK
5. Automate the What - When - Who investigations with models
   a. Models in NLP, Clustering , Chaining
6. Examples
7. QA

Ezz Tahoun

Cyber Data Scientist
Cofounder @ Cypienta.com

UW CS PhD Dropout, MMATH, BENG, Adj Professor
GIAC Advisory Board (GIACx3), CISM, aCCISO, CRISC, PMP
GCIH, CEH, GSEC, GFACT, GCP Cloud Professional Architect,

X-RBC, X-OrangeCyberDefense, X-Huawei, X-Forescout
Yale, Princeton, Northwestern, Microsoft, PIA, Trustwave, CCCS


THIS IS THE WORST SECURITY DISASTER THIS YEAR
Instagram: @cybermemez
THIS IS THE WORST SECURITY DISASTER THIS YEAR, SO FAR

ATTACKS ARE SO STEALTHY

ONLY 9%

OF ATTACKS GENERATE ALERTS (MANDIANT)

YET, ON AVERAGE

+11,000 Alerts/Day

RECEIVED BY SECURITY TEAMS (FORRESTER)

AND WITH UP TO

130 Tools

IN USE BY SECURITY TEAMS (PALO ALTO NETWORKS)

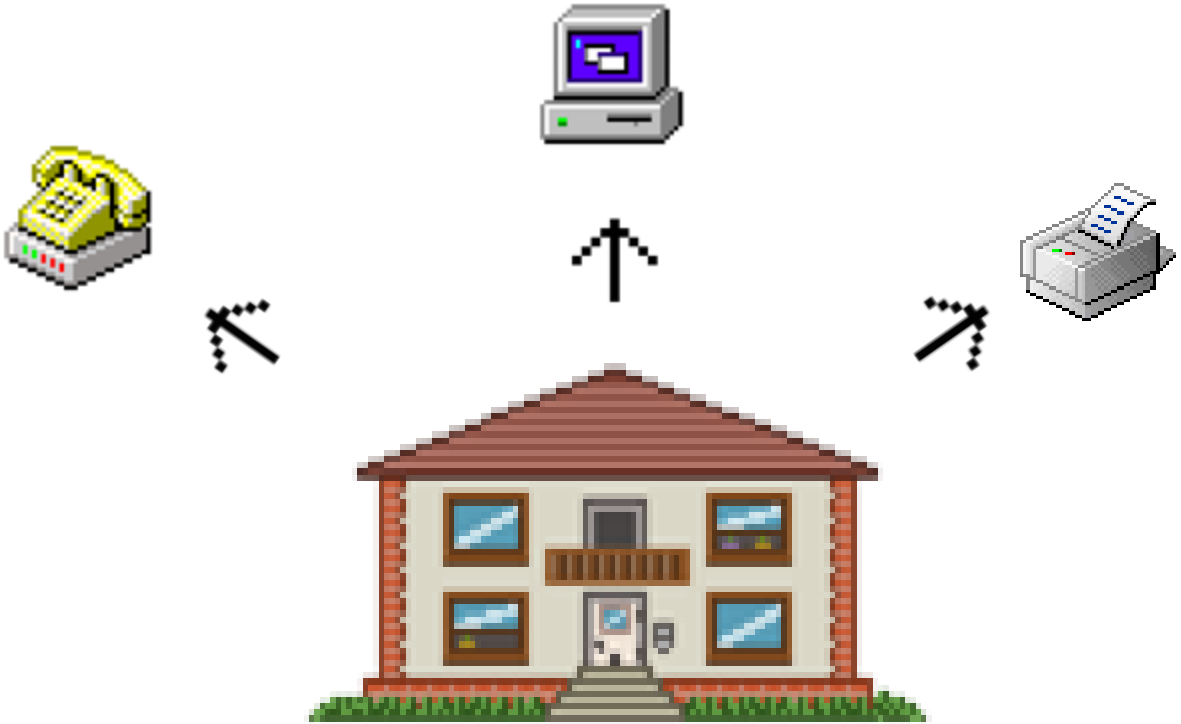
THERE IS NO DOUBT, ATTACK DETECTION IS

bloated & ineffective

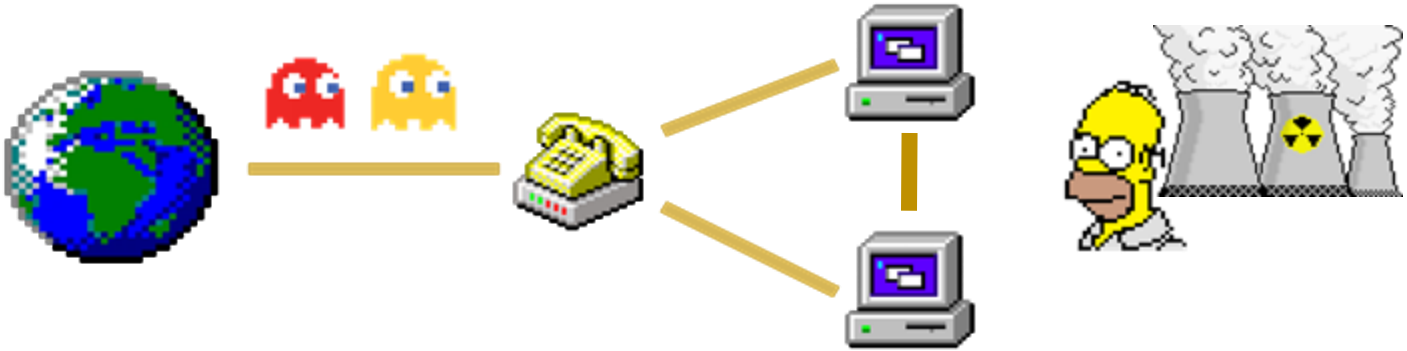
IN FACE OF RAPIDLY EVOLVING ADVERSARIES

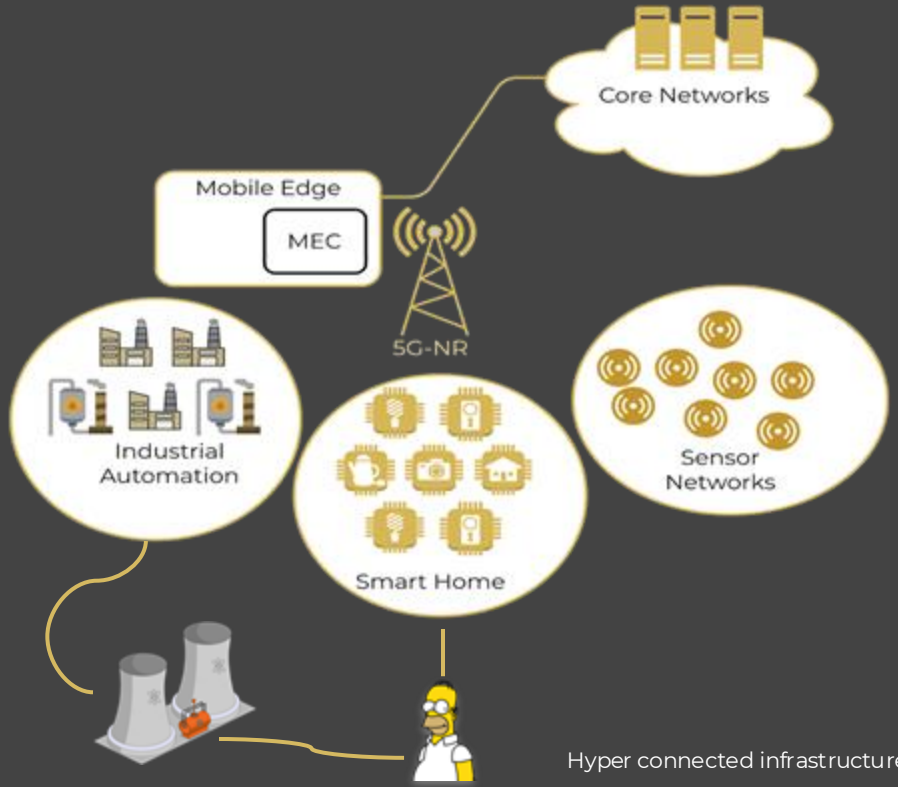
Our systems today are less secure than those of the

1970s

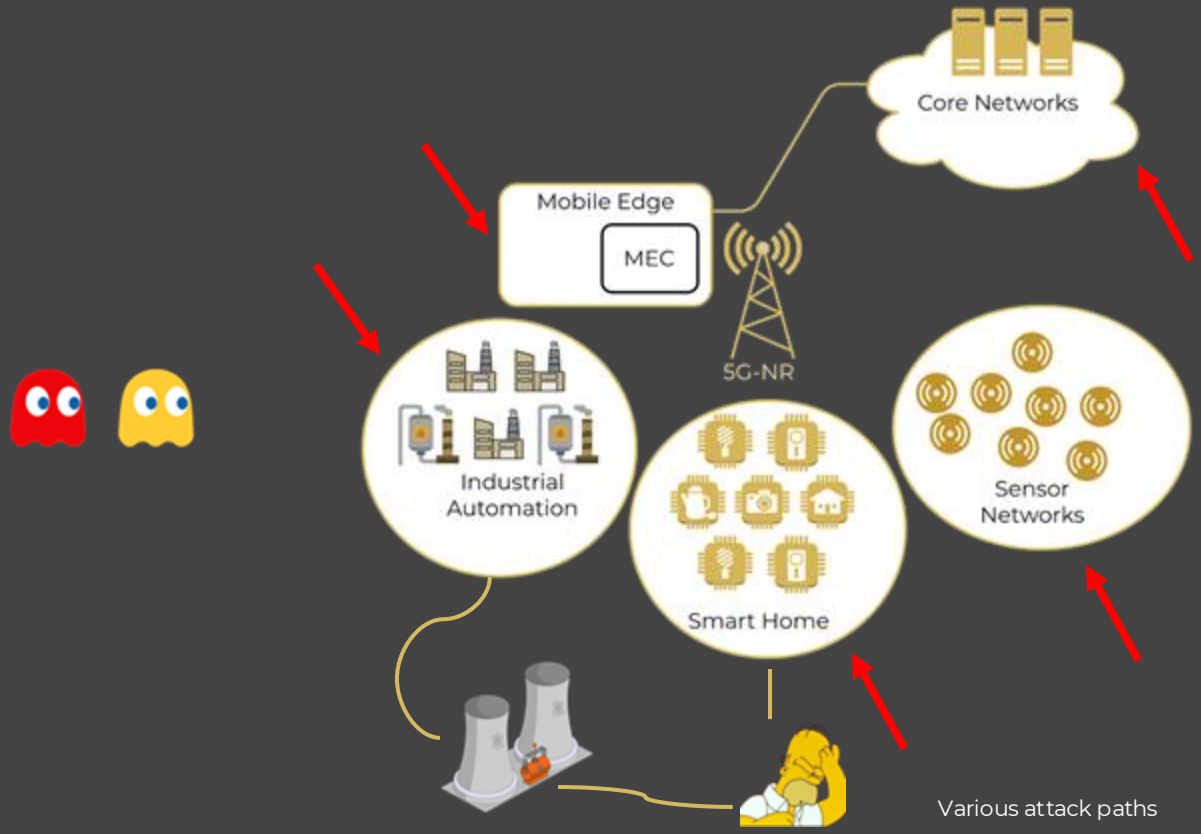



5G
AI
VR

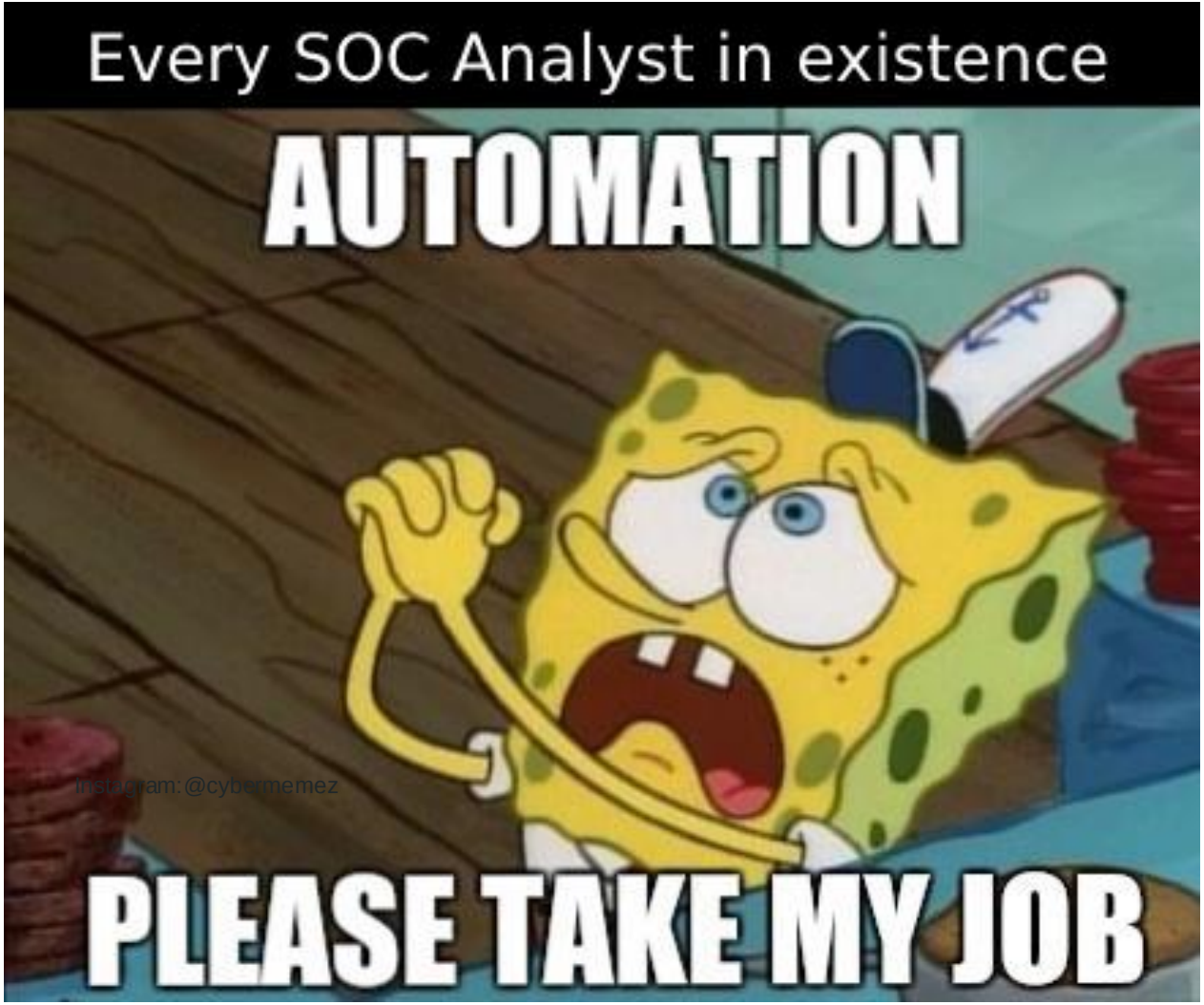




Hyper connected infrastructure



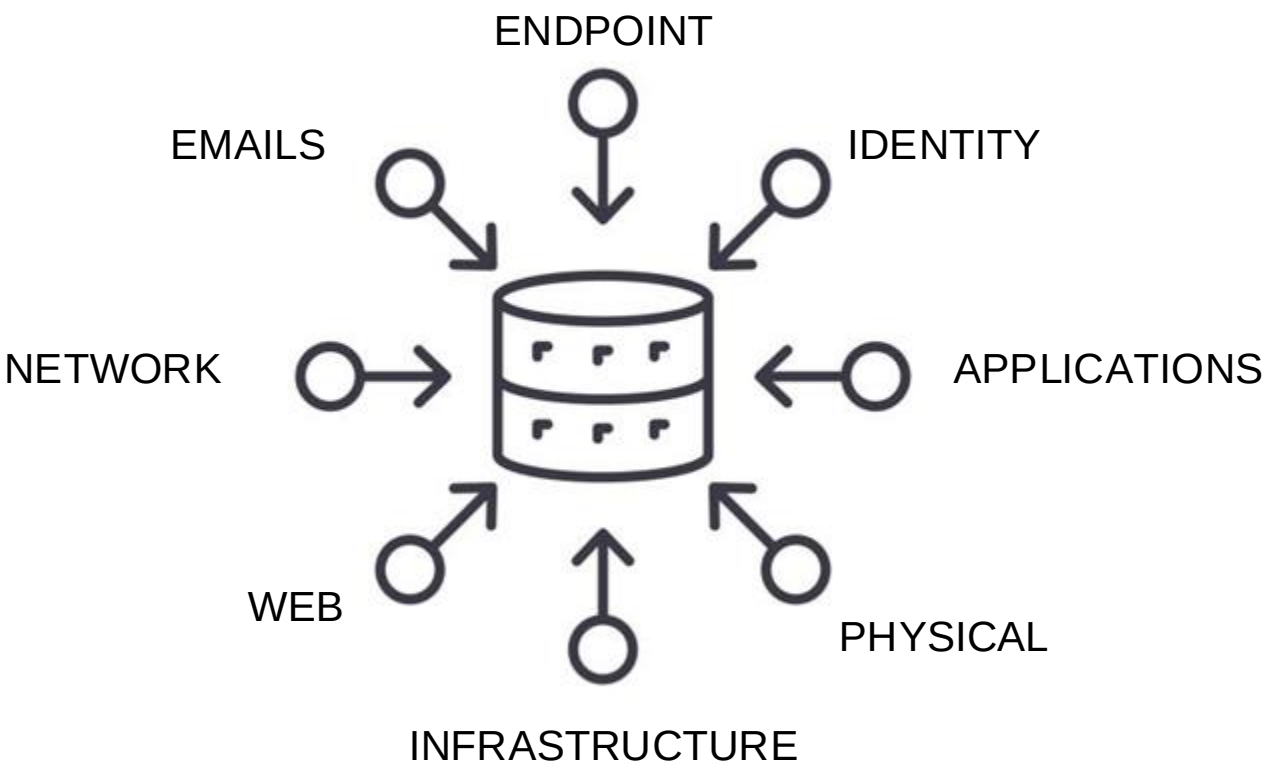
Various attack paths


Every SOC Analyst in existence
AUTOMATION
Instagram: @cybermemez
PLEASE TAKE MY JOB

Surveyed in 2017-2023 (by SANS), security experts blame

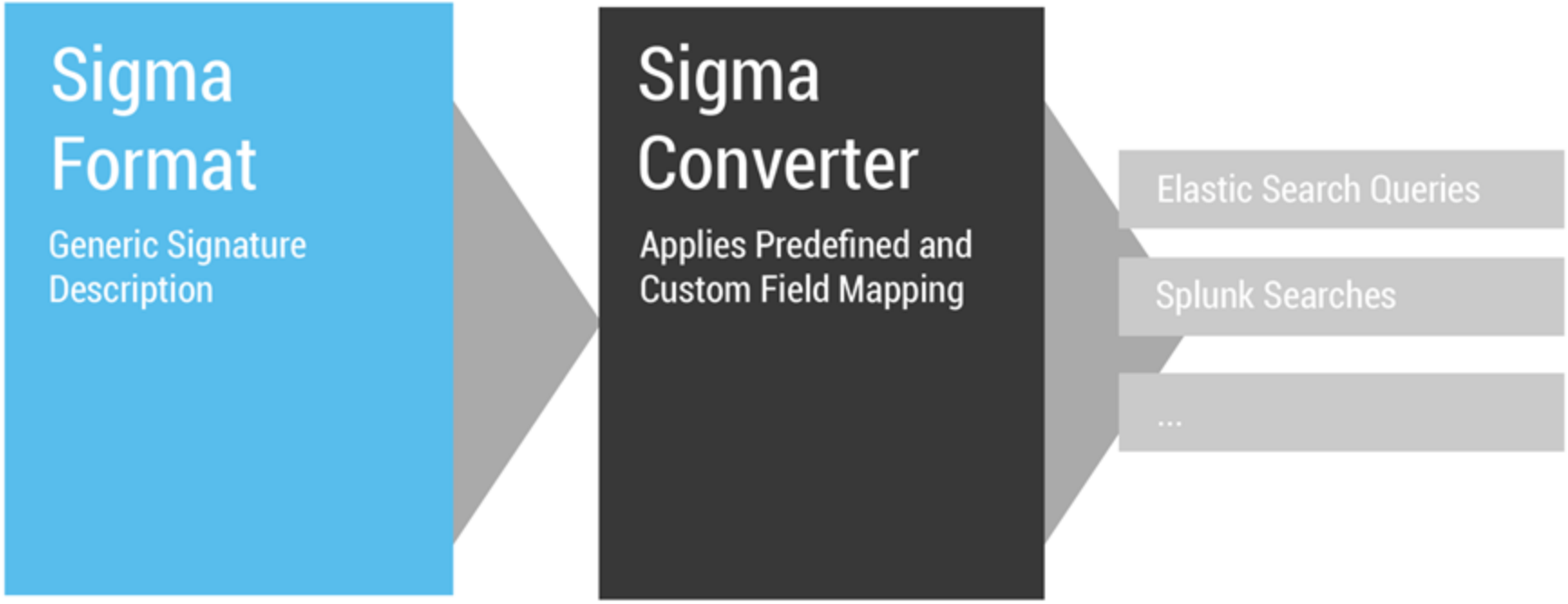
Lack of Correlation

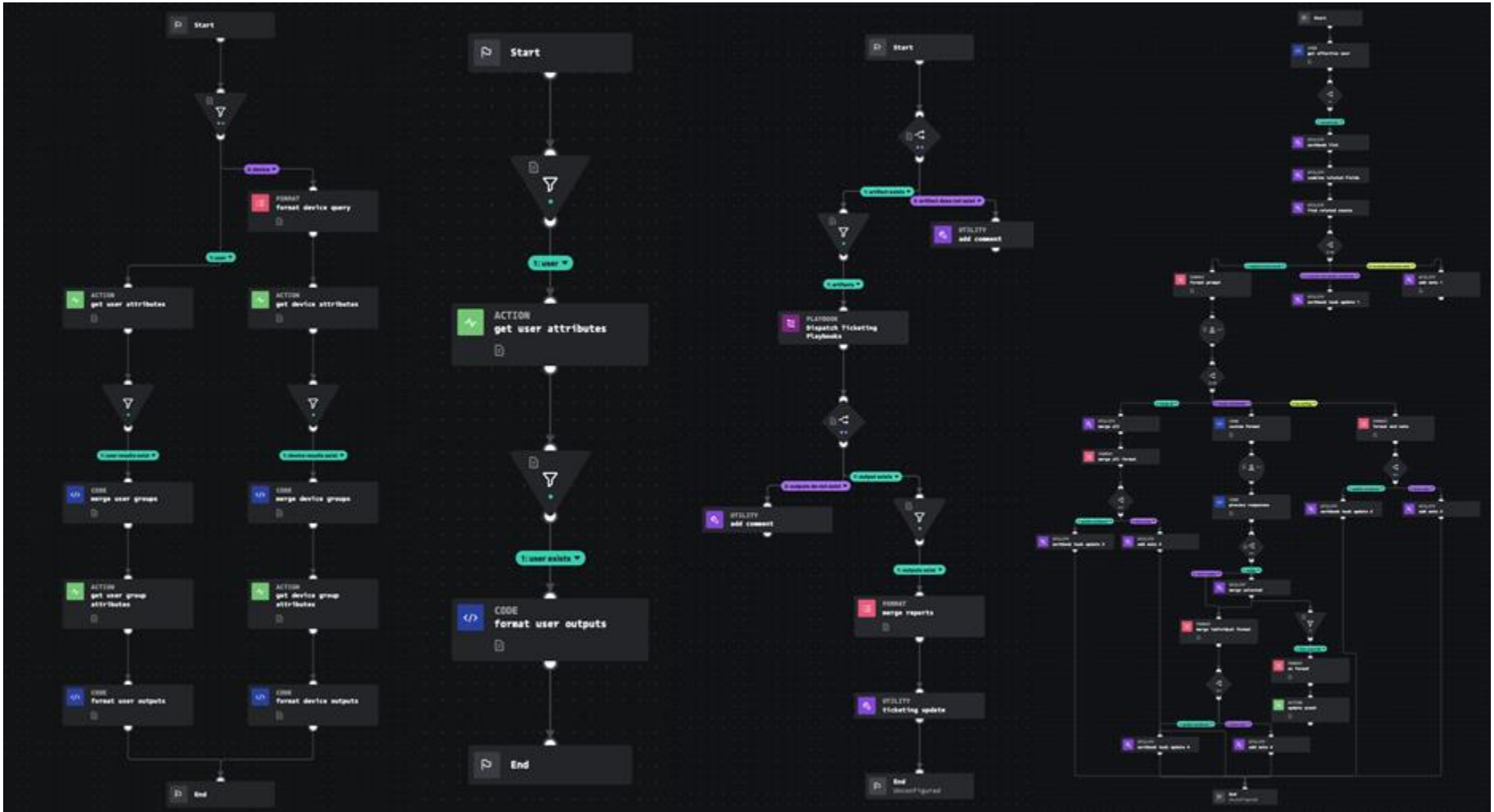
of seemingly disparate events. Hidden within, are attack kill chains.


ENDPOINT
EMAILS
IDENTITY
NETWORK
APPLICATIONS
WEB
PHYSICAL
INFRASTRUCTURE


Query

```yaml
title: Webshell ReGeorg Detection Via Web Logs
id: 2ea44a60-cfda-11ea-87d0-0242ac130003
status: test
description: >
    Certain strings in the uri_query field when combined with
    null referer and null user agent can indicate activity
    associated with the webshell ReGeorg.
references:
    - https://community.rsa.com/community/products/netwitness/blog/2019/02/19/
    - https://github.com/sensepost/reGeorg
author: Cian Heasley
date: 2020/08/04
modified: 2023/01/02
tags:
    - attack.persistence
    - attack.t1505.003
logsource:
    category: webserver
detection:
    selection:
        cs-uri-query|contains:
            - 'cmd=read'
            - 'connect&target'
            - 'cmd=connect'
            - 'cmd=disconnect'
            - 'cmd=forward'
    filter:
        cs-referer: null
        cs-user-agent: null
        cs-method: POST
    condition: selection and filter
falsepositives:
    - Web applications that use the same URL parameters as ReGeorg
fields:
```


Sigma Format
Generic Signature Description
Sigma Converter
Applies Predefined and Custom Field Mapping
Elastic Search Queries
Splunk Searches
...


Start
format device query
ACTION
get user attributes
ACTION
get device attributes
CODE
merge user groups
CODE
merge device groups
ACTION
get user group attributes
ACTION
get device group attributes
CODE
format user outputs
CODE
format device outputs
End
Start
ACTION
get user attributes
CODE
format user outputs
End
Start
UTILITY
add comment
PLAYBOOK
Dispatch Ticketing Playbooks
UTILITY
add comment
FORMAT
merge reports
UTILITY
ticketing update
End

```yaml
title: Webshell ReGeorg Dete
id: 2ea44a60-cfda-11ea-87d0-
status: test
description: >
    Certain strings in the u
    null referer and null us
    associated with the webs
references:
    - https://community.rsa.
    - https://github.com/sen
author: Cian Heasley
date: 2020/08/04
modified: 2023/01/02
tags:
    - attack.persistence
    - attack.t1505.003
```

ATT&CK

ID	Technique	Tactic
T1003.001	LSASS Memory	Credential Access
T1003	OS Credential Dumping	Credential Access

- Kill Chain Phase
- NIST
- CIS20
- CVE

Search

```
`sysmon` EventCode=10 TargetImage=*lsass.exe NOT (SourceUser="NT AUTHORITY\\*")
| stats count min(_time) as firstTime max(_time) as lastTime by dest, parent_process_
| rename TargetUser as user
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `windows_non_system_account_targeting_lsass_filter`
```

Tactics: the adversary's technical goals

Techniques: how the goals are achieved

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task			Binary Padding	Network Sniffing			Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
	Local Job Scheduling		Bypass User Account Control		Bash History	Application Window Discovery		Clipboard Data		Data Encrypted	Defacement
External Remote Services	LSASS Driver		Extra Window Memory Injection		Brute Force		Distributed Component Object Model	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Trap		Process Injection		Credential Dumping	Browser Bookmark Discovery			Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Replication Through Removable Media	AppleScript	DLL Search Order Hijacking			Credentials in Files		Exploitation of Remote Services	Data from Local System			Endpoint Denial of Service
	CMSTP	Image File Execution Options Injection			Credentials in Registry	Domain Trust Discovery		Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Firmware Corruption
Spearphishing Attachment	Command-Line Interface	Plist Modification			Exploitation for Credential Access	File and Directory Discovery	Logon Scripts				Inhibit System Recovery
Spearphishing Link	Compiled HTML File	Valid Accounts				Network Service Scanning	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Alternative Protocol	Network Denial of Service
Spearphishing via Service	Control Panel Items	Accessibility Features		BITS Jobs	Forced Authentication	Network Share Discovery	Pass the Ticket	Data Staged	Data Obfuscation		Resource Hijacking
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Hooking	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Fronting	Exfiltration Over Physical Medium	Runtime Data Manipulation
Trusted Relationship	Execution through API	AppInit DLLs		Code Signing	Input Capture	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms		Service Stop
Valid Accounts	Execution through Module Load	Application Shimming		Compiled HTML File	Input Prompt	Permission Groups Discovery	Remote Services	Man in the Browser		Scheduled Transfer	Stored Data Manipulation
		Dylib Hijacking		Component Firmware	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture	Fallback Channels		Transmitted Data Manipulation
	Exploitation for Client Execution	File System Permissions Weakness		Component Object Model Hijacking	Keychain	Query Registry		Video Capture	Multiband Communication		
		Hooking		Control Panel Items	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Shared Webroot		Multi-hop Proxy		
	Graphical User Interface	Launch Daemon			Password Filter DLL	Security Software Discovery	SSH Hijacking		Multilayer Encryption		
	InstallUtil	New Service				System Information Discovery	Taint Shared Content		Multi-Stage Channels		
	Mshta										
	PowerShell										
	Regsvcs/Regasm	Ser									
	Regsvr32										
	Rundll32										
	Scripting										
	Service Execution	bash_profile a									
	Signed Binary Proxy Execution	Account Man									
		Authenticator									
	Signed Script Proxy Execution	BITS J									
		Boot									
	Source	Browser Ext									
	Space after Filename	Change D File Associ									
	Third-party Software										
	Trusted Developer Utilities	Component									
	User Execution	Component Model Hij									
	Windows Management Instrumentation	Create Ac									
	Windows Remote Management	External Remo									
		Hidden Files an									
	XSL Script Processing	Hypervisor									
		Kernel Modules and Extensions									

Procedures: Specific technique implementation

Spearphishing Attachment

Procedure Examples

Name	Description
APT12	APT12 has sent emails with malicious Microsoft Office documents and PDFs attached. [88] [89]
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits. [62]

Phishing: Spearphishing Attachment

Other sub-techniques of Phishing (3)

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

ID: T1566.001
Sub-technique of: T1566
Tactic: Initial Access
Platforms: Linux, Windows, macOS
CAPEC ID: CAPEC-163
Contributors: Philip Winther
Version: 2.2
Created: 02 March 2020
Last Modified: 18 October 2021

Version Permalink

Detection

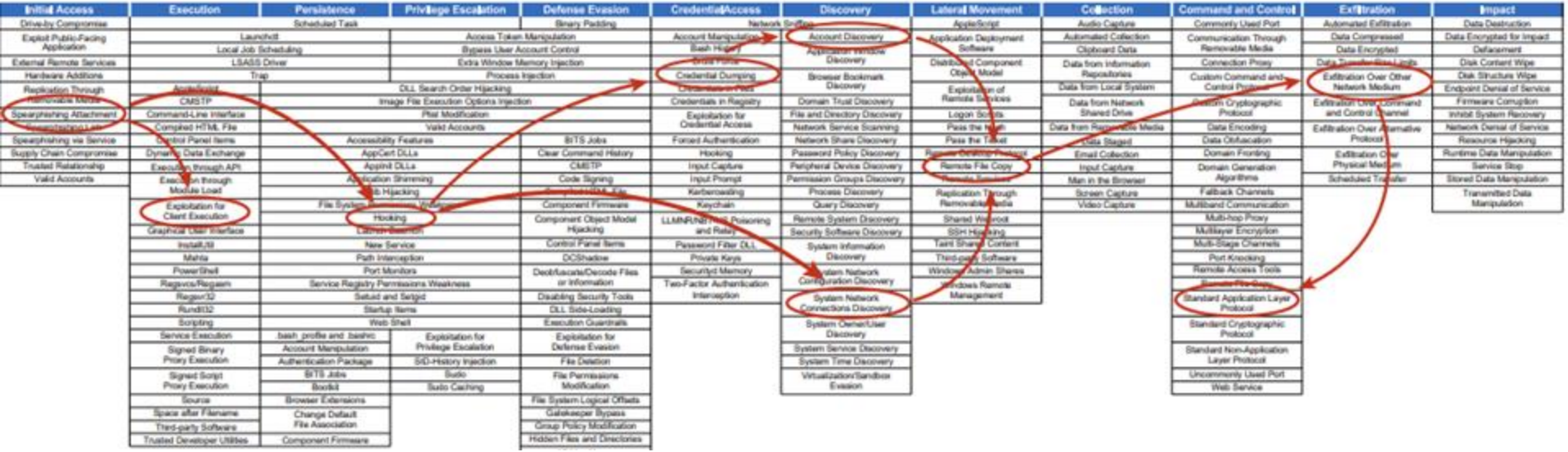
ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor for third-party appli based on DKIM+SPF or hea on the email server or on th
DS0022	File	File Creation	Monitor for newly construct

Mitigations

ID	Mitigation	Description
M1049	Antivirus/Antimalware	Anti-virus can also automatically qu
M1031	Network Intrusion Prevention	Network intrusion prevention system

Procedure Examples

ID	Name	Description
G0018	admin@338	admin@338 has sent emails with malicious Microsoft Office documents a
S0331	Agent Tesla	The primary delivered mechaism for Agent Tesla is through email phishing
G0130	Ajax Security Team	Ajax Security Team has used personalized spearphishing attachments.[3]
G0138	Andariel	Andariel has conducted spearphishing campaigns that included malicious
S0622	AppleSeed	AppleSeed has been distributed to victims through malicious e-mail attach
G0099	APT-C-36	APT-C-36 has used spearphishing emails with password protected RAR at


Initial Access
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
Scheduled Task
Launchctl
Local Job Scheduling
LSASS Driver
Trap
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scripting
Service Execution
Signed Binary Proxy Execution
Signed Script Proxy Execution
Source
Space after Filename
Third-party Software
Trusted Developer Utilities
Persistence
Privilege Escalation
Defense Evasion
Binary Padding
Access Token Manipulation
Bypass User Account Control
Extra Window Memory Injection
Process Injection
DLL Search Order Hijacking
Image File Execution Options Injection
Plist Modification
Valid Accounts
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bootkit
Hooking
New Service
Path Interception
Port Monitors
Service Registry Permissions Weakness
Setuid and Setgid
Startup Items
Web Shell
bash_profile and .bashrc
Account Manipulation
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Exploitation for Privilege Escalation
SID-History Injection
Sudo
Sudo Caching
BITS Jobs
Clear Command History
CMSTP
Code Signing
Component Firmware
Component Object Model Hijacking
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Side-Loading
Execution Guardrails
Exploitation for Defense Evasion
File Deletion
File Permissions Modification
File System Logical Offsets
Gatekeeper Bypass
Group Policy Modification
Hidden Files and Directories
Credential Access
Network Sniffing
Account Manipulation
Credential Dumping
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
Keychain
Password Filter DLL
Private Keys
Securityd Memory
Two-Factor Authentication Interception
Discovery
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion
Lateral Movement
AppleScript
Application Deployment Software
Distributed Component Object Model
Exploitation of Remote Services
Logon Scripts
Pass the Hash
Pass the Ticket
Remote File Copy
Replication Through Removable Media
Shared Webroot
SSH Hijacking
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management
Collection
Audio Capture
Automated Collection
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture
Command and Control
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Domain Generation Algorithms
Fallback Channels
Multiband Communication
Multi-hop Proxy
Multilayer Encryption
Multi-Stage Channels
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service
Exfiltration
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Other Network Medium
Exfiltration Over Command and Control Channel
Exfiltration Over Alternative Protocol
Exfiltration Over Physical Medium
Scheduled Transfer
Impact
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Runtime Data Manipulation
Service Stop
Stored Data Manipulation
Transmitted Data Manipulation

Attack Flow

Problem

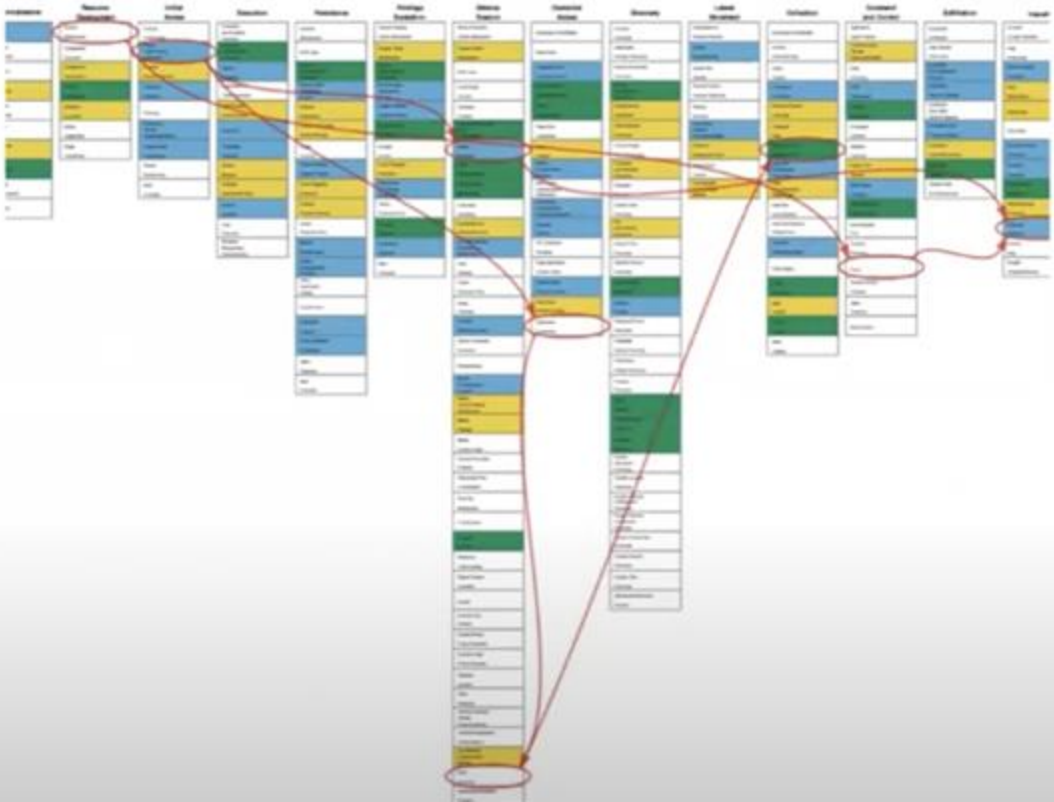
Defenders **often track adversary behaviors atomically**, focusing on one specific action at a time. This makes it **harder to understand adversary attacks and to build effective defenses** against those attacks.

Solution

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

Impact

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



Recipe to correlate data and find attacks

Spot the killchain progression!

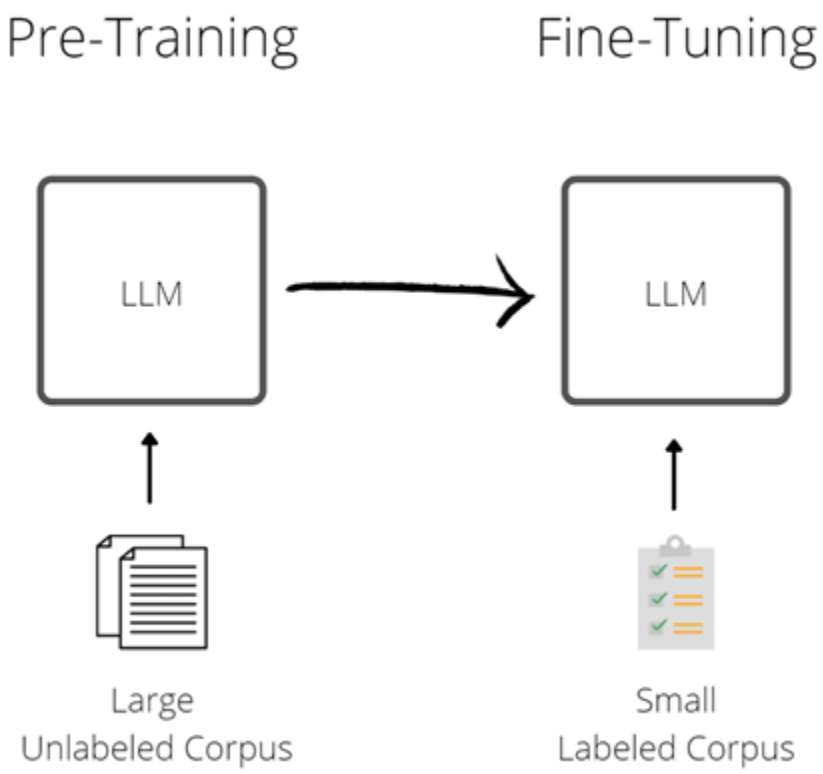
- Step 1: Get relevant MITRE ATT&CK Techniques & Tactics for all events

- Step 2: Find events that are highly related to each other and form MITRE ATT&CK FLOWS
  - Consider all events attributes similarity and time
  - Consider all entities attributes similarity
    - PS: Similarity is not shared characteristics but SIMILAR ones

Step 1: Get relevant MITRE ATT&CK Techniques & Tactics for ALL events

Step 1: ATT&CK Technique Detector Model

Classify Events with their relevant ATT&CK Techniques


Pre-Training
Fine-Tuning
LLM
LLM
Large
Unlabeled Corpus
Small
Labeled Corpus

aws Services Ohio

Amazon SageMaker > Endpoints > seshat-technique-endpoint

seshat-technique-endpoint

De

Endpoint summary

Name	Status
seshat-technique-endpoint	InService

AWS CloudShell

Actions

us-east-2

```
[cloudshell-user@ip-10-6-84-19 ~]$ python3 test_tech
rundll32 adds the Registry Run key
['T1218']
[cloudshell-user@ip-10-6-84-19 ~]$ vim test_tech

[cloudshell-user@ip-10-6-84-19 ~]$ python3 test_tech

email spam alert
['T1566']
[cloudshell-user@ip-10-6-84-19 ~]$
```

us-east-2

```
[cloudshell-user@ip-10-6-84-19 ~]$ python3 test_tech
rundll32 adds the Registry Run key
['T1218']
[cloudshell-user@ip-10-6-84-19 ~]$ vim test_tech
[cloudshell-user@ip-10-6-84-19 ~]$ python3 test_tech
email spam alert
['T1566']
```

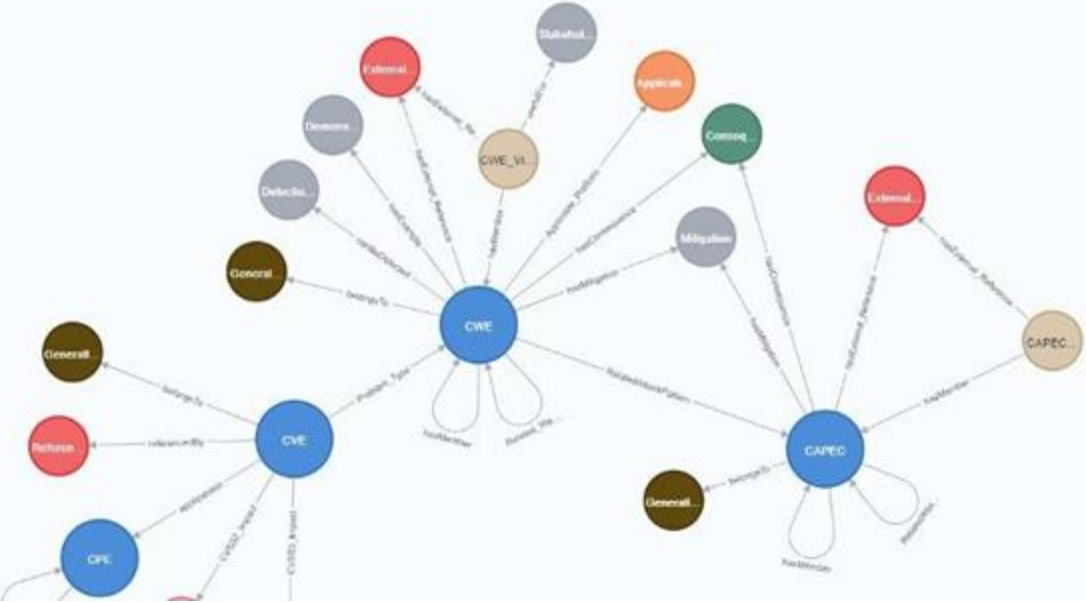
```
[cloudshell-user@ip-10-6-84-19 ~]$ python3 test_tech
os windows microsoft windows remote desktop web access cross site scripting attempt post request
['T1189']
```

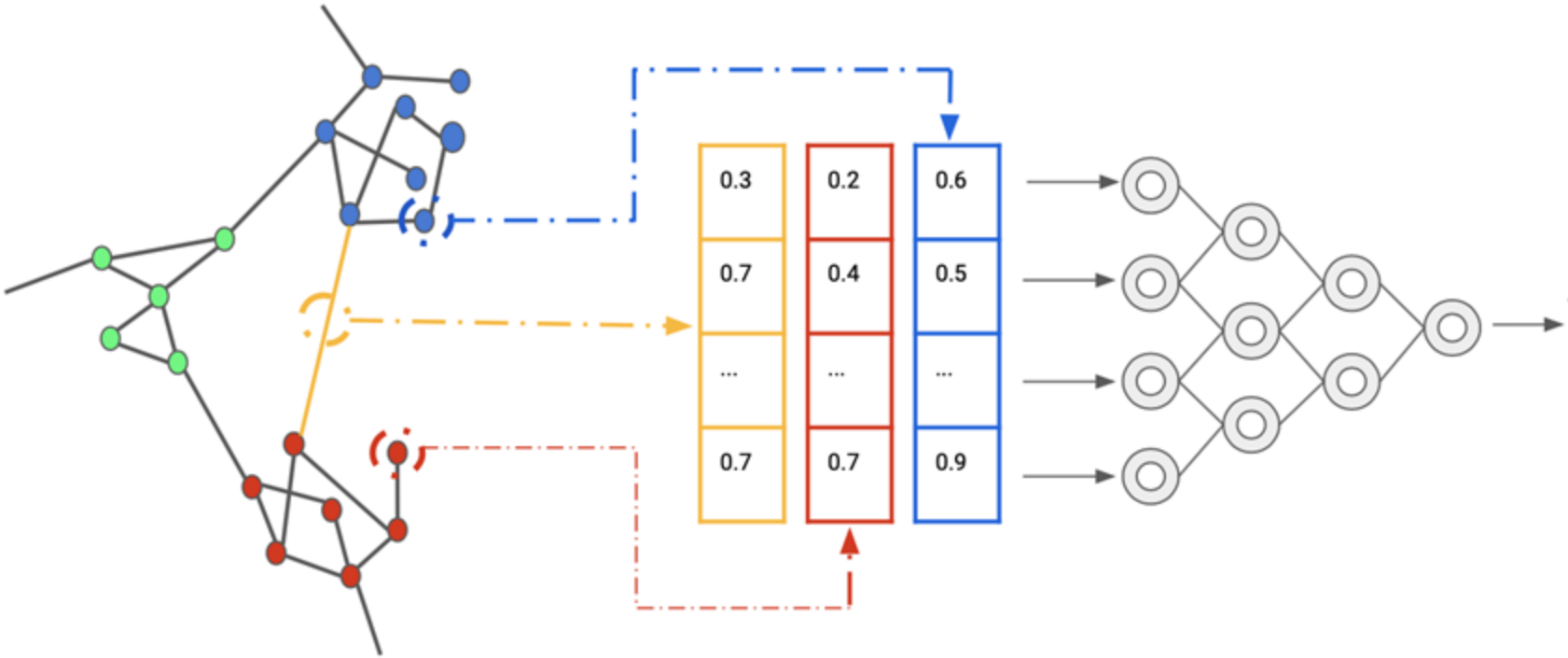
```
first account password change for local user
['T1098']
```

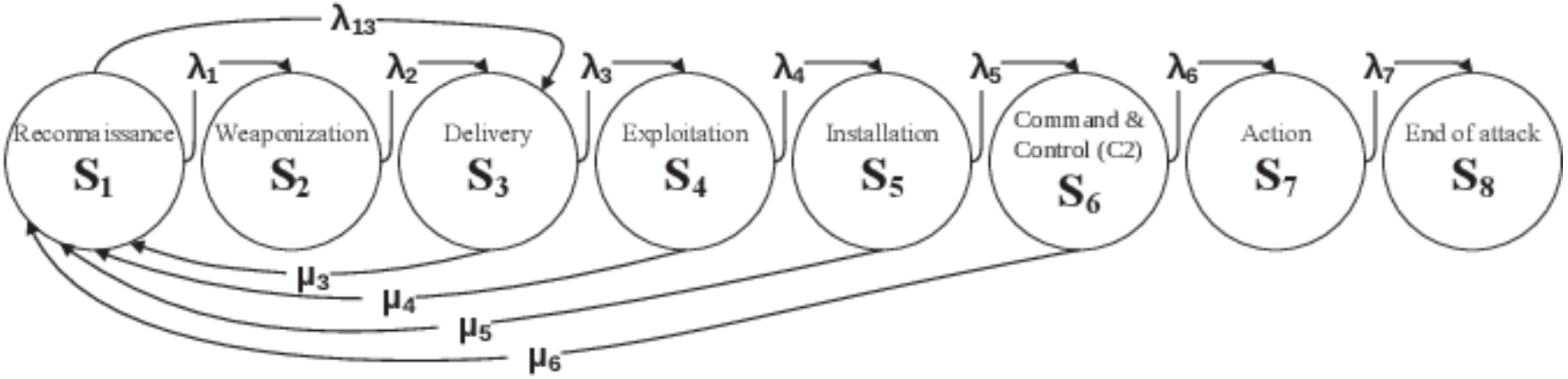
Step 2: Find events that are highly related to each other and form MITRE ATT&CK FLOWS

Step 2: MITRE ATT&CK FLOW Detector Model

Cluster events that are related.
Find event clusters that are causal and sequential.


CWE
CVE
CPE
CAPEC
CAPEC
CWE_VI...
Stakeho...
External
Applicab...
Consequ...
Detection...
Mitigation
External...
General
General...
General...
Relation...
CAPEC...


0.3
0.7
...
0.7
0.2
0.4
...
0.7
0.6
0.5
...
0.9


λ13
λ1
λ2
λ3
λ4
λ5
λ6
λ7
Reconnaissance
S1
Weaponization
S2
Delivery
S3
Exploitation
S4
Installation
S5
Command &
Control (C2)
S6
Action
S7
End of attack
S8
μ3
μ4
μ5
μ6

aws Services Ohio ezsec.org

Amazon SageMaker > Endpoints > seshat-correlation-gpu-endpoint

seshat-correlation-gpu-endpoint

Delete

Endpoint summary

Name	Status
seshat-correlation-gpu-endpoint	InService

AWS CloudShell Actions

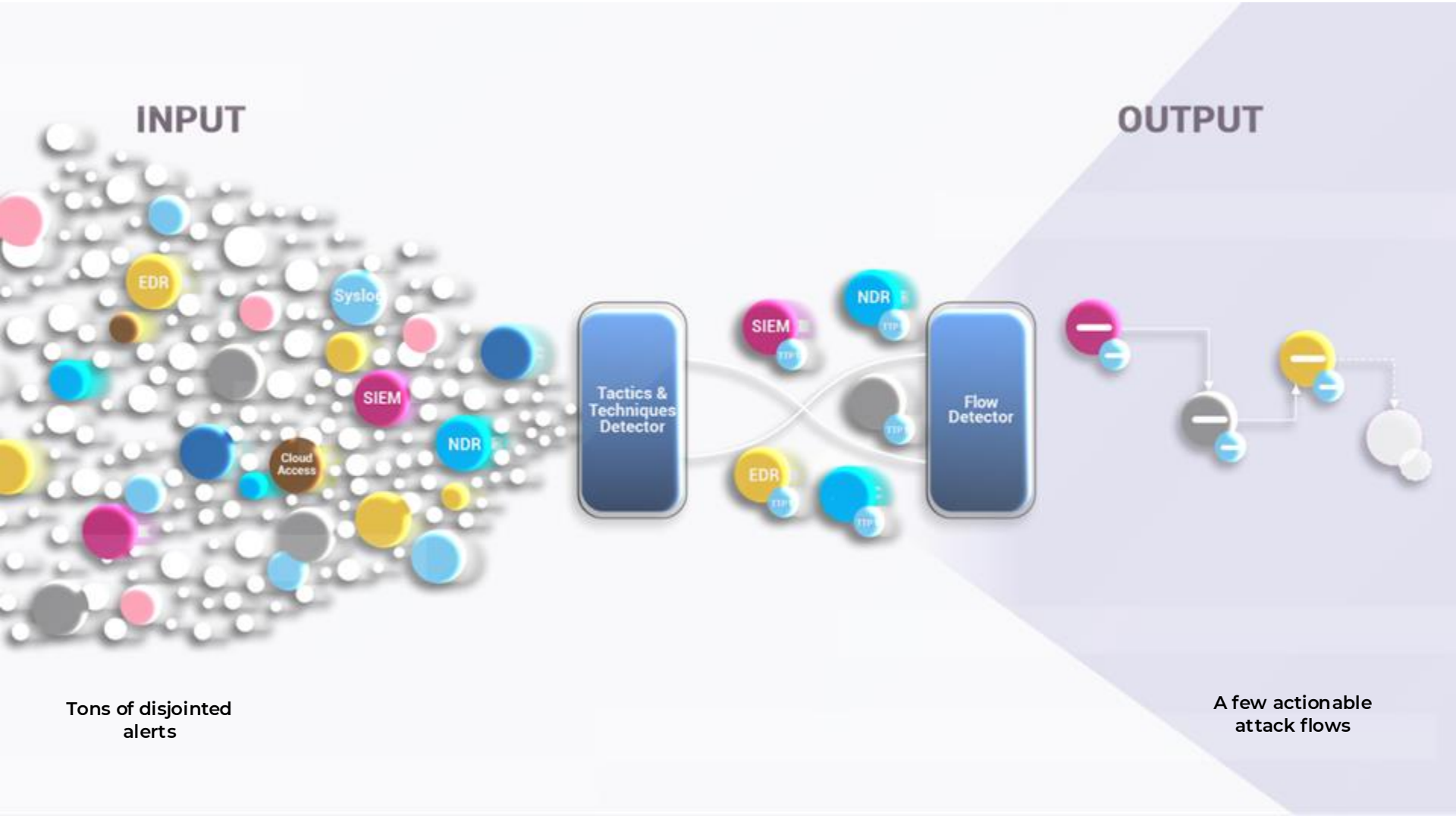
us-east-2

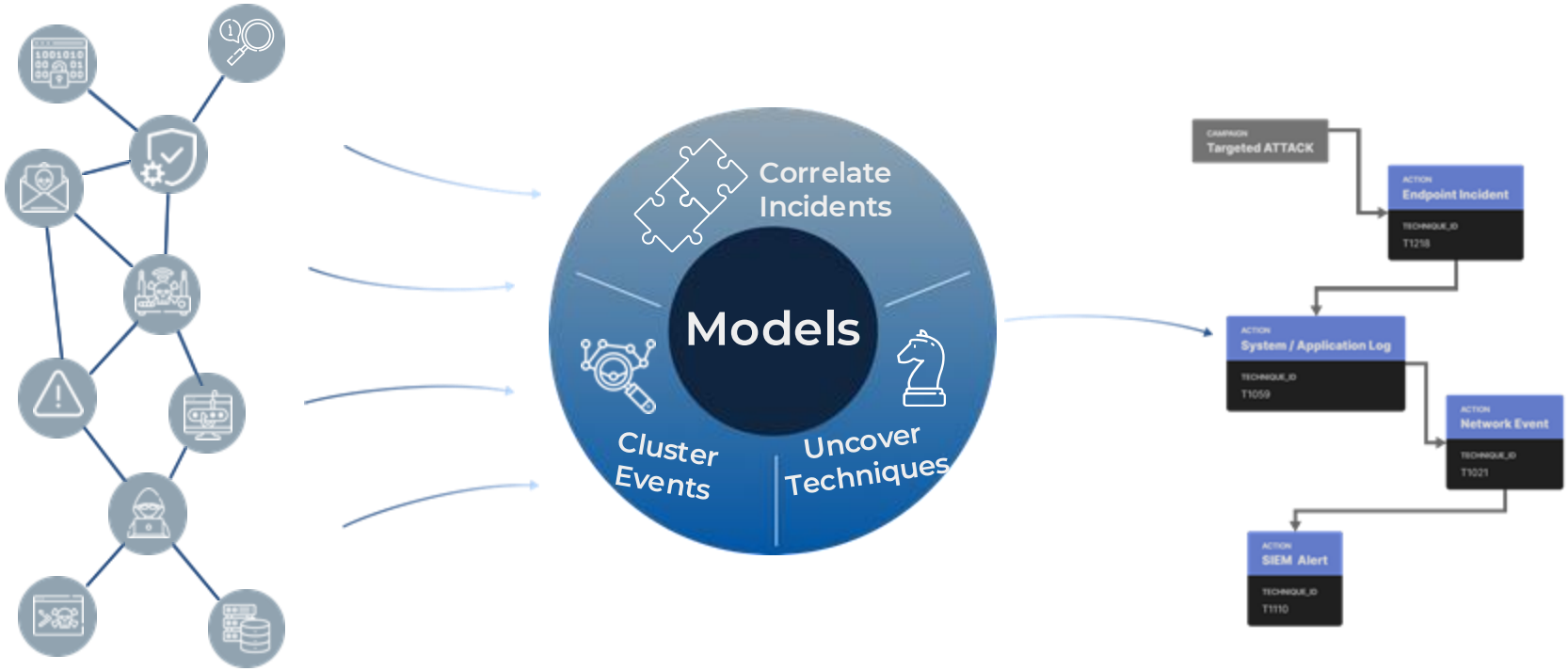
```
02/14/2018-17:18:34.400632  [**] [1:2014384:8] ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second
Read json file
flows:
[[0, 3, 13, 16, 19, 20, 21, 25, 28, 32, 35, 38, 39, 42, 43, 47, 48, 51, 52, 55, 58, 61, 62, 65, 67, 71, 72, 7
5, 78, 81, 85, 88, 90, 93, 94, 97, 98, 101, 104, 107, 108, 111, 112, 115, 116, 119, 120, 123, 124, 127, 129,
132, 133, 136, 137, 140, 146, 149, 151, 154, 157, 160, 161, 164, 168, 171, 174, 177, 179, 182, 185, 188, 191,
 194, 196, 199, 200, 203, 205, 208, 209, 212, 213, 216, 217, 220, 221, 224, 227, 230, 231, 234, 235, 238, 239
, 243, 244, 247, 248, 251, 252, 255, 256, 259, 261, 264, 267, 270, 271, 274, 278, 281, 282, 285, 290, 293, 29
4, 297, 298, 301, 302, 305, 309, 312, 313, 316, 318, 321, 322, 325, 328, 331, 334, 337, 338, 341, 343, 346, 3
47, 350, 352, 355, 356, 359, 360, 363, 364, 367, 368, 371, 373, 376, 378, 381, 384, 387, 391, 394, 395, 398,
399, 402, 405, 408, 409, 412, 413, 416, 417, 420, 421, 424, 425, 428, 429, 432, 433, 436, 437, 440, 441, 442,
 445, 447, 450, 453, 454, 457, 459, 462, 464, 471, 474, 475, 478, 479, 480, 481, 484, 488, 491, 492, 494, 497
 498, 501] [26, 27, 76, 145, 150, 165, 166, 167, 173, 178, 195, 204, 260, 275, 307, 317, 327, 342, 377, 388
```

```
flows:
[[0, 3, 13, 16, 19, 20, 21, 25, 28, 32, 35, 38, 39, 42, 43, 47, 48, 51, 52, 55, 58, 61, 62, 65, 67, 71, 72, 7
5, 78, 81, 85, 88, 90, 93, 94, 97, 98, 101, 104, 107, 108, 111, 112, 115, 116, 119, 120, 123, 124, 127, 129,
132, 133, 136, 137, 140, 146, 149, 151, 154, 157, 160, 161, 164, 168, 171, 174, 177, 179, 182, 185, 188, 191,
 194, 196, 199, 200, 203, 205, 208, 209, 212, 213, 216, 217, 220, 221, 224, 227, 230, 231, 234, 235, 238, 239
, 243, 244, 247, 248, 251, 252, 255, 256, 259, 261, 264, 267, 270, 271, 274, 278, 281, 282, 285, 290, 293, 29
4, 297, 298, 301, 302, 305, 309, 312, 313, 316, 318, 321, 322, 325, 328, 331, 334, 337, 338, 341, 343, 346, 3
47, 350, 352, 355, 356, 359, 360, 363, 364, 367, 368, 371, 373, 376, 378, 381, 384, 387, 391, 394, 395, 398,
399, 402, 405, 408, 409, 412, 413, 416, 417, 420, 421, 424, 425, 428, 429, 432, 433, 436, 437, 440, 441, 442,
 445, 447, 450, 453, 454, 457, 459, 462, 464, 471, 474, 475, 478, 479, 480, 481, 484, 488, 491, 492, 494, 497
, 498, 501], [26, 27, 76, 145, 150, 165, 166, 167, 173, 178, 195, 204, 260, 275, 307, 317, 327, 342, 377, 388
, 390, 403, 404, 458, 467, 470, 486, 487, 503], [190, 326, 332, 372], [24, 46, 70], [4, 5, 6, 7, 8, 9, 10, 12
, 31, 56, 57, 66, 77, 82, 83, 84, 89, 102, 103, 128, 143, 172, 189, 225, 226, 306, 308, 333, 351, 389, 446, 4
63, 493, 502], [1, 2, 14, 15, 17, 18, 22, 23, 29, 30, 36, 37, 40, 41, 44, 45, 49, 50, 53, 54, 59, 60, 63, 64,
 68, 69, 73, 74, 79, 80, 86, 87, 91, 92, 95, 96, 99, 100, 105, 106, 109, 110, 113, 114, 117, 118, 121, 122, 1
25, 126, 130, 131, 134, 135, 138, 139, 147, 148, 152, 153, 158, 159, 162, 163, 169, 170, 175, 176, 180, 181,
186, 187, 192, 193, 197, 198, 201, 202, 206, 207, 210, 211, 214, 215, 218, 219, 222, 223, 228, 229, 232, 233,
 236, 237, 241, 242, 245, 246, 249, 250, 253, 254, 257, 258, 262, 263, 268, 269, 272, 273, 279, 280, 283, 284
, 291, 292, 295, 296, 299, 300, 303, 304, 310, 311, 314, 315, 319, 320, 323, 324, 329, 330, 335, 336, 339, 34
0, 344, 345, 348, 349, 353, 354, 357, 358, 361, 362, 365, 366, 369, 370, 374, 375, 379, 380, 385, 386, 392, 3
93, 396, 397, 400, 401, 406, 407, 410, 411, 414, 415, 418, 419, 422, 423, 426, 427, 430, 431, 434, 435, 438,
439, 443, 444, 448, 449, 455, 456, 460, 461, 465, 466, 472, 473, 476, 477, 482, 483, 489, 490, 495, 496, 499,
 500], [33, 34, 141, 142, 144, 155, 156, 183, 184, 265, 266, 276, 277, 286, 287, 288, 289, 382, 383, 451, 452
, 468, 469, 485], [11, 240]]
```

```
num of alerts:
2460
```

```
206
29
4
3
34
202
24
2
```


INPUT
OUTPUT
EDR
Syslog
SIEM
NDR
Cloud Access
Tactics & Techniques Detector
SIEM
NDR
EDR
Flow Detector
Tons of disjointed alerts
A few actionable attack flows


Correlate Incidents
Models
Cluster Events
Uncover Techniques
CAMPAIGN
Targeted ATTACK
ACTION
Endpoint Incident
TECHNIQUE_ID
T1218
ACTION
System / Application Log
TECHNIQUE_ID
T1059
ACTION
Network Event
TECHNIQUE_ID
T1021
ACTION
SIEM Alert
TECHNIQUE_ID
T1110

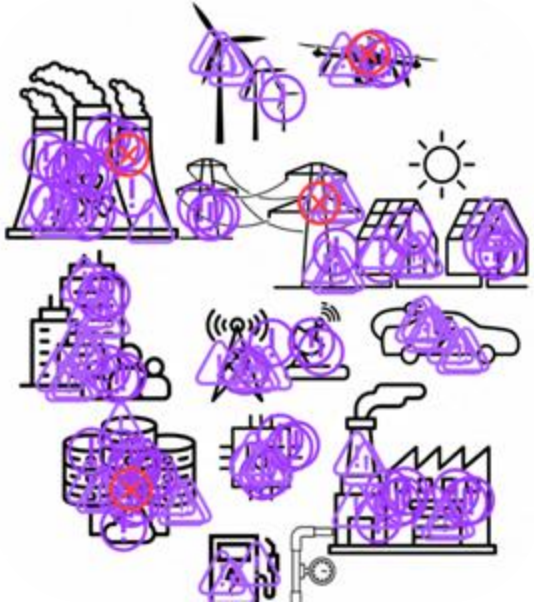
```
        "priority": 3
    }
}, {
    "instalertid": 29732,
    "time": 1499460957.94943,
    "src": "172.16.0.1",
    "dst": "192.168.10.50",
    "name": " ET SCAN Potential SSH Scan ",
    "tech": [],
    "other_attributes_dict": {
        "sid": "2001219",
        "port": 22,
        "functionality": "missile guiding"
    }
}, {
    "instalertid": 29733,
```

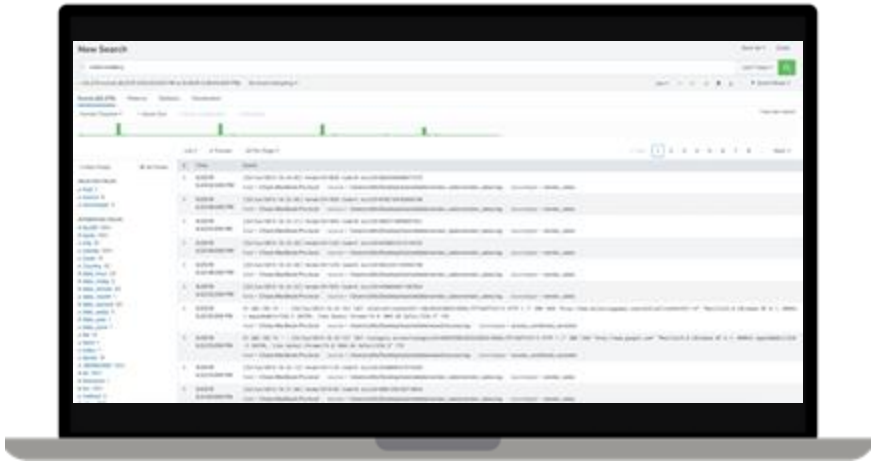
```
}, {
    "src": "192.168.10.19",
    "dst": "91.189.92.152",
    "tech": ["T1041", "T1205"],
    "name": " ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management ",
    "count": 15,
    "other_attributes_dict": {
        "priority": 3,
        "sid": "2013504"
    },
    "start_time": 1499358653.040222,
    "finish_time": 1499358654.458431,
    "alert_id": 55,
    "avg_time": 1499358653.7493265,
    "tac": [10, 3, 5, 11],
    "stage": [4, 2, 2, 4]
}, {
```

[
{"cluster_id":0,
"cluster_aggalertids":[0,1,30,31,36,42,43,57,59,65,75,77,81,83,84,85,86,87,88,90,92,93,95],
"cluster_starttime":1499097405.578172,
"cluster_endtime":1499097405.580233,
"cluster_aggalertsinstcounts":[4,2,8,20,13,4,1,16,18,4,14,11,4,6,13,8,8,1,1,4,4,2,4],
"cluster_avgtimes":[1499097405.5792027,1499097425.7034035,1499099184.7989412,1499100875.252252,
1499104739.010302,1499100357.800194,1499100357.801032,1499107218.832768,1499107410.0530129,
1499108778.7735716,1499114361.9800575,1499117370.1295162,1499116062.1096836,1499120105.754424,
1499122817.2008875,1499120745.391366,1499121099.9550355,1499121447.229496,1499121447.229975,
1499122165.814289,1499124785.835641,1499124785.8357886,1499183837.3205105],
"cluster_srcips":["192.168.10.9","192.168.10.3","192.168.10.16","192.168.10.17"],
"cluster_dstips":["192.168.10.3","192.168.10.1","23.194.182.93"],
"cluster_techs":["T1071","T1021","T1071","T1071","T1071","T1071","T1071","T1071","T1071","T1082","T1071",
"T1071","T1071","T1071","T1071","T1071","T1071","T1071","T1071","T1071","T1071","T1071","T1071"],
"cluster_tacs":[8,11,7],
"cluster_stages":[3,4],
"all_int_ips":["U0001","U0002","U0004","U0003"]
},

```
[
    {
        "Flow_id": 0,
        "cluster_ids": [
            0,
            1,
            2,
            3,
            4,
            5,
            6,
            7,
            8,
            9,
            10,
            11,
            12
        ]
    },
    {
        "Flow_id": 1,
```

	EFFICIENT SCALABLE FLEXIBLE COMPUTING	EASY TO ADAPT AND MAINTAIN	CORRELATE WELL KNOWN COORDINATED ATTACKS	CORRELATE NEW ATTACKS W NUANCES	STANDALONE INTEROPERABLE
ANALYTICAL STORIES	✗	✗	✓	✗	✗
THREAT CHAINING RULES	✗	✗	✓	✗	✗
CLUSTERING	✓	✓	✓	✓	✓




New Search

EX: FP Ticket

Ticket ID: FP-20230807-001

Date/Time: 2023-08-07 10:15 AM

Reporter: John Doe

Source/System: Intrusion Detection System (IDS)

Alert ID: IDS-12345

Description: The alert was triggered due to a legitimate internal vulnerability scan.

Resolution: Added the internal scan server's IP address to the whitelist.

Comments: Confirmed with the network team about the scheduled scan.

Status: Closed

EX: Lone Incident Ticket

Ticket ID: INC-20230807-002

Incident Type: Phishing

Severity: High

Description: Multiple employees reported receiving a suspicious email with a malicious link.

Affected Systems/Users: 15 employees in the Sales department.

Investigation Details: Analyzed the email headers and confirmed it was a phishing attempt. Identified the IP address of the sender.

Mitigation Actions: Blocked the sender's IP address, removed the email from all mailboxes, and informed affected employees to avoid clicking on the link.

Comments: No users reported clicking the link.

Status: Resolved

EX: Attack Story Ticket

Attack Type: Ransomware

Description: A ransomware attack was detected on the company's main file server, encrypting sensitive data and demanding a ransom in Bitcoin.

Indicators of Compromise (IOCs):

- MD5 Hash: d41d8cd98f00b204e9800998ecf8427e
- IP Address: 192.168.1.100
- File Name: ransomware.exe

Affected Systems/Users: Main file server and 100+ users.

Timeline of Events:

- 2023-08-07 01:00 PM: Unusual file activity detected on the main file server.
- 2023-08-07 01:15 PM: Ransom note discovered.
- 2023-08-07 02:00 PM: Incident reported to the security team.

EX: Attack Story Ticket - cont’d

Investigation Details: Conducted forensic analysis on the affected server, identified the entry point as a phishing email opened by an employee.

Mitigation Actions: Isolated the affected server, restored data from backups, applied patches, and conducted a security awareness training for employees.

Lessons Learned: Importance of regular backups and employee training on phishing.

Comments: Coordinated with law enforcement for further investigation.

Status: Closed

EX: Coordinated attack ticket


```
"AttackType": "Advanced Persistent Threat (APT)",

"Severity": "Critical",

"Description": "A sophisticated and prolonged APT attack targeting the company’s financial systems, involving multiple tactics and spanning over a month.",

"IndicatorsOfCompromise": {

  "IPAddresses": ["192.168.100.100", "192.168.200.200"],

  "Domains": ["badactor.com", "malicious.net"],

  "FileNames": ["trojan1.exe", "ransomware_v2.dll"],

  "Hashes": {

    "MD5": "e99a18c428cb38d5f260853678922e03",

    "SHA-256": "5d41402abc4b2a76b9719d911017c592"
```

EX: Coordinated attack ticket - cont’d


```
"AffectedSystemsUsers": [
  "Financial systems servers",     "150+ user workstations",     "Executive email accounts"],
"TimelineOfEvents": [    {
    "DateTime": "2023-07-01 09:00 AM",
    "Event": "Initial breach via spear-phishing email to CFO.",
    "Source": "Email gateway logs",
    "Tactic": "Social engineering"},   {
    "DateTime": "2023-07-03 10:15 AM",
    "Event": "Installation of a remote access trojan (RAT).",
    "Source": "Endpoint detection and response (EDR) system",
    "Tactic": "Malware deployment"
  },
```

EX: Coordinated attack ticket - cont’d - cont’d

"DateTime": "2023-07-05 11:30 AM",

"Event": "Unauthorized access to financial database.",

"Source": "Database access logs",

"Tactic": "Credential theft"

"DateTime": "2023-07-10 02:45 PM",

"Event": "Data exfiltration detected.",

"Source": "Network traffic analysis",

"Tactic": "Data exfiltration"

"DateTime": "2023-07-12 04:00 PM",

"Event": "Lateral movement within the network.",

"Source": "Internal network monitoring",

"Tactic": "Lateral movement"

EX: Coordinated attack ticket - cont’d - cont’d - cont’d

"DateTime": "2023-07-15 09:30 AM",

"Event": "Use of legitimate tools for persistence.",

"Source": "System process logs",

"Tactic": "Living off the land"

"DateTime": "2023-07-18 01:00 PM",

"Event": "Credential dumping from a compromised admin account.",

"Source": "Security information and event management (SIEM) system",

"Tactic": "Credential access"

"DateTime": "2023-07-20 11:15 AM",

"Event": "Privilege escalation on multiple servers.",

"Source": "Server audit logs",

"Tactic": "Privilege escalation"

EX: Coordinated attack ticket - cont’d - cont’d - cont’d - cont’d

"DateTime": "2023-07-25 03:00 PM",

"Event": "Ransomware deployed on user workstations.", "Source": "Endpoint antivirus alerts", "Tactic": "Ransomware"

"DateTime": "2023-07-27 05:30 PM",

"Event": "Communication with C2 server.", "Source": "Firewall logs", "Tactic": "Command and control"

"DateTime": "2023-07-30 08:45 AM",

"Event": "Secondary data exfiltration attempt.", "Source": "Data Loss Prevention system", "Tactic": "Data exfiltration"

"DateTime": "2023-08-05 10:00 AM",

"Event": "Discovery of additional backdoors.", "Source": "Comprehensive system scan", "Tactic": "Persistence"

"InvestigationDetails": "Conducted thorough forensic analysis on affected systems. Collaborated with third-party cybersecurity experts to analyze malware samples. Monitored network traffic for unusual patterns and identified exfiltration channels. Performed a detailed review of all logs from multiple sources, including SIEM, EDR, firewall, and DLP systems.",

EX: Coordinated attack ticket -cont’d-cont’d-cont’d-cont’d-cont’d

"MitigationActions": ["Isolated compromised systems and removed malware.", "Reset passwords for all affected accounts.", "Implemented multi-factor authentication (MFA) for critical systems.", "Applied security patches and updated firewall rules.", "Conducted a company-wide security awareness training.",

"LessonsLearned": [

"Importance of regular phishing awareness training.",

"Need for robust endpoint protection and monitoring.",

"Criticality of having a comprehensive incident response plan."

],

"Comments": "Incident report and recommendations shared with executive management and board of directors. Ongoing monitoring to ensure no further malicious activity.",

"Status": "Closed"

}

https://gist.github.com/ezzeldinadel/

https://hf.co/chat/assistant/6692eb85ce7a1a25328ab049

https://hf.co/chat/assistant/6692ea1980d075bf4961ecdf