FORTINET®

Technologické nástroje účinnej kybernetickej obrany

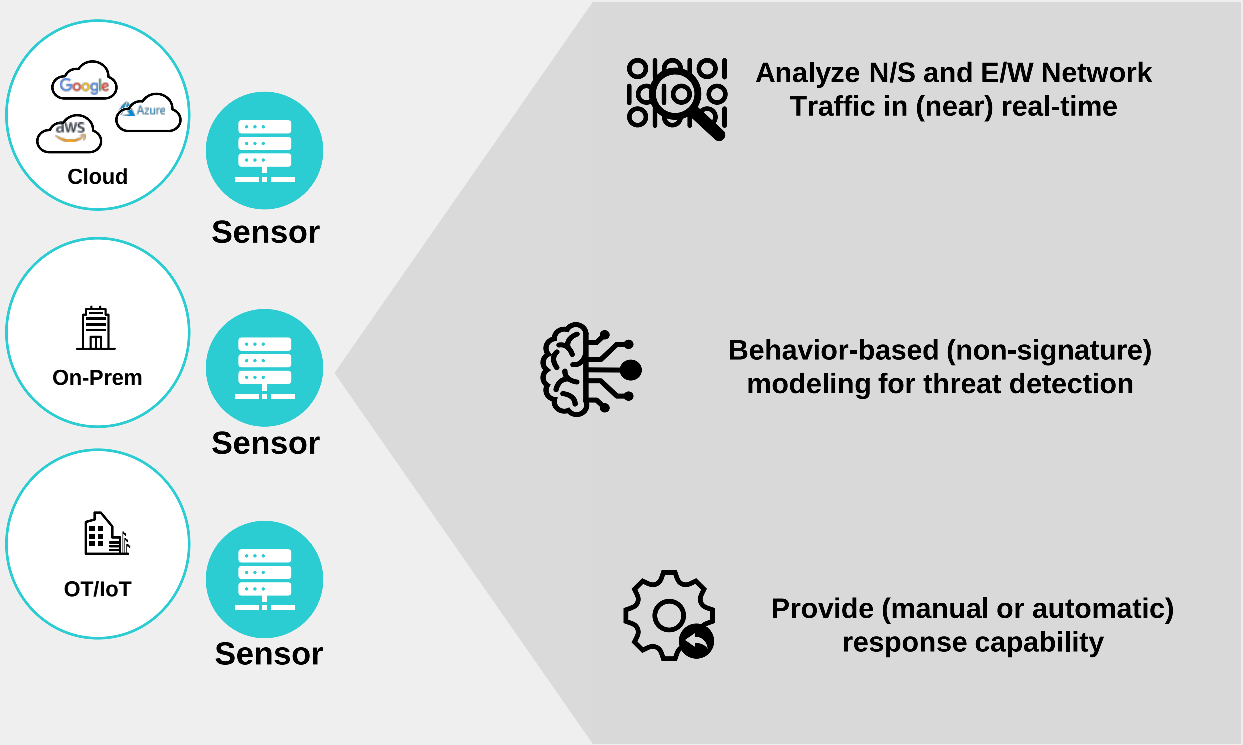
FortiNDR & FortiNDR Cloud

Juraj Belko

Systems Engineering

What is Network Detection and Response

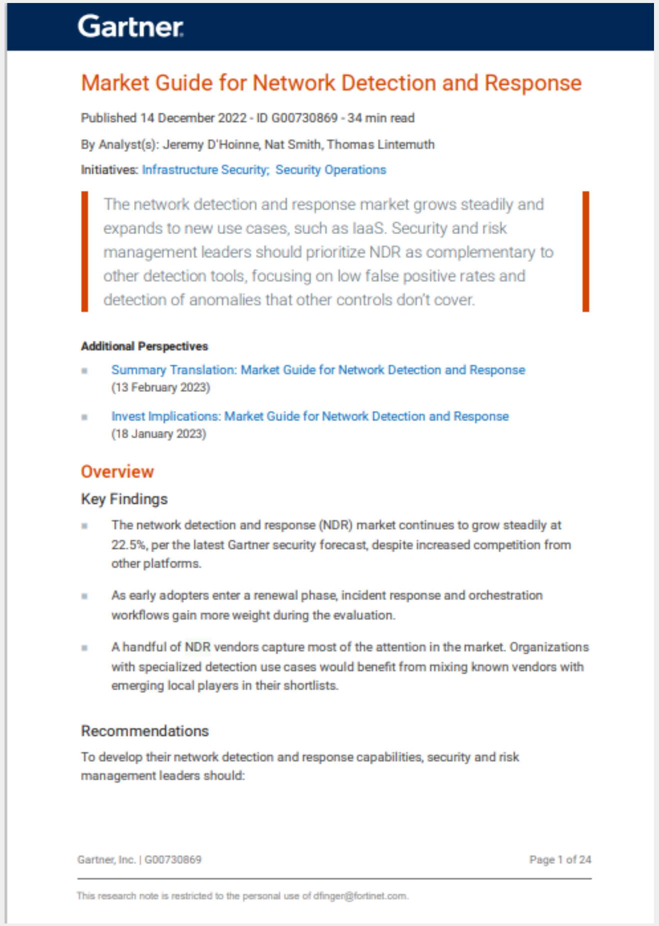
Detect **abnormal** system behaviors by applying behavioral analytics to **network traffic** data.



Analyze N/S and E/W Network Traffic in (near) real-time

Behavior-based (non-signature) modeling for threat detection

Provide (manual or automatic) response capability



Gartner

Market Guide for Network Detection and Response

Published 14 December 2022 - ID G00730869 - 34 min read

By Analyst(s): Jeremy D'Hoinne, Nat Smith, Thomas Lintemuth

Initiatives: Infrastructure Security; Security Operations

> The network detection and response market grows steadily and expands to new use cases, such as IaaS. Security and risk management leaders should prioritize NDR as complementary to other detection tools, focusing on low false positive rates and detection of anomalies that other controls don't cover.

Additional Perspectives

- Summary Translation: Market Guide for Network Detection and Response (13 February 2023)
- Invest Implications: Market Guide for Network Detection and Response (18 January 2023)

Overview

Key Findings

- The network detection and response (NDR) market continues to grow steadily at 22.5%, per the latest Gartner security forecast, despite increased competition from other platforms.
- As early adopters enter a renewal phase, incident response and orchestration workflows gain more weight during the evaluation.
- A handful of NDR vendors capture most of the attention in the market. Organizations with specialized detection use cases would benefit from mixing known vendors with emerging local players in their shortlists.

Recommendations

To develop their network detection and response capabilities, security and risk management leaders should:

Gartner, Inc. | G00730869 Page 1 of 24

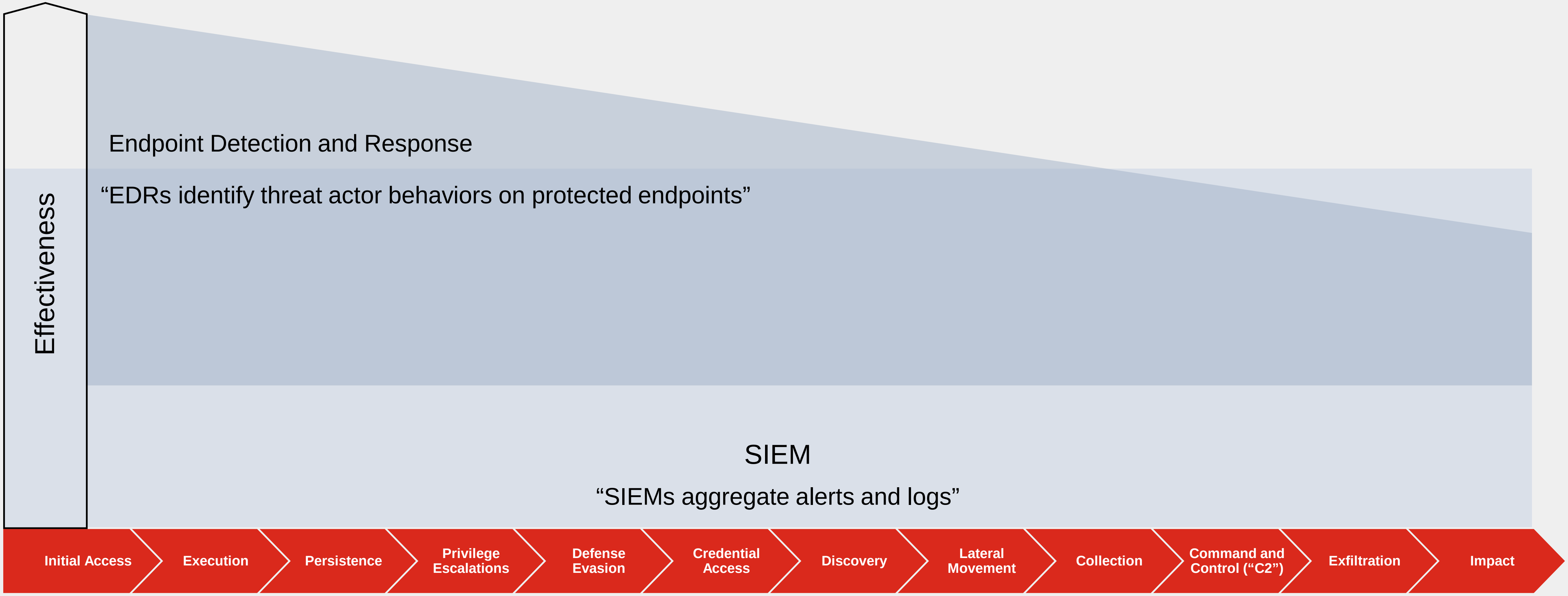
This research note is restricted to the personal use of dfinger@fortinet.com.

Complements other technologies, which trigger alerts primarily based on rules and signatures, by building heuristic **models of normal behavior and spotting anomalies**

The SOC Visibility Gap

But gaps remain

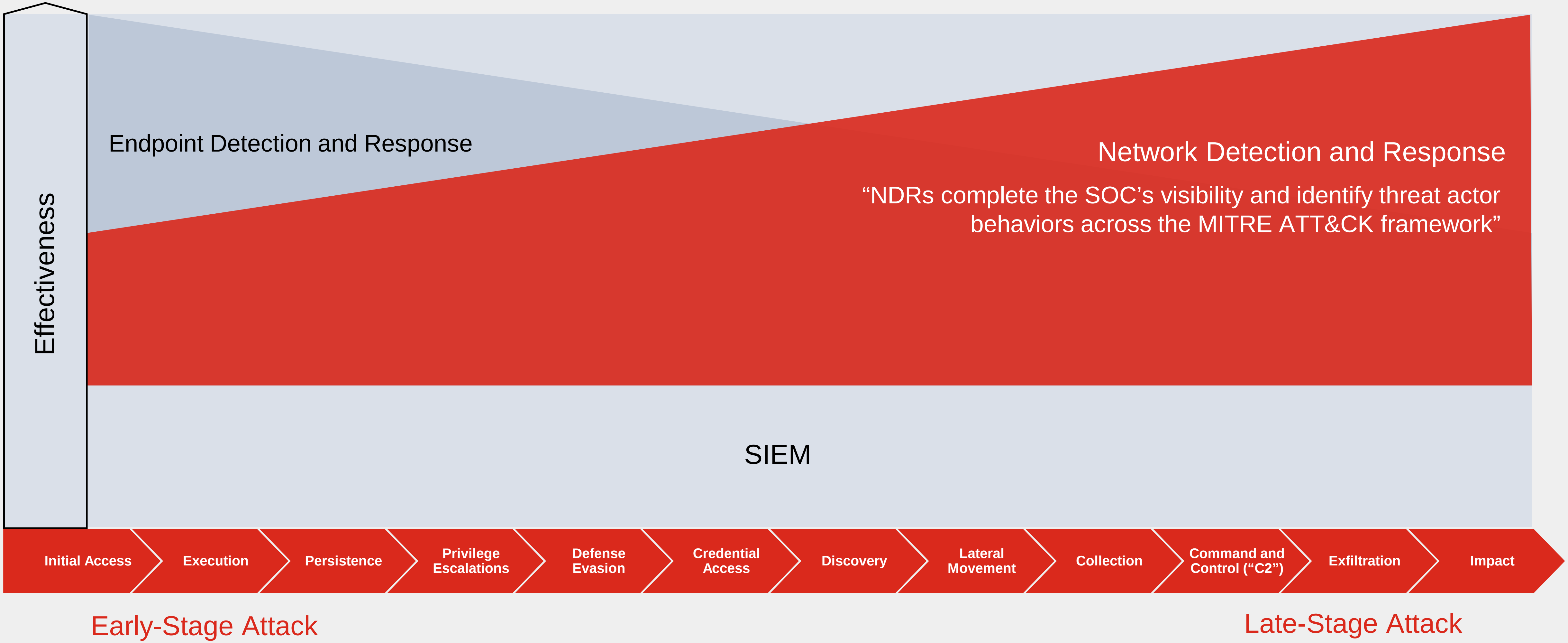
- ✓ Visibility of all devices: **managed**, **unmanaged**, including **IoT and WFH**
- ✓ Visibility of all networks: **on-prem**, **private**, or **public cloud**
- ✓ Visibility of all traffic/protocols: **North-South-East-West**



Early-Stage Attack

Late-Stage Attack

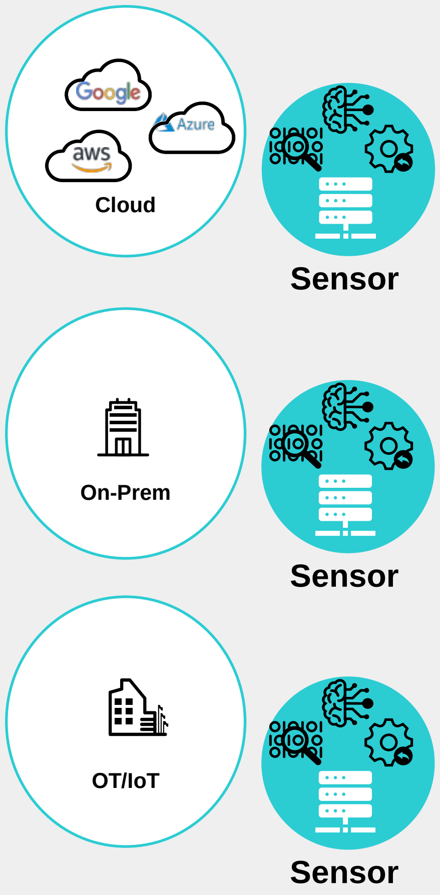
Full SOC Visibility Achieved

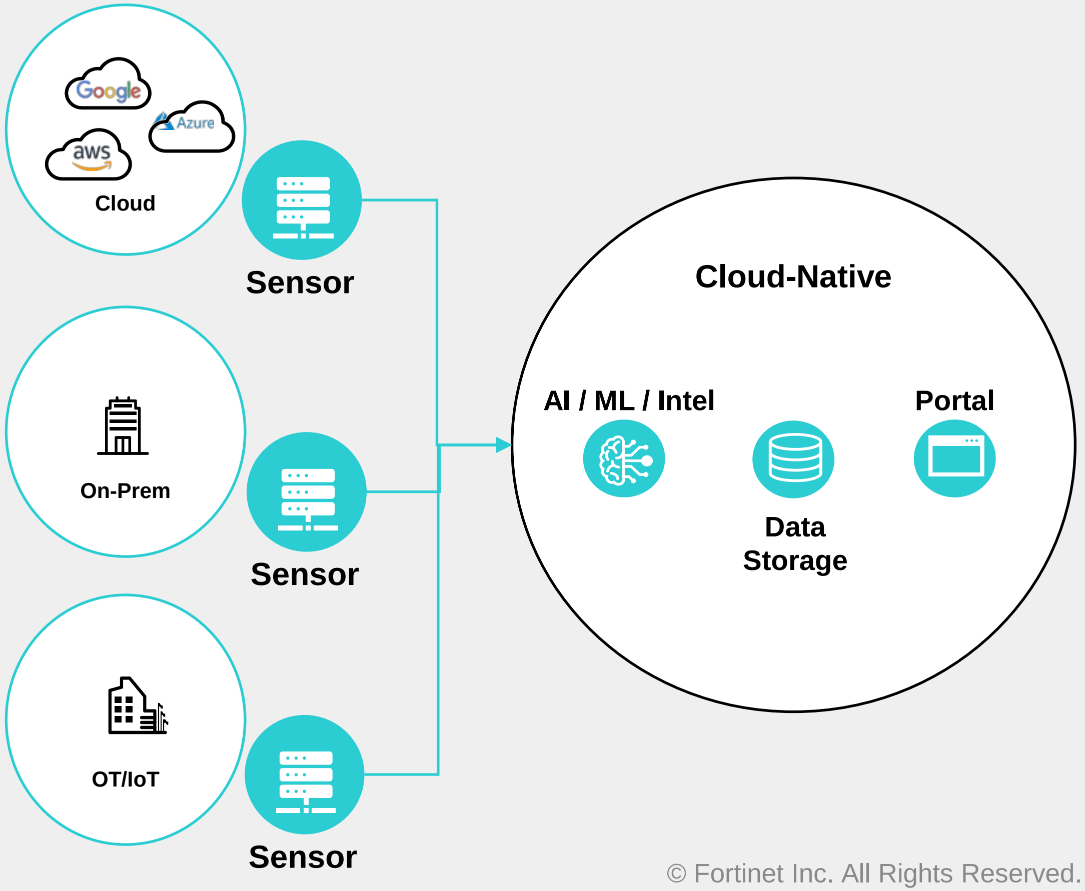


“NDRs complete the SOC’s visibility and identify threat actor behaviors across the MITRE ATT&CK framework”

FortiNDR Key Concept - Deployment Model

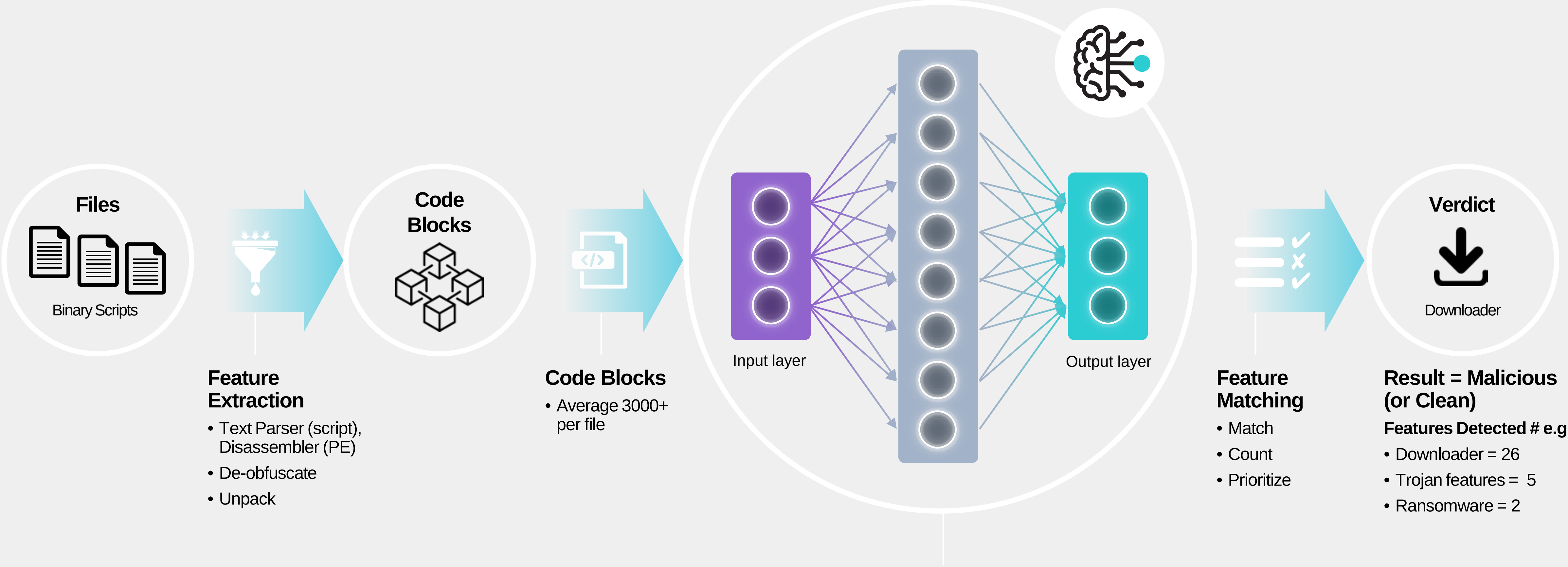
FortiNDR	FortiNDR Cloud
On-premises analytics	**SaaS-based**, cloud-native analytics





FortiNDR Advanced Malware Detection

Patent pending # U.S. Serial No.: 16/053,479



Files

Binary Scripts

Code Blocks

Input layer

Output layer

Verdict

Downloader

Feature Extraction

- Text Parser (script), Disassembler (PE)
- De-obfuscate
- Unpack

Code Blocks

- Average 3000+ per file

Feature Matching

- Match
- Count
- Prioritize

Result = Malicious (or Clean)

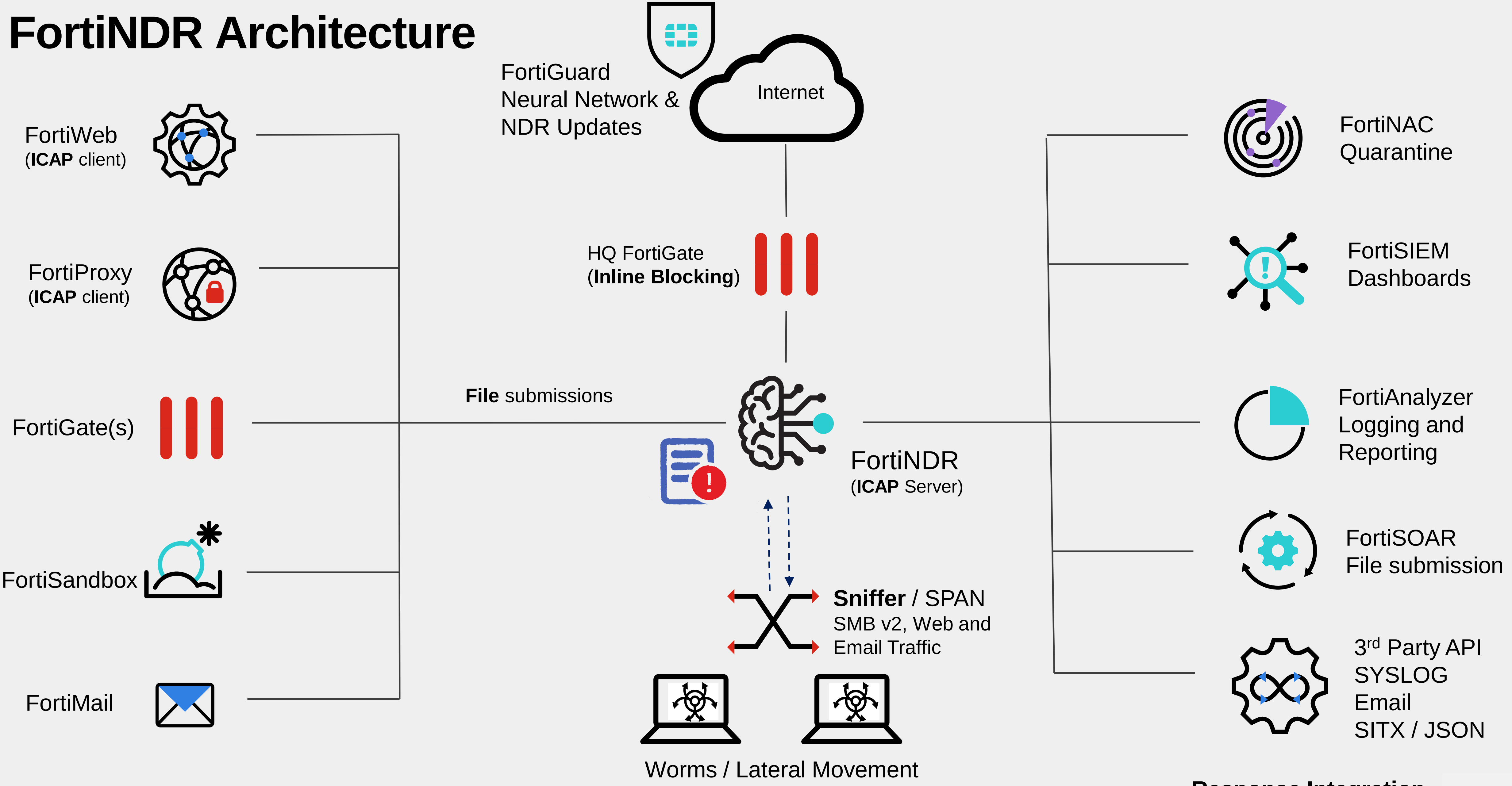
Features Detected # e.g.

- Downloader = 26
- Trojan features = 5
- Ransomware = 2

Artificial Neural Network

- Features DB
- 6mil+ Features
- GPU/hardware accelerated

FortiNDR Architecture



FortiGuard
Neural Network &
NDR Updates

Internet

HQ FortiGate
(**Inline Blocking**)

FortiWeb
(**ICAP** client)

FortiProxy
(**ICAP** client)

FortiGate(s)

FortiSandbox

FortiMail

File submissions

FortiNDR
(**ICAP** Server)

Sniffer / SPAN
SMB v2, Web and
Email Traffic

Worms / Lateral Movement

FortiNAC
Quarantine

FortiSIEM
Dashboards

FortiAnalyzer
Logging and
Reporting

FortiSOAR
File submission

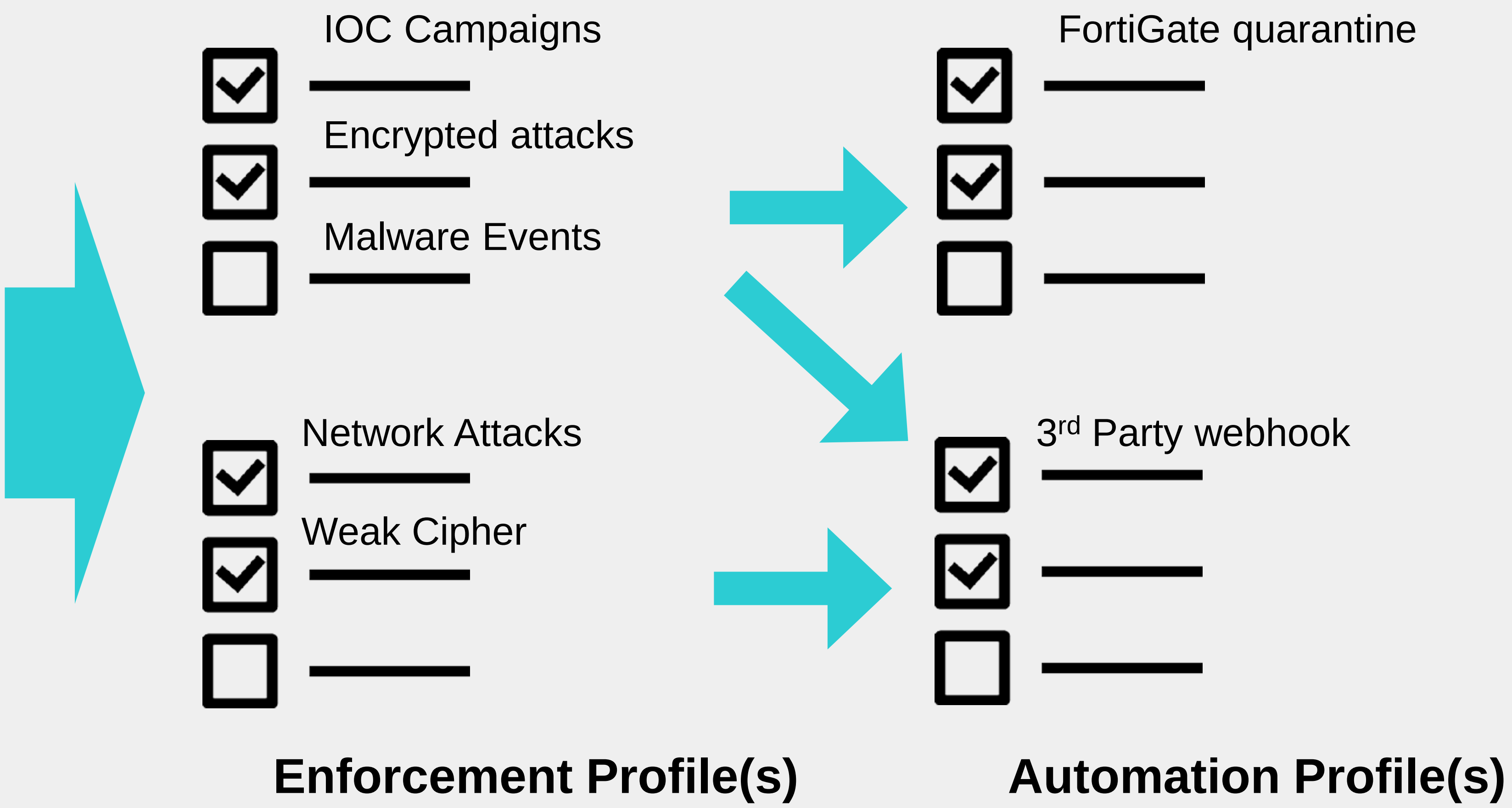
3rd Party API
SYSLOG
Email
SITX / JSON

Response Integration

FortiNDR Response

Understanding Enforcement and Automation Profiles

Events Trigger
e.g. Network Attacks
IOC Campaigns
Encrypted attacks
Malware Events etc



☑ IOC Campaigns
☑ Encrypted attacks
□ Malware Events

☑ Network Attacks
☑ Weak Cipher
□ ______

☑ FortiGate quarantine
☑ ______
□ ______

☑ 3rd Party webhook
☑ ______
□ ______

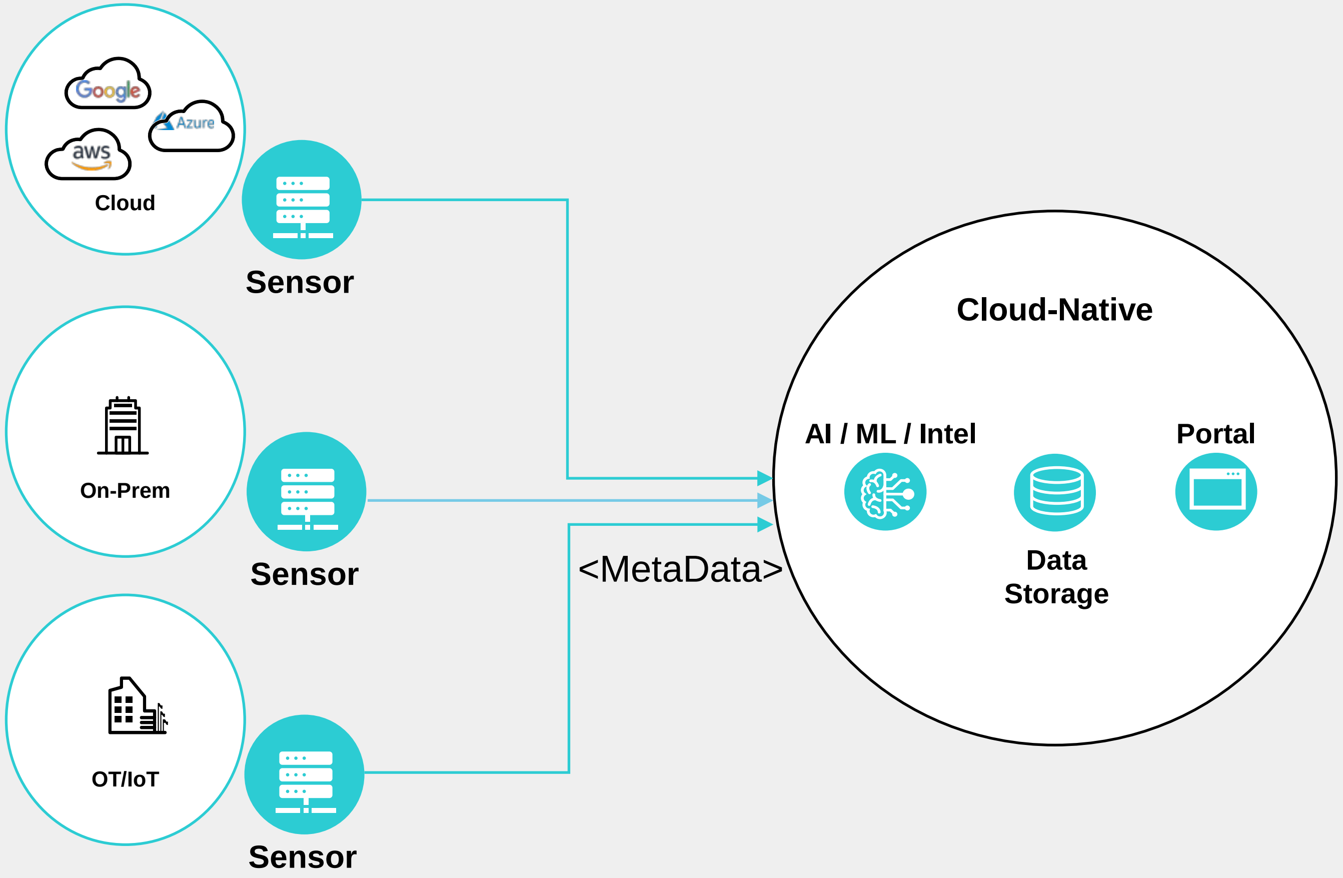
Enforcement Profile(s)

Automation Profile(s)

FortiNDR Cloud - Overview

Architecture

- Sensors
- Cloud-Native backend
  - Detection & Analytics
  - Cloud Data Warehouse
  - Portal/API

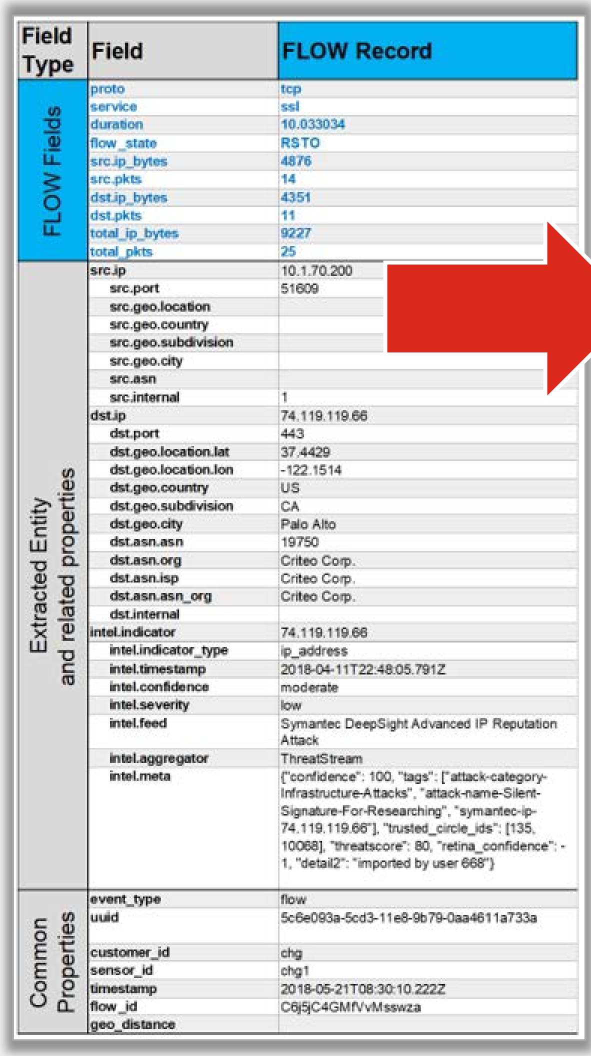


Protocols and Events

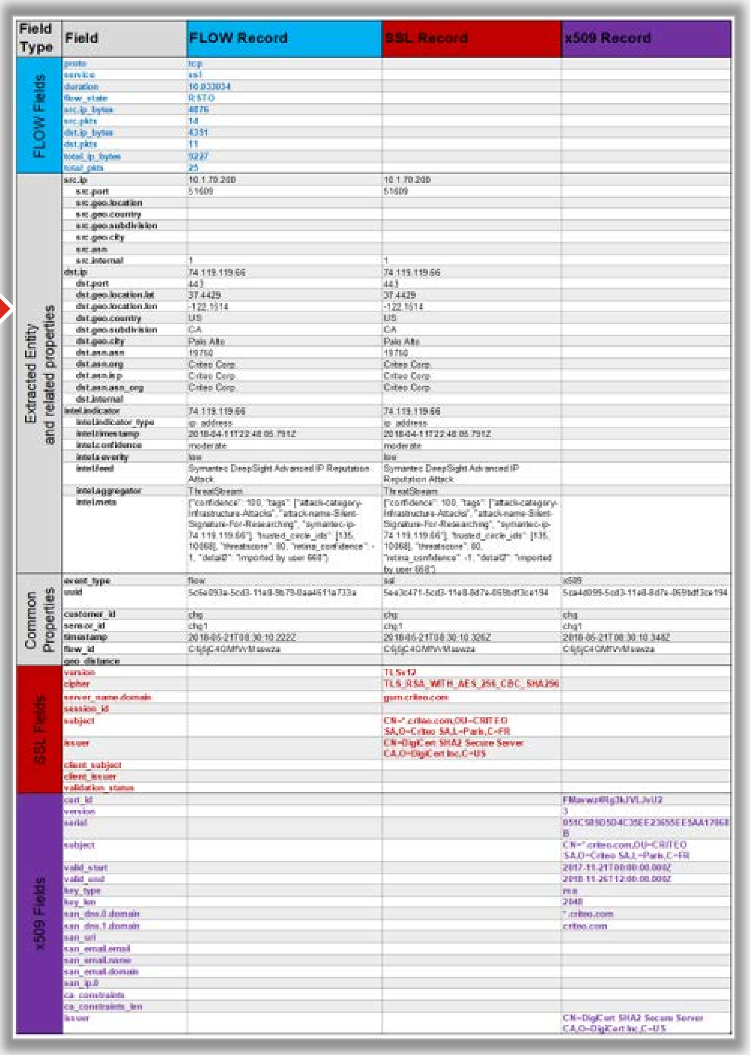
Event overview

Event data

- FLOW fields
  - Basic connection information
- Extracted Entity and related properties
  - Extracted data properties
- Common properties
  - Common event information (event type, sensor, customer info, etc.)
- Additional Protocol-specific and Application-specific metadata



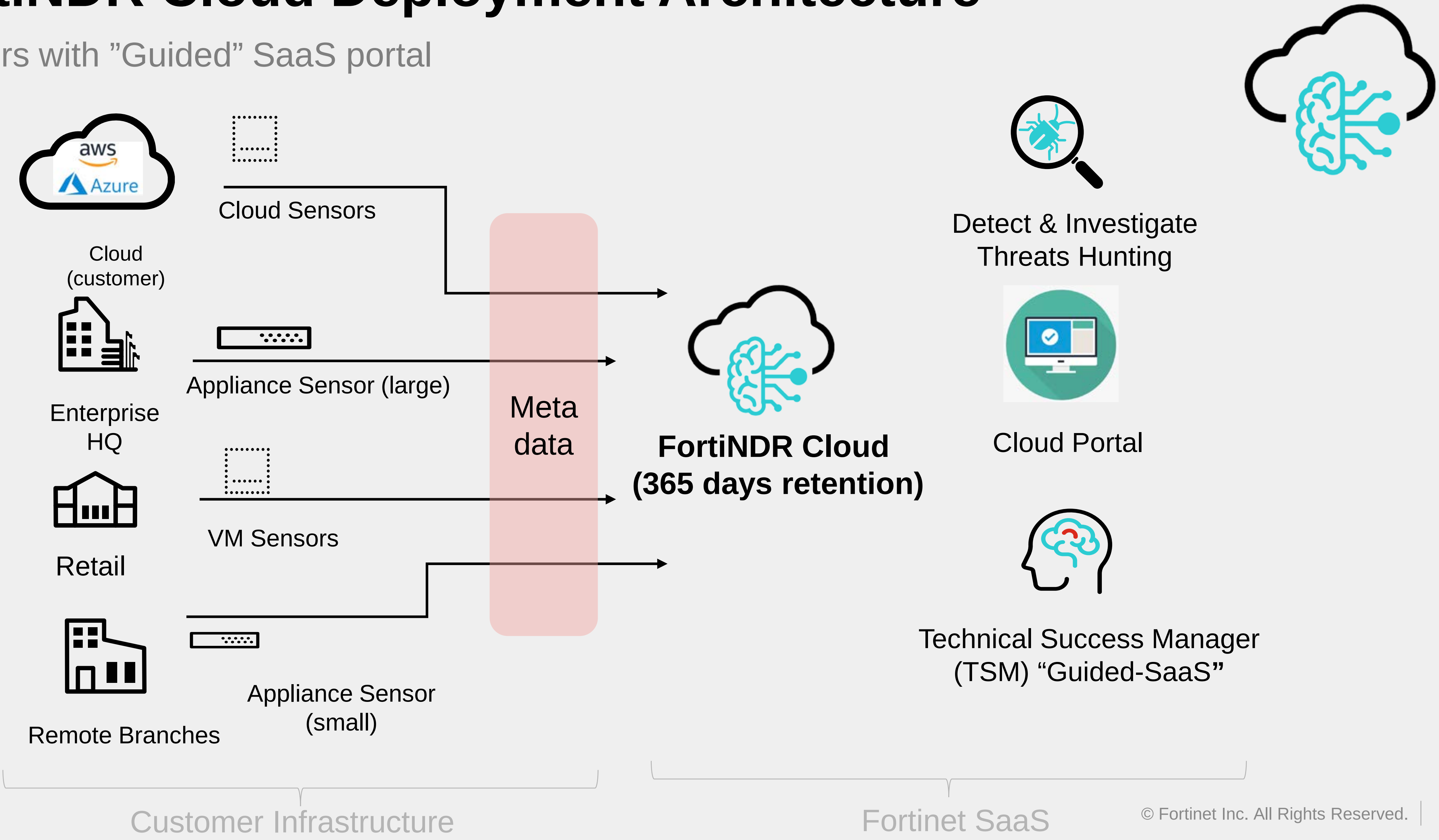
Field Type	Field	FLOW Record
FLOW Fields	proto	tcp
	service	ssl
	duration	10.033034
	flow_state	RSTO
	src.ip_bytes	4876
	src.pkts	14
	dst.ip_bytes	4351
	dst.pkts	11
	total_ip_bytes	9227
	total_pkts	25
Extracted Entity and related properties	src.ip	10.1.70.200
	src.port	51609
	src.geo.location	
	src.geo.country	
	src.geo.subdivision	
	src.geo.city	
	src.asn	
	src.internal	1
	dst.ip	74.119.119.66
	dst.port	443
	dst.geo.location.lat	37.4429
	dst.geo.location.lon	-122.1514
	dst.geo.country	US
	dst.geo.subdivision	CA
	dst.geo.city	Palo Alto
	dst.asn.asn	19750
	dst.asn.org	Criteo Corp.
	dst.asn.isp	Criteo Corp.
	dst.asn.asn_org	Criteo Corp.
	dst.internal	
	intel.indicator	74.119.119.66
	intel.indicator_type	ip_address
	intel.timestamp	2018-04-11T22:48:05.791Z
	intel.confidence	moderate
	intel.severity	low
	intel.feed	Symantec DeepSight Advanced IP Reputation Attack
	intel.aggregator	ThreatStream
	intel.meta	{"confidence": 100, "tags": ["attack-category-Infrastructure-Attacks", "attack-name-Silent-Signature-For-Researching", "symantec-ip-74.119.119.66"], "trusted_circle_ids": [135, 10068], "threatscore": 80, "retina_confidence": -1, "detail2": "imported by user 668"}
Common Properties	event_type	flow
	uuid	5c6e093a-5cd3-11e8-9b79-0aa4611a733a
	customer_id	chg
	sensor_id	chg1
	timestamp	2018-05-21T08:30:10.222Z
	flow_id	C6j5jC4GMfVvMsswza
	geo_distance	



Field Type	Field	FLOW Record	SSL Record	x509 Record
FLOW Fields	proto	tcp		
	service	ssl		
	duration	10.033034		
	flow_state	RSTO		
	src.ip_bytes	4876		
	src.pkts	14		
	dst.ip_bytes	4351		
	dst.pkts	11		
	total_ip_bytes	9227		
	total_pkts	25		
Extracted Entity and related properties	src.ip	10.1.70.200	10.1.70.200	
	src.port	51609	51609	
	src.geo.location			
	src.geo.country			
	src.geo.subdivision			
	src.geo.city			
	src.asn			
	src.internal	1	1	
	dst.ip	74.119.119.66	74.119.119.66	
	dst.port	443	443	
	dst.geo.location.lat	37.4429	37.4429	
	dst.geo.location.lon	-122.1514	-122.1514	
	dst.geo.country	US	US	
	dst.geo.subdivision	CA	CA	
	dst.geo.city	Palo Alto	Palo Alto	
	dst.asn.asn	19750	19750	
	dst.asn.org	Criteo Corp.	Criteo Corp.	
	dst.asn.isp	Criteo Corp.	Criteo Corp.	
	dst.asn.asn_org	Criteo Corp.	Criteo Corp.	
	dst.internal			
	intel.indicator	74.119.119.66	74.119.119.66	
	intel.indicator_type	ip_address	ip_address	
	intel.timestamp	2018-04-11T22:48:05.791Z	2018-04-11T22:48:05.791Z	
	intel.confidence	moderate	moderate	
	intel.severity	low	low	
	intel.feed	Symantec DeepSight Advanced IP Reputation Attack	Symantec DeepSight Advanced IP Reputation Attack	
	intel.aggregator	ThreatStream	ThreatStream	
	intel.meta	{"confidence": 100, "tags": ["attack-category-Infrastructure-Attacks", "attack-name-Silent-Signature-For-Researching", "symantec-ip-74.119.119.66"], "trusted_circle_ids": [135, 10068], "threatscore": 80, "retina_confidence": -1, "detail2": "imported by user 668"}	{"confidence": 100, "tags": ["attack-category-Infrastructure-Attacks", "attack-name-Silent-Signature-For-Researching", "symantec-ip-74.119.119.66"], "trusted_circle_ids": [135, 10068], "threatscore": 80, "retina_confidence": -1, "detail2": "imported by user 668"}	
Common Properties	event_type	flow	ssl	x509
	uuid	5c6e093a-5cd3-11e8-9b79-0aa4611a733a	5ea3c471-5cd3-11e8-8d7e-069bdf3ce194	5ca4d099-5cd3-11e8-8d7e-069bdf3ce194
	customer_id	chg	chg	chg
	sensor_id	chg1	chg1	chg1
	timestamp	2018-05-21T08:30:10.222Z	2018-05-21T08:30:10.326Z	2018-05-21T08:30:10.348Z
	flow_id	C6j5jC4GMfVvMsswza	C6j5jC4GMfVvMsswza	C6j5jC4GMfVvMsswza
	geo_distance			
SSL Fields	version		TLSv12	
	cipher		TLS_RSA_WITH_AES_256_CBC_SHA256	
	server_name.domain		gum.criteo.com	
	session_id			
	subject		CN=*.criteo.com,OU=CRITEO SA,O=Criteo SA,L=Paris,C=FR	
	issuer		CN=DigiCert SHA2 Secure Server CA,O=DigiCert Inc,C=US	
	client_subject			
	client_issuer			
	validation_status			
x509 Fields	cert_id			FMavwz4lIg3kJVLJvU2
	version			3
	serial			051C589D504C35EE23655EE5AA17868B
	subject			CN=*.criteo.com,OU=CRITEO SA,O=Criteo SA,L=Paris,C=FR
	valid_start			2017-11-21T00:00:00.000Z
	valid_end			2018-11-26T12:00:00.000Z
	key_type			rsa
	key_len			2048
	san_dns.0.domain			*.criteo.com
	san_dns.1.domain			criteo.com
	san_uri			
	san_email.email			
	san_email.name			
	san_email.domain			
	san_ip.0			
	ca_constraints			
	ca_constraints_len			
	issuer			CN=DigiCert SHA2 Secure Server CA,O=DigiCert Inc,C=US

FortiNDR Cloud Deployment Architecture

Sensors with ”Guided” SaaS portal



Cloud (customer)

Cloud Sensors

Enterprise HQ

Appliance Sensor (large)

Retail

VM Sensors

Remote Branches

Appliance Sensor (small)

Meta data

FortiNDR Cloud (365 days retention)

Detect & Investigate Threats Hunting

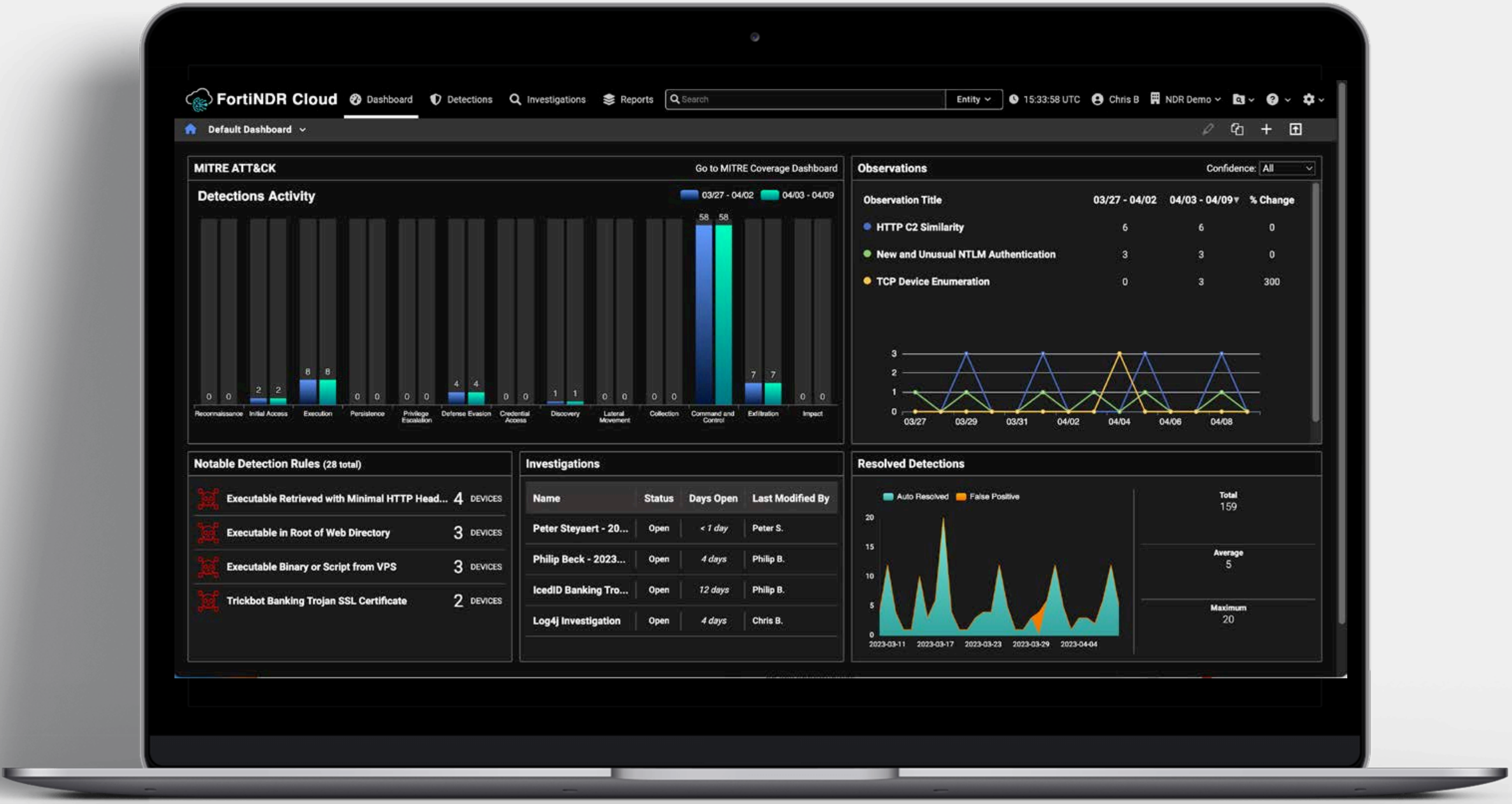
Cloud Portal

Technical Success Manager (TSM) “Guided-SaaS”

Customer Infrastructure

Fortinet SaaS

FortiNDR Cloud - Default Dashboard



Observation Title	03/27 - 04/02	04/03 - 04/09▾	% Change
● HTTP C2 Similarity	6	6	0
● New and Unusual NTLM Authentication	3	3	0
● TCP Device Enumeration	0	3	300

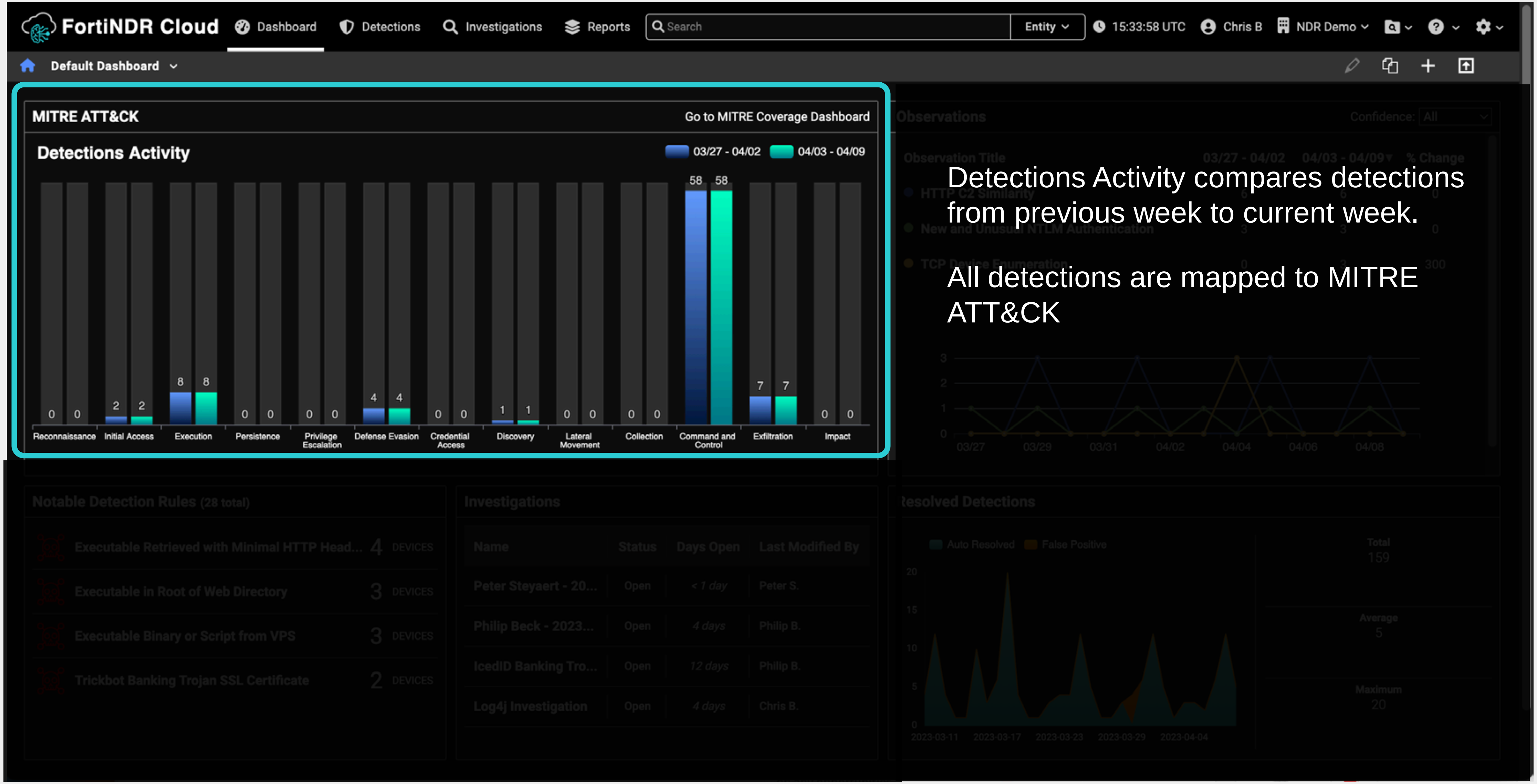
Notable Detection Rules (28 total)

Executable Retrieved with Minimal HTTP Head...	4	DEVICES
Executable in Root of Web Directory	3	DEVICES
Executable Binary or Script from VPS	3	DEVICES
Trickbot Banking Trojan SSL Certificate	2	DEVICES

Investigations

Name	Status	Days Open	Last Modified By
Peter Steyaert - 20...	Open	*< 1 day*	Peter S.
Philip Beck - 2023...	Open	*4 days*	Philip B.
IcedID Banking Tro...	Open	*12 days*	Philip B.
Log4j Investigation	Open	*4 days*	Chris B.

Default Dashboard – Detections Activity



Notable Detection Rules (28 total)

Executable Retrieved with Minimal HTTP Head...	4	DEVICES
Executable in Root of Web Directory	3	DEVICES
Executable Binary or Script from VPS	3	DEVICES
Trickbot Banking Trojan SSL Certificate	2	DEVICES

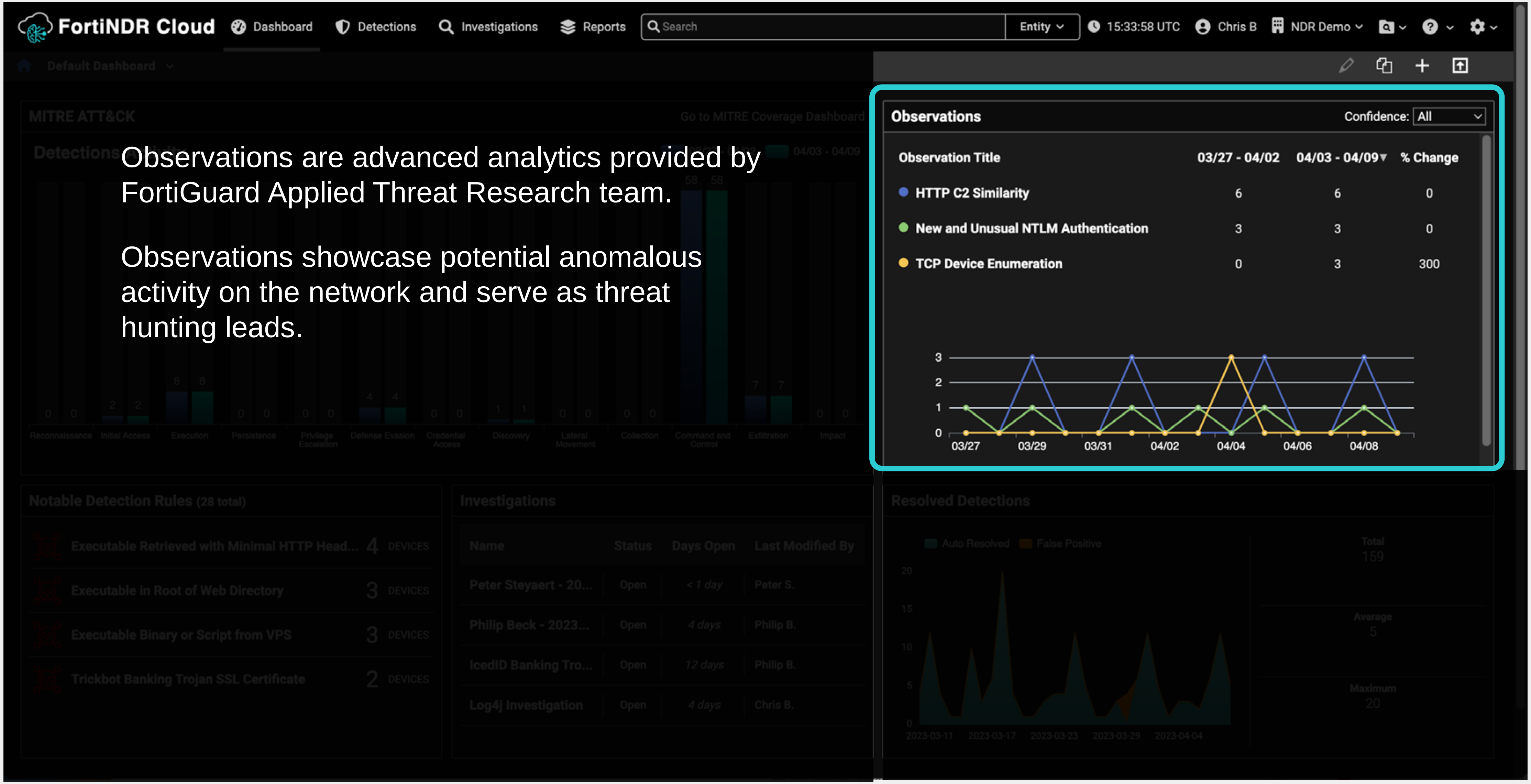
Investigations

Name	Status	Days Open	Last Modified By
Peter Steyaert - 20...	Open	< 1 day	Peter S.
Philip Beck - 2023...	Open	4 days	Philip B.
IcedID Banking Tro...	Open	12 days	Philip B.
Log4j Investigation	Open	4 days	Chris B.

Detections Activity compares detections from previous week to current week.

All detections are mapped to MITRE ATT&CK

The Default Dashboard - Observations



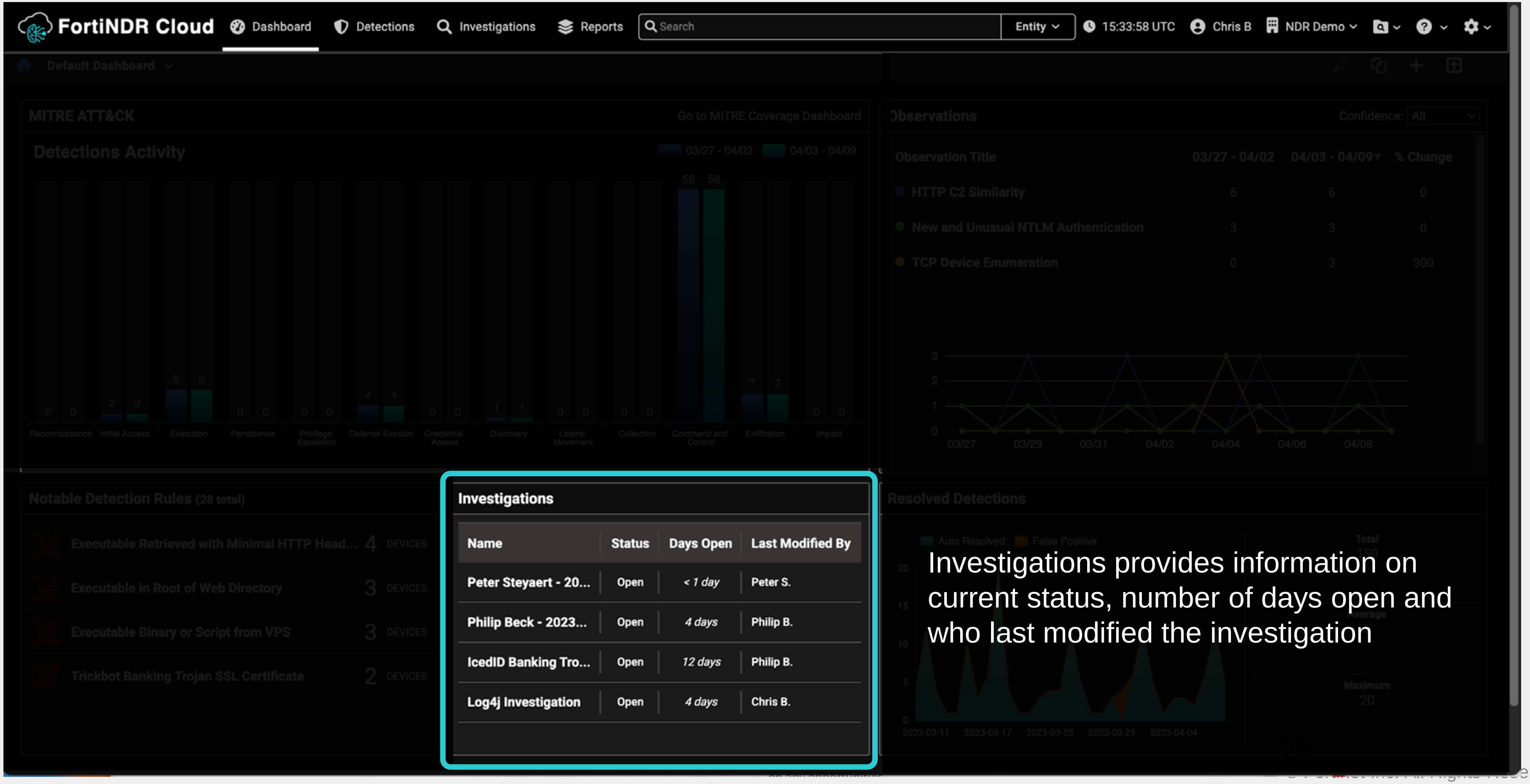
Observations are advanced analytics provided by FortiGuard Applied Threat Research team.

Observations showcase potential anomalous activity on the network and serve as threat hunting leads.

Observations Confidence: All

Observation Title	03/27 - 04/02	04/03 - 04/09	% Change
HTTP C2 Similarity	6	6	0
New and Unusual NTLM Authentication	3	3	0
TCP Device Enumeration	0	3	300

Default Dashboard - Investigations



Observation Title	03/27 - 04/02	04/03 - 04/09	% Change
HTTP C2 Similarity	6	6	0
New and Unusual NTLM Authentication	3	3	0
TCP Device Enumeration	0	3	300

Notable Detection Rules (28 total)

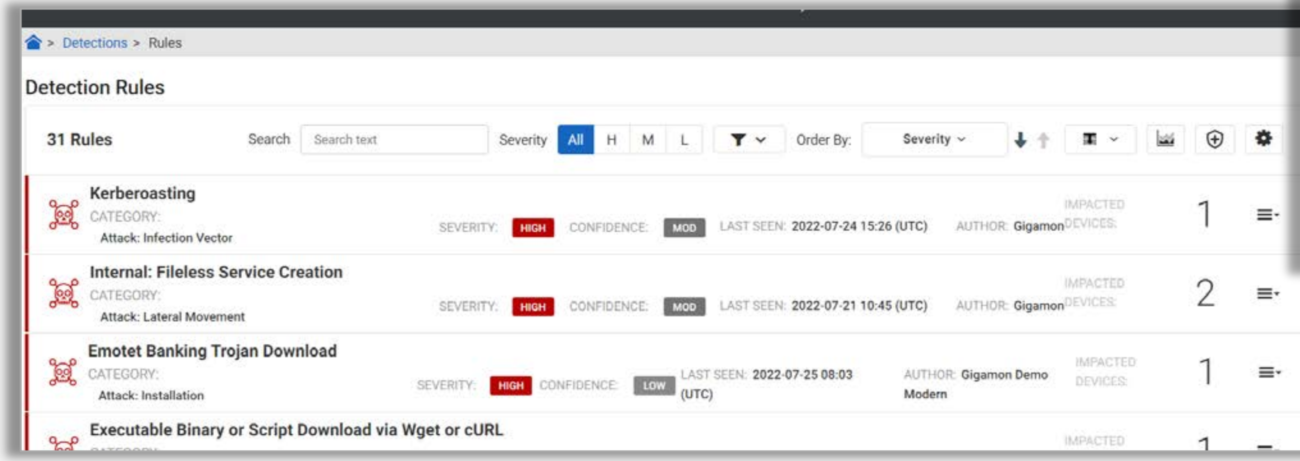
Executable Retrieved with Minimal HTTP Head...	4	DEVICES
Executable in Root of Web Directory	3	DEVICES
Executable Binary or Script from VPS	3	DEVICES
Trickbot Banking Trojan SSL Certificate	2	DEVICES

Investigations

Name	Status	Days Open	Last Modified By
Peter Steyaert - 20...	Open	< 1 day	Peter S.
Philip Beck - 2023...	Open	4 days	Philip B.
IcedID Banking Tro...	Open	12 days	Philip B.
Log4j Investigation	Open	4 days	Chris B.

Investigations provides information on current status, number of days open and who last modified the investigation

FortNDR Cloud Detections



Detections > Rules

Detection Rules

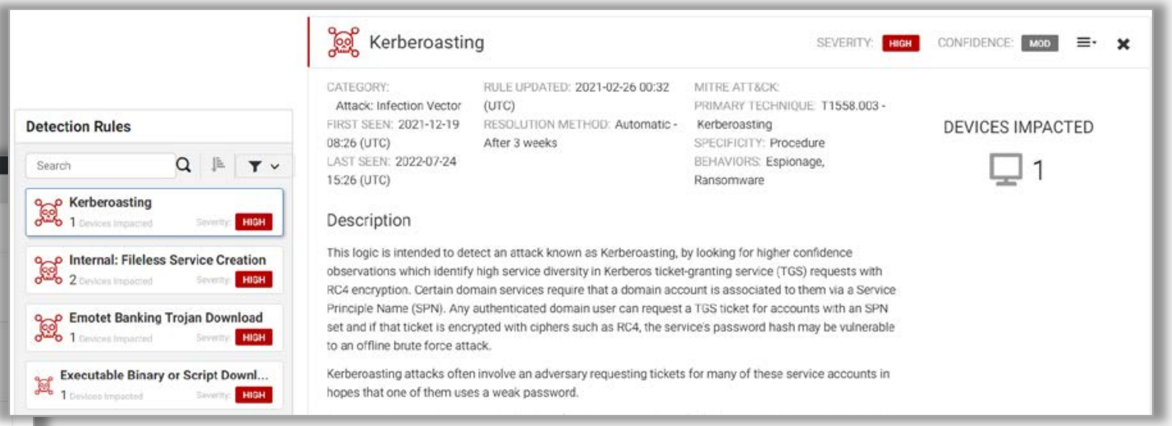
31 Rules — Search: Search text — Severity: All | H | M | L — Order By: Severity

Kerberoasting
CATEGORY: Attack: Infection Vector
SEVERITY: HIGH CONFIDENCE: MOD LAST SEEN: 2022-07-24 15:26 (UTC) AUTHOR: Gigamon IMPACTED DEVICES: 1

Internal: Fileless Service Creation
CATEGORY: Attack: Lateral Movement
SEVERITY: HIGH CONFIDENCE: MOD LAST SEEN: 2022-07-21 10:45 (UTC) AUTHOR: Gigamon IMPACTED DEVICES: 2

Emotet Banking Trojan Download
CATEGORY: Attack: Installation
SEVERITY: HIGH CONFIDENCE: LOW LAST SEEN: 2022-07-25 08:03 (UTC) AUTHOR: Gigamon Demo Modern IMPACTED DEVICES: 1

Executable Binary or Script Download via Wget or cURL
IMPACTED 1



Detection Rules

Search

Kerberoasting — 1 Devices Impacted — Severity: HIGH

Internal: Fileless Service Creation — 2 Devices Impacted — Severity: HIGH

Emotet Banking Trojan Download — 1 Devices Impacted — Severity: HIGH

Executable Binary or Script Downl... — 1 Devices Impacted — Severity: HIGH

Kerberoasting — SEVERITY: HIGH CONFIDENCE: MOD

CATEGORY: Attack: Infection Vector
FIRST SEEN: 2021-12-19 08:26 (UTC)
LAST SEEN: 2022-07-24 15:26 (UTC)

RULE UPDATED: 2021-02-26 00:32 (UTC)
RESOLUTION METHOD: Automatic - After 3 weeks

MITRE ATT&CK:
PRIMARY TECHNIQUE: T1558.003 - Kerberoasting
SPECIFICITY: Procedure
BEHAVIORS: Espionage, Ransomware

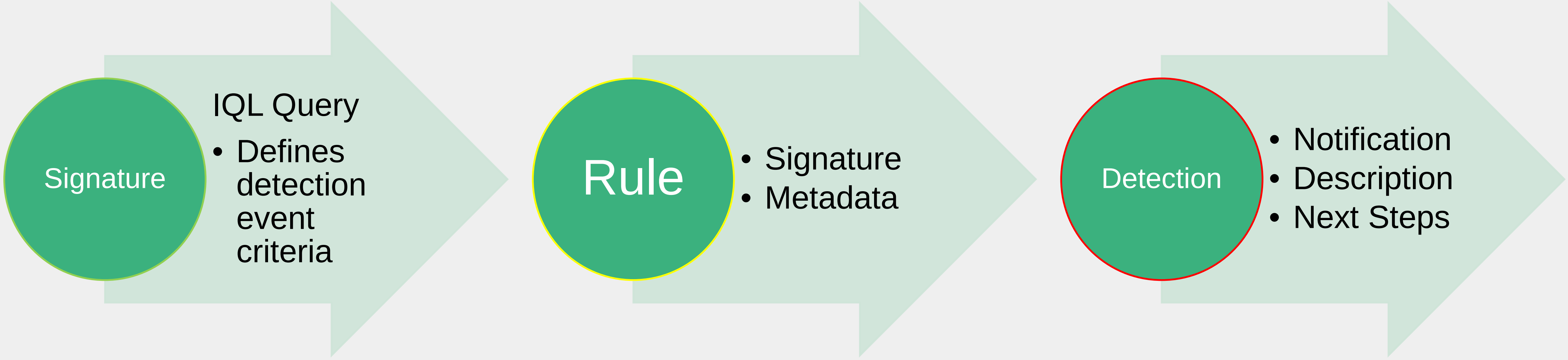
DEVICES IMPACTED 1

Description

This logic is intended to detect an attack known as Kerberoasting, by looking for higher confidence observations which identify high service diversity in Kerberos ticket-granting service (TGS) requests with RC4 encryption. Certain domain services require that a domain account is associated to them via a Service Principle Name (SPN). Any authenticated domain user can request a TGS ticket for accounts with an SPN set and if that ticket is encrypted with ciphers such as RC4, the service's password hash may be vulnerable to an offline brute force attack.

Kerberoasting attacks often involve an adversary requesting tickets for many of these service accounts in hopes that one of them uses a weak password.

Term	Description
Rule	A signature and other parameters to detect something (event)
Detection	A unique set of events that satisfy a rule



Signature

IQL Query

- Defines detection event criteria

Rule

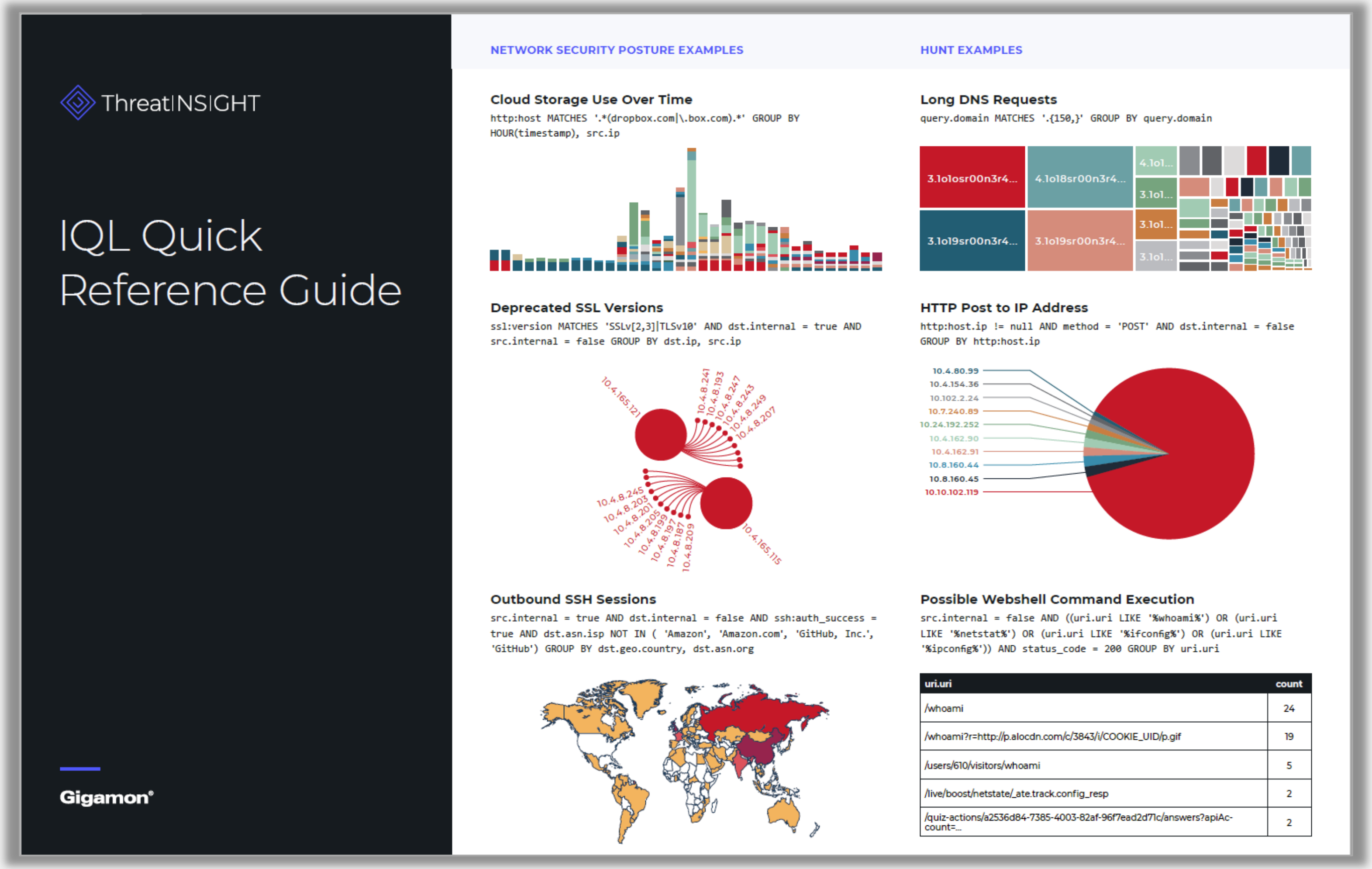
- Signature
- Metadata

Detection

- Notification
- Description
- Next Steps

IQL

- IQL – Insight Query Language
- SQL-like language for writing queries (Investigations, Playbooks)



ThreatINSIGHT

IQL Quick Reference Guide

Gigamon®

NETWORK SECURITY POSTURE EXAMPLES

Cloud Storage Use Over Time

```
http:host MATCHES '.*(dropbox.com|\.box.com).*' GROUP BY
HOUR(timestamp), src.ip
```

Deprecated SSL Versions

```
ssl:version MATCHES 'SSLv[2,3]|TLSv10' AND dst.internal = true AND
src.internal = false GROUP BY dst.ip, src.ip
```

Outbound SSH Sessions

```
src.internal = true AND dst.internal = false AND ssh:auth_success =
true AND dst.asn.isp NOT IN ( 'Amazon', 'Amazon.com', 'GitHub, Inc.',
'GitHub') GROUP BY dst.geo.country, dst.asn.org
```

HUNT EXAMPLES

Long DNS Requests

```
query.domain MATCHES '.{150,}' GROUP BY query.domain
```

HTTP Post to IP Address

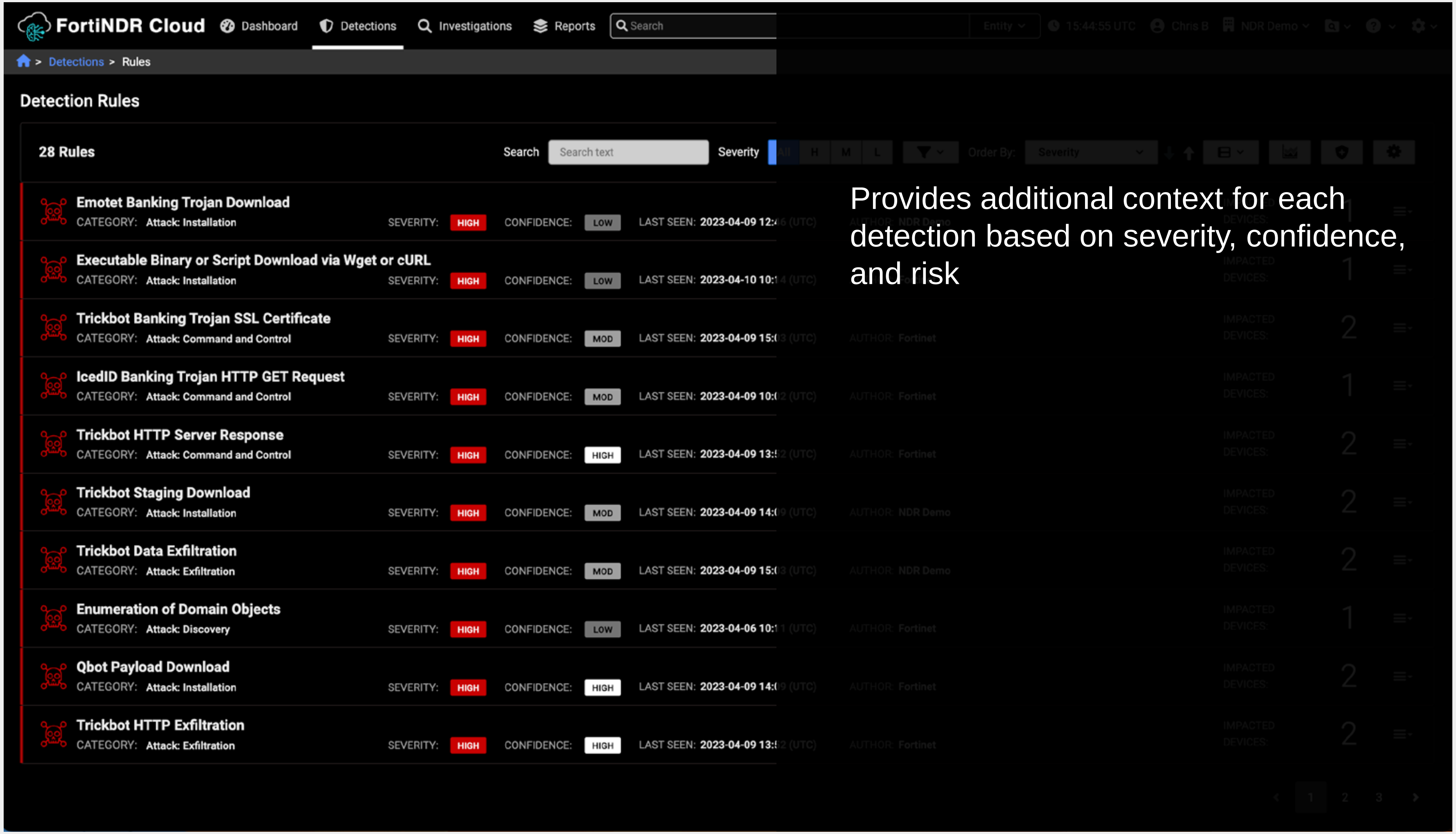
```
http:host.ip != null AND method = 'POST' AND dst.internal = false
GROUP BY http:host.ip
```

Possible Webshell Command Execution

```
src.internal = false AND ((uri.uri LIKE '%whoami%') OR (uri.uri
LIKE '%netstat%') OR (uri.uri LIKE '%ifconfig%') OR (uri.uri LIKE
'%ipconfig%')) AND status_code = 200 GROUP BY uri.uri
```

uri.uri	count
/whoami	24
/whoami?r=http://p.alocdn.com/c/3843/i/COOKIE_UID/p.gif	19
/users/610/visitors/whoami	5
/live/boost/netstate/_ate.track.config_resp	2
/quiz-actions/a2536d84-7385-4003-82af-96f7ead2d71c/answers?apiAc-count=...	2

Detection Rules



Detections > Rules

Detection Rules

28 Rules

Search: Search text — Severity: All | H | M | L — Order By: Severity

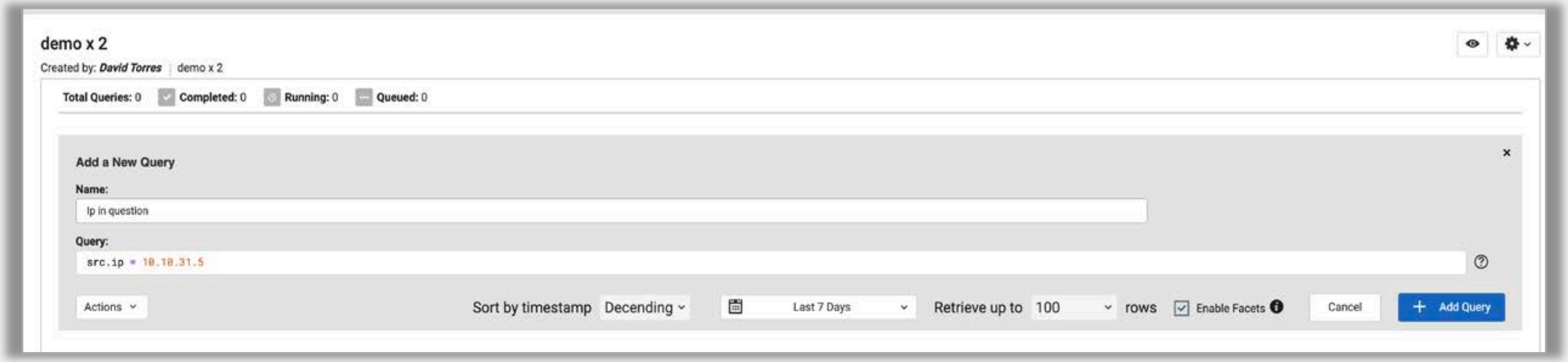
Rule	Category	Severity	Confidence	Last Seen	Author	Impacted Devices
Emotet Banking Trojan Download	Attack: Installation	HIGH	LOW	2023-04-09 12:46 (UTC)	NDR Demo	1
Executable Binary or Script Download via Wget or cURL	Attack: Installation	HIGH	LOW	2023-04-10 10:14 (UTC)	Fortinet	1
Trickbot Banking Trojan SSL Certificate	Attack: Command and Control	HIGH	MOD	2023-04-09 15:03 (UTC)	Fortinet	2
IcedID Banking Trojan HTTP GET Request	Attack: Command and Control	HIGH	MOD	2023-04-09 10:02 (UTC)	Fortinet	1
Trickbot HTTP Server Response	Attack: Command and Control	HIGH	HIGH	2023-04-09 13:52 (UTC)	Fortinet	2
Trickbot Staging Download	Attack: Installation	HIGH	MOD	2023-04-09 14:09 (UTC)	NDR Demo	2
Trickbot Data Exfiltration	Attack: Exfiltration	HIGH	MOD	2023-04-09 15:03 (UTC)	NDR Demo	2
Enumeration of Domain Objects	Attack: Discovery	HIGH	LOW	2023-04-06 10:11 (UTC)	Fortinet	1
Qbot Payload Download	Attack: Installation	HIGH	HIGH	2023-04-09 14:09 (UTC)	Fortinet	2
Trickbot HTTP Exfiltration	Attack: Exfiltration	HIGH	HIGH	2023-04-09 13:52 (UTC)	Fortinet	2

1 2 3

Provides additional context for each detection based on severity, confidence, and risk

Investigations

- One or more queries to the events collected
- Essential for collaboration in hunting



demo x 2

Created by: *David Torres* | demo x 2

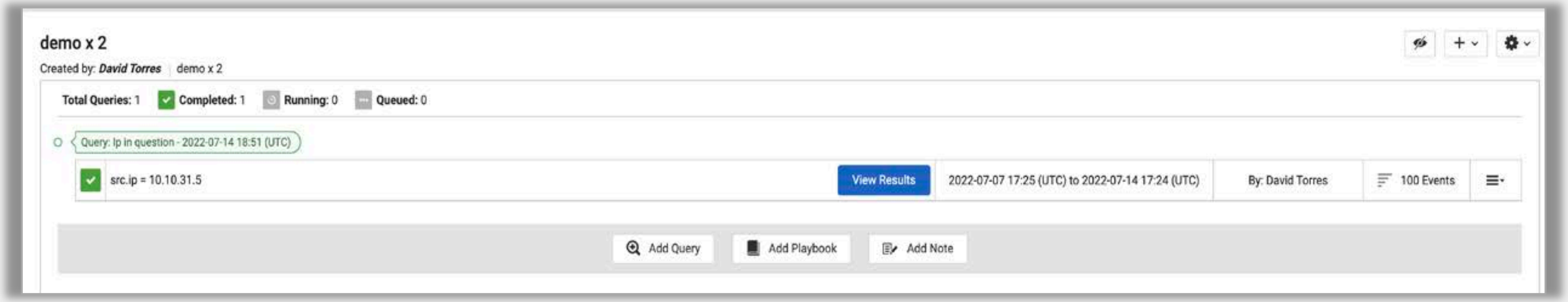
Total Queries: 0 ☑ **Completed:** 0 **Running:** 0 **Queued:** 0

Add a New Query

Name: Ip in question

Query:

```
src.ip = 10.10.31.5
```



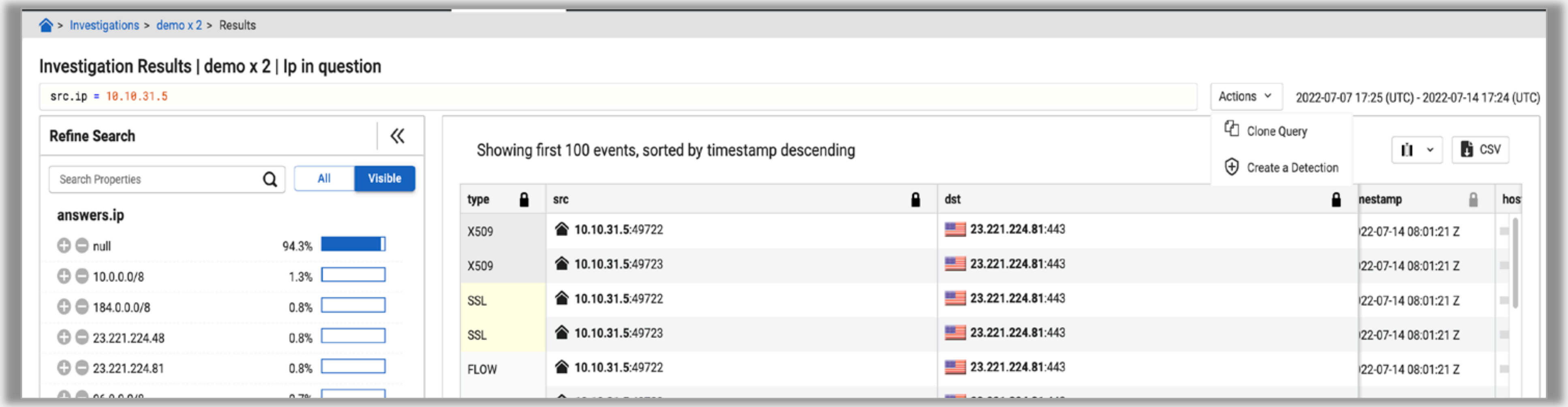
demo x 2

Created by: *David Torres* | demo x 2

Total Queries: 1 ☑ **Completed:** 1 **Running:** 0 **Queued:** 0

Query: Ip in question - 2022-07-14 18:51 (UTC)

☑ src.ip = 10.10.31.5 | 2022-07-07 17:25 (UTC) to 2022-07-14 17:24 (UTC) | By: David Torres | 100 Events



Investigations > demo x 2 > Results

Investigation Results | demo x 2 | Ip in question

```
src.ip = 10.10.31.5
```

2022-07-07 17:25 (UTC) - 2022-07-14 17:24 (UTC)

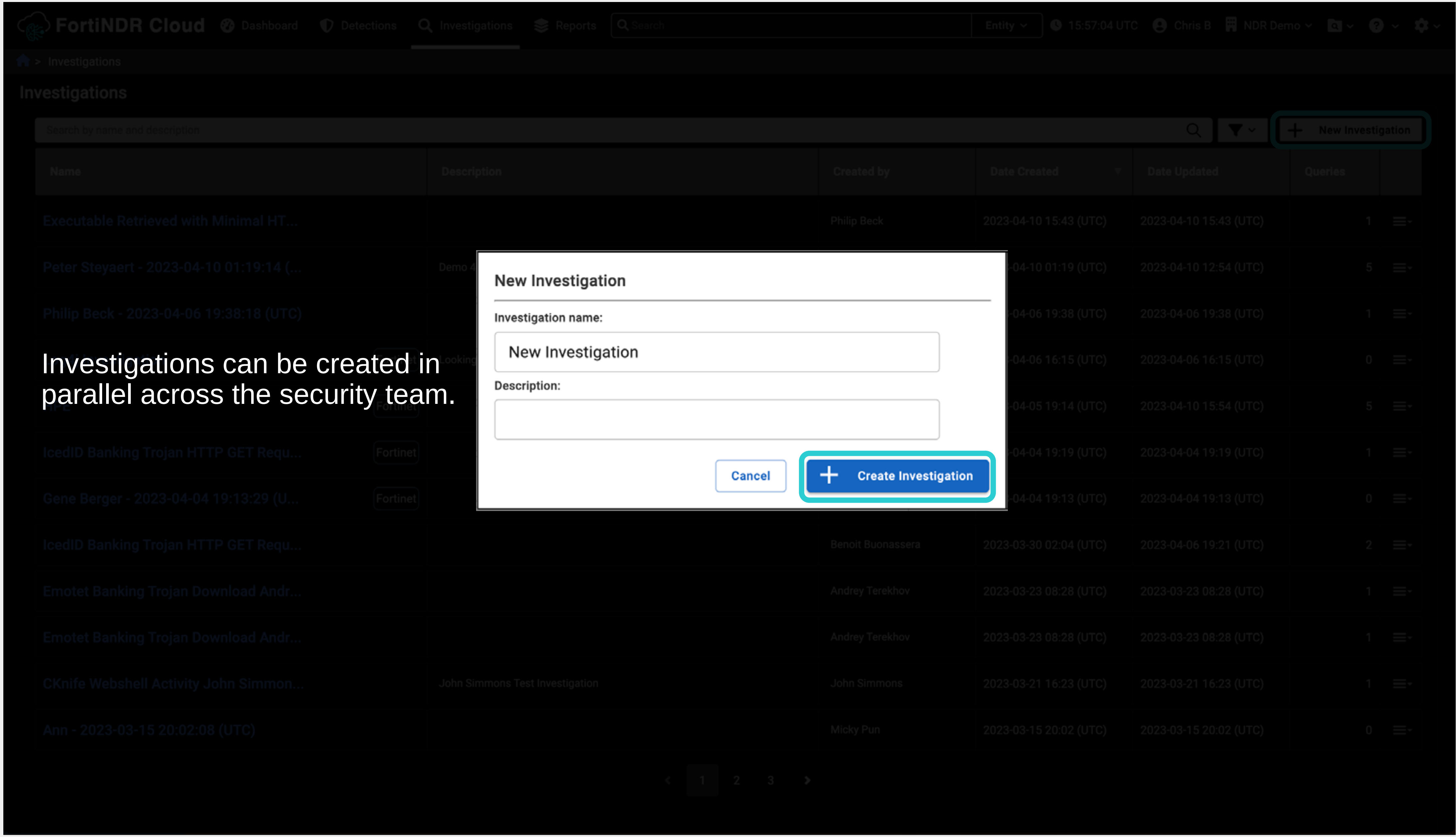
answers.ip

null	94.3%
10.0.0.0/8	1.3%
184.0.0.0/8	0.8%
23.221.224.48	0.8%
23.221.224.81	0.8%

Showing first 100 events, sorted by timestamp descending

type	src	dst	nestamp	hos
X509	10.10.31.5:49722	23.221.224.81:443	22-07-14 08:01:21 Z	
X509	10.10.31.5:49723	23.221.224.81:443	22-07-14 08:01:21 Z	
SSL	10.10.31.5:49722	23.221.224.81:443	22-07-14 08:01:21 Z	
SSL	10.10.31.5:49723	23.221.224.81:443	22-07-14 08:01:21 Z	
FLOW	10.10.31.5:49722	23.221.224.81:443	22-07-14 08:01:21 Z	

Investigations



Investigations

Search by name and description

Name	Description	Created by	Date Created	Date Updated	Queries
Executable Retrieved with Minimal HT...		Philip Beck	2023-04-10 15:43 (UTC)	2023-04-10 15:43 (UTC)	1
Peter Steyaert - 2023-04-10 01:19:14 (...	Demo 4	[illegible]	-04-10 01:19 (UTC)	2023-04-10 12:54 (UTC)	5
Philip Beck - 2023-04-06 19:38:18 (UTC)		[illegible]	-04-06 19:38 (UTC)	2023-04-06 19:38 (UTC)	1
[illegible]	Looking	[illegible]	-04-06 16:15 (UTC)	2023-04-06 16:15 (UTC)	0
[illegible]		[illegible]	-04-05 19:14 (UTC)	2023-04-10 15:54 (UTC)	5
IcedID Banking Trojan HTTP GET Requ... Fortinet		[illegible]	-04-04 19:19 (UTC)	2023-04-04 19:19 (UTC)	1
Gene Berger - 2023-04-04 19:13:29 (U... Fortinet		[illegible]	-04-04 19:13 (UTC)	2023-04-04 19:13 (UTC)	0
IcedID Banking Trojan HTTP GET Requ...		Benoit Buonassera	2023-03-30 02:04 (UTC)	2023-04-06 19:21 (UTC)	2
Emotet Banking Trojan Download Andr...		Andrey Terekhov	2023-03-23 08:28 (UTC)	2023-03-23 08:28 (UTC)	1
Emotet Banking Trojan Download Andr...		Andrey Terekhov	2023-03-23 08:28 (UTC)	2023-03-23 08:28 (UTC)	1
CKnife Webshell Activity John Simmon...	John Simmons Test Investigation	John Simmons	2023-03-21 16:23 (UTC)	2023-03-21 16:23 (UTC)	1
Ann - 2023-03-15 20:02:08 (UTC)		Micky Pun	2023-03-15 20:02 (UTC)	2023-03-15 20:02 (UTC)	0

New Investigation

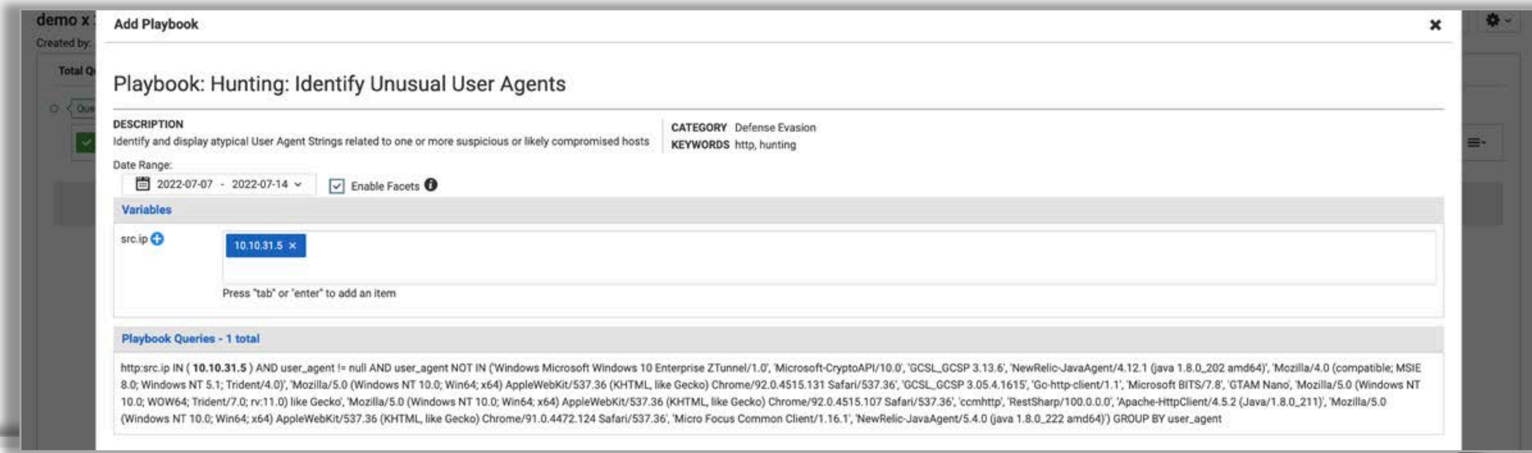
Investigation name: New Investigation

Description:

Investigations can be created in parallel across the security team.

Playbooks

- A pre-configured set of queries
- Assists hunting for specific threats
- Created and maintained by ATR team



Add Playbook ×

Playbook: Hunting: Identify Unusual User Agents

DESCRIPTION
Identify and display atypical User Agent Strings related to one or more suspicious or likely compromised hosts

CATEGORY Defense Evasion
KEYWORDS http, hunting

Date Range:
2022-07-07 - 2022-07-14

☑ Enable Facets

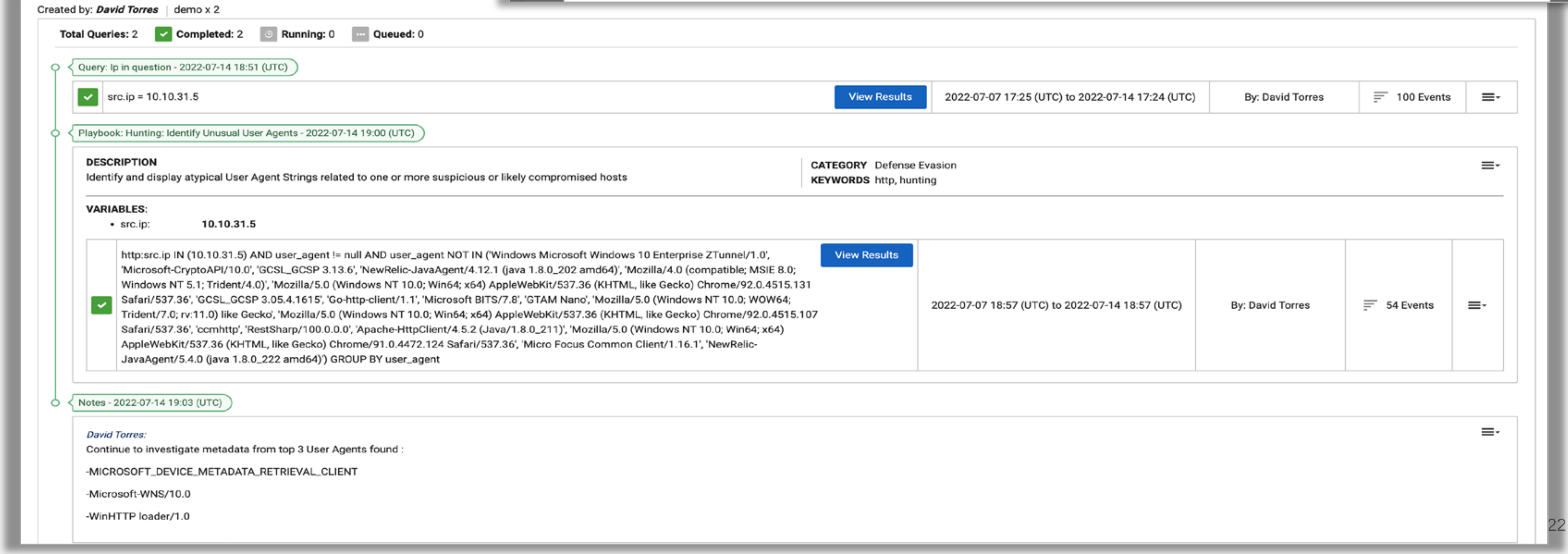
Variables

src.ip: 10.10.31.5 ×

Press "tab" or "enter" to add an item

Playbook Queries - 1 total

```
http:src.ip IN ( 10.10.31.5 ) AND user_agent != null AND user_agent NOT IN ('Windows Microsoft Windows 10 Enterprise ZTunnel/1.0', 'Microsoft-CryptoAPI/10.0', 'GCSL_GCSP 3.13.6', 'NewRelic-JavaAgent/4.12.1 (java 1.8.0_202 amd64)', 'Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)', 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36', 'GCSL_GCSP 3.05.4.1615', 'Go-http-client/1.1', 'Microsoft BITS/7.8', 'GTAM Nano', 'Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko', 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36', 'ccmhttp', 'RestSharp/100.0.0.0', 'Apache-HttpClient/4.5.2 (Java/1.8.0_211)', 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36', 'Micro Focus Common Client/1.16.1', 'NewRelic-JavaAgent/5.4.0 (java 1.8.0_222 amd64)') GROUP BY user_agent
```



Created by: ***David Torres*** | demo x 2

Total Queries: 2 ✓ **Completed:** 2 **Running:** 0 **Queued:** 0

Query: Ip in question - 2022-07-14 18:51 (UTC)

✓ src.ip = 10.10.31.5 | View Results | 2022-07-07 17:25 (UTC) to 2022-07-14 17:24 (UTC) | By: David Torres | 100 Events

Playbook: Hunting: Identify Unusual User Agents - 2022-07-14 19:00 (UTC)

DESCRIPTION
Identify and display atypical User Agent Strings related to one or more suspicious or likely compromised hosts

CATEGORY Defense Evasion
KEYWORDS http, hunting

VARIABLES:
- src.ip: **10.10.31.5**

```
http:src.ip IN (10.10.31.5) AND user_agent != null AND user_agent NOT IN ('Windows Microsoft Windows 10 Enterprise ZTunnel/1.0',
'Microsoft-CryptoAPI/10.0', 'GCSL_GCSP 3.13.6', 'NewRelic-JavaAgent/4.12.1 (java 1.8.0_202 amd64)', 'Mozilla/4.0 (compatible; MSIE 8.0;
Windows NT 5.1; Trident/4.0)', 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131
Safari/537.36', 'GCSL_GCSP 3.05.4.1615', 'Go-http-client/1.1', 'Microsoft BITS/7.8', 'GTAM Nano', 'Mozilla/5.0 (Windows NT 10.0; WOW64;
Trident/7.0; rv:11.0) like Gecko', 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107
Safari/537.36', 'ccmhttp', 'RestSharp/100.0.0.0', 'Apache-HttpClient/4.5.2 (Java/1.8.0_211)', 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36', 'Micro Focus Common Client/1.16.1', 'NewRelic-
JavaAgent/5.4.0 (java 1.8.0_222 amd64)') GROUP BY user_agent
```

✓ | View Results | 2022-07-07 18:57 (UTC) to 2022-07-14 18:57 (UTC) | By: David Torres | 54 Events

Notes - 2022-07-14 19:03 (UTC)

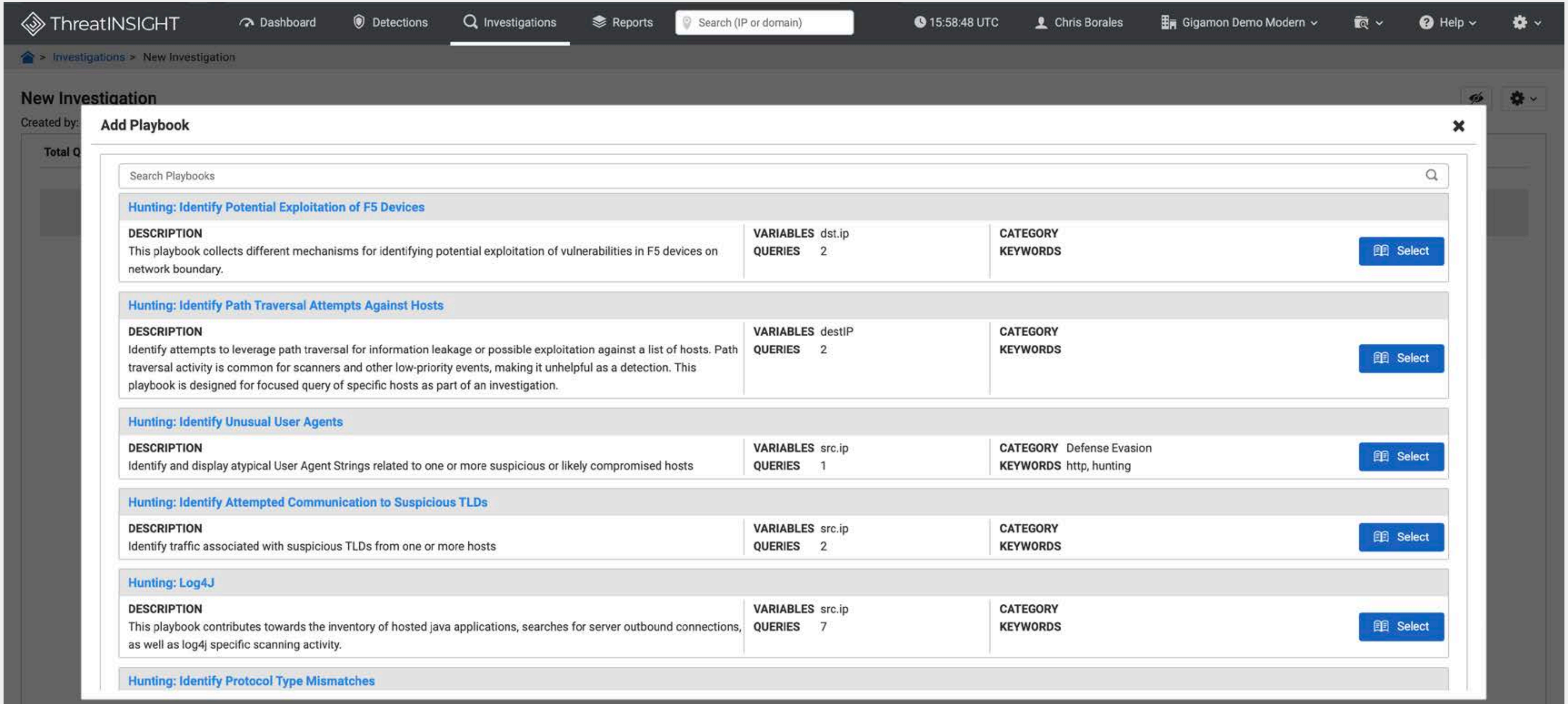
David Torres:
Continue to investigate metadata from top 3 User Agents found :

-MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT

-Microsoft-WNS/10.0

-WinHTTP loader/1.0

Playbooks



Add Playbook

Hunting: Identify Potential Exploitation of F5 Devices

DESCRIPTION
This playbook collects different mechanisms for identifying potential exploitation of vulnerabilities in F5 devices on network boundary.
VARIABLES dst.ip
QUERIES 2
CATEGORY
KEYWORDS

Hunting: Identify Path Traversal Attempts Against Hosts

DESCRIPTION
Identify attempts to leverage path traversal for information leakage or possible exploitation against a list of hosts. Path traversal activity is common for scanners and other low-priority events, making it unhelpful as a detection. This playbook is designed for focused query of specific hosts as part of an investigation.
VARIABLES destIP
QUERIES 2
CATEGORY
KEYWORDS

Hunting: Identify Unusual User Agents

DESCRIPTION
Identify and display atypical User Agent Strings related to one or more suspicious or likely compromised hosts
VARIABLES src.ip
QUERIES 1
CATEGORY Defense Evasion
KEYWORDS http, hunting

Hunting: Identify Attempted Communication to Suspicious TLDs

DESCRIPTION
Identify traffic associated with suspicious TLDs from one or more hosts
VARIABLES src.ip
QUERIES 2
CATEGORY
KEYWORDS

Hunting: Log4J

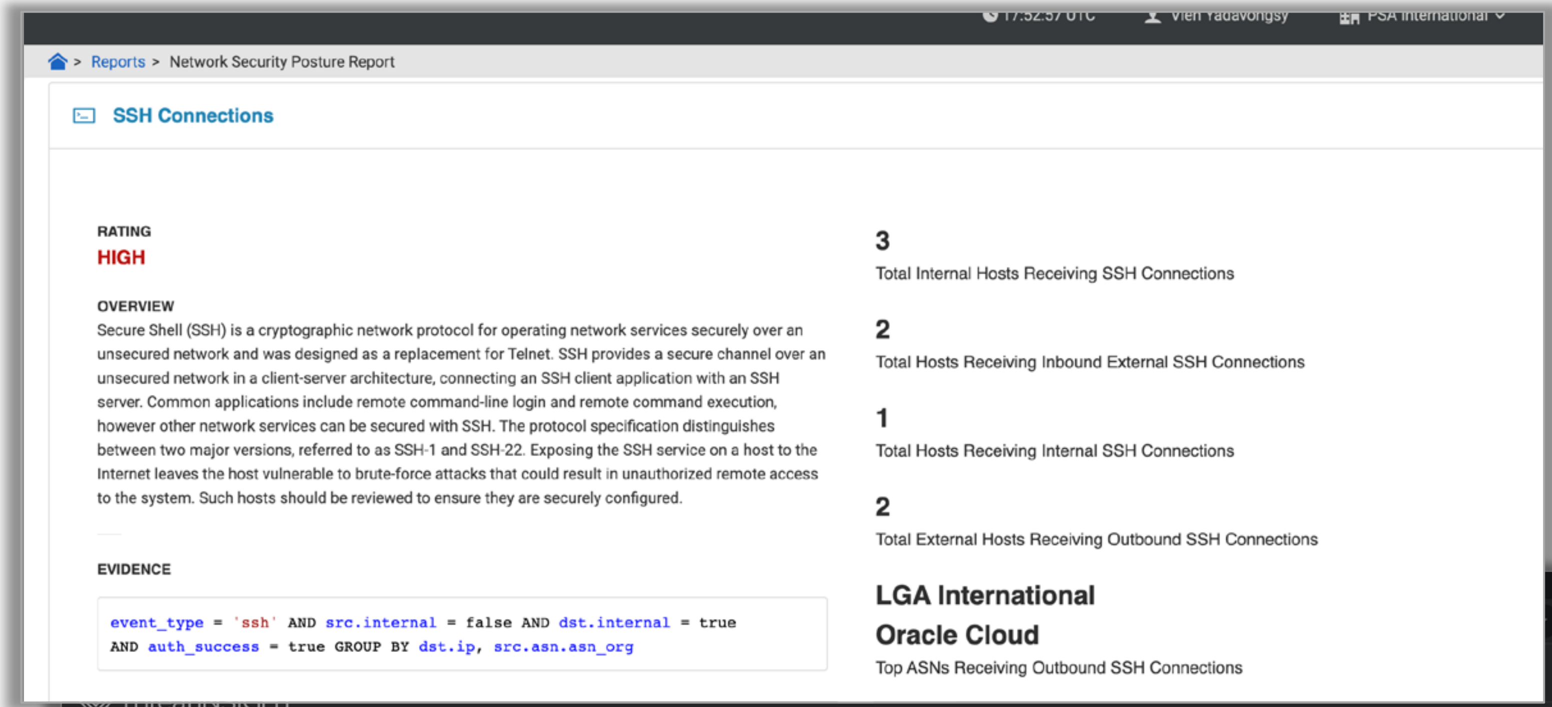
DESCRIPTION
This playbook contributes towards the inventory of hosted java applications, searches for server outbound connections, as well as log4j specific scanning activity.
VARIABLES src.ip
QUERIES 7
CATEGORY
KEYWORDS

Hunting: Identify Protocol Type Mismatches

Developed FortiGuard Applied Threat Research (ATR) team, Guided Playbooks are based on real-world attacker behavior and are refined based on the latest threat intelligence.

Reports

- 2 pre-configured report types
    - Network Security Posture Report
    - Detections Report
- Reports features
    - High-level summary
    - Interactive links within report
    - Exact queries provided
    - Printable to PDF
- Report date range
    - 7 days by default
    - Up to 3 months



17:52:57 UTC Vien Yadavongsy PSA International

Reports > Network Security Posture Report

SSH Connections

RATING

HIGH

OVERVIEW

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network and was designed as a replacement for Telnet. SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login and remote command execution, however other network services can be secured with SSH. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-22. Exposing the SSH service on a host to the Internet leaves the host vulnerable to brute-force attacks that could result in unauthorized remote access to the system. Such hosts should be reviewed to ensure they are securely configured.

EVIDENCE

```
event_type = 'ssh' AND src.internal = false AND dst.internal = true
AND auth_success = true GROUP BY dst.ip, src.asn.asn_org
```

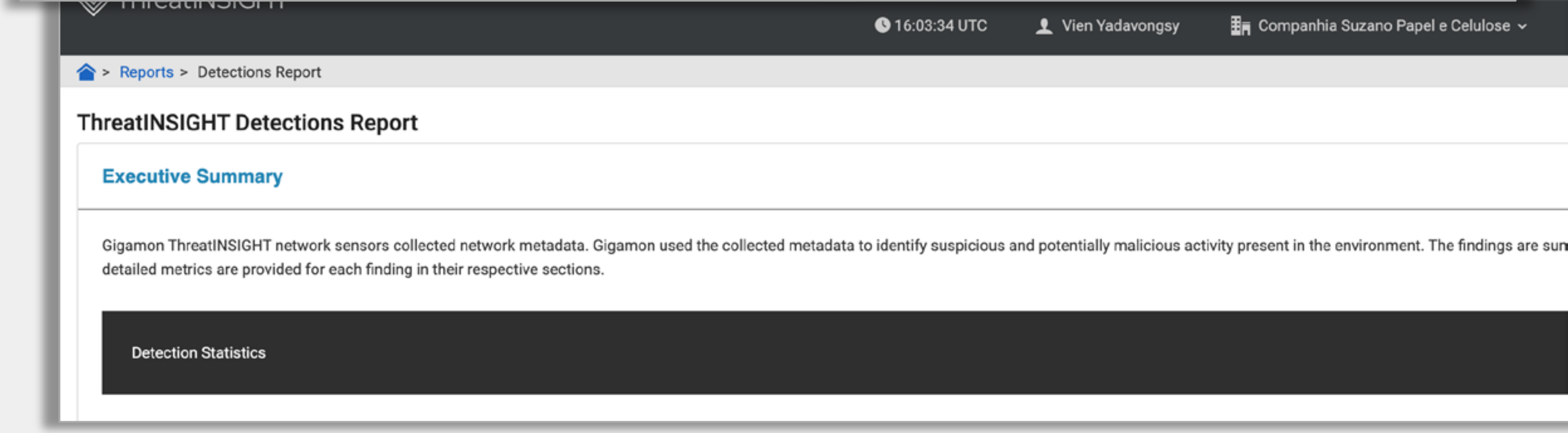
3
Total Internal Hosts Receiving SSH Connections

2
Total Hosts Receiving Inbound External SSH Connections

1
Total Hosts Receiving Internal SSH Connections

2
Total External Hosts Receiving Outbound SSH Connections

LGA International
Oracle Cloud
Top ASNs Receiving Outbound SSH Connections



ThreatINSIGHT

16:03:34 UTC Vien Yadavongsy Companhia Suzano Papel e Celulose

Reports > Detections Report

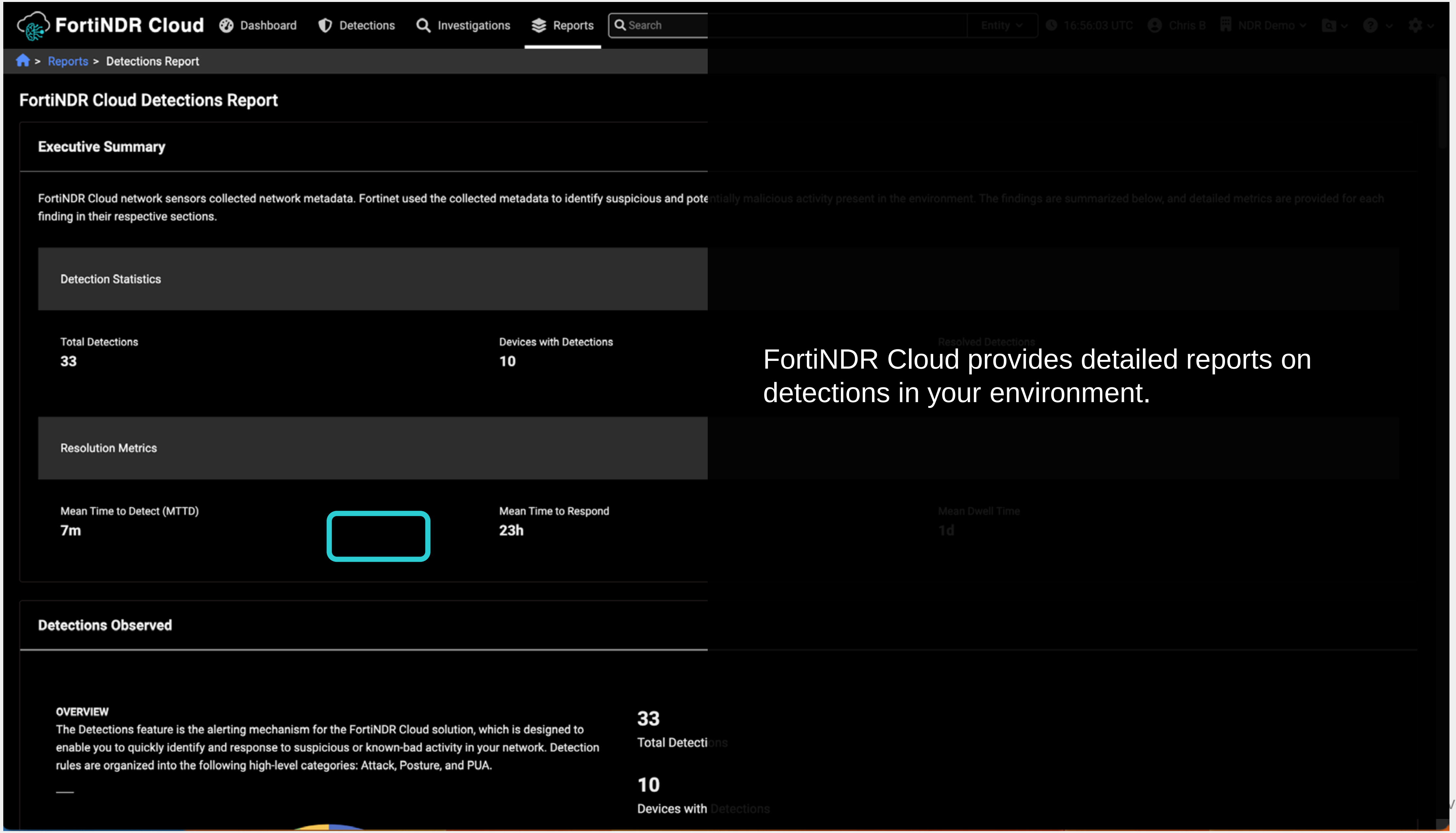
ThreatINSIGHT Detections Report

Executive Summary

Gigamon ThreatINSIGHT network sensors collected network metadata. Gigamon used the collected metadata to identify suspicious and potentially malicious activity present in the environment. The findings are sum
detailed metrics are provided for each finding in their respective sections.

Detection Statistics

Reporting



FortiNDR Cloud Detections Report

Executive Summary

FortiNDR Cloud network sensors collected network metadata. Fortinet used the collected metadata to identify suspicious and potentially malicious activity present in the environment. The findings are summarized below, and detailed metrics are provided for each finding in their respective sections.

Detection Statistics

Total Detections
33

Devices with Detections
10

Resolved Detections

Resolution Metrics

Mean Time to Detect (MTTD)
7m

Mean Time to Respond
23h

Mean Dwell Time
1d

Detections Observed

OVERVIEW

The Detections feature is the alerting mechanism for the FortiNDR Cloud solution, which is designed to enable you to quickly identify and response to suspicious or known-bad activity in your network. Detection rules are organized into the following high-level categories: Attack, Posture, and PUA.

33
Total Detections

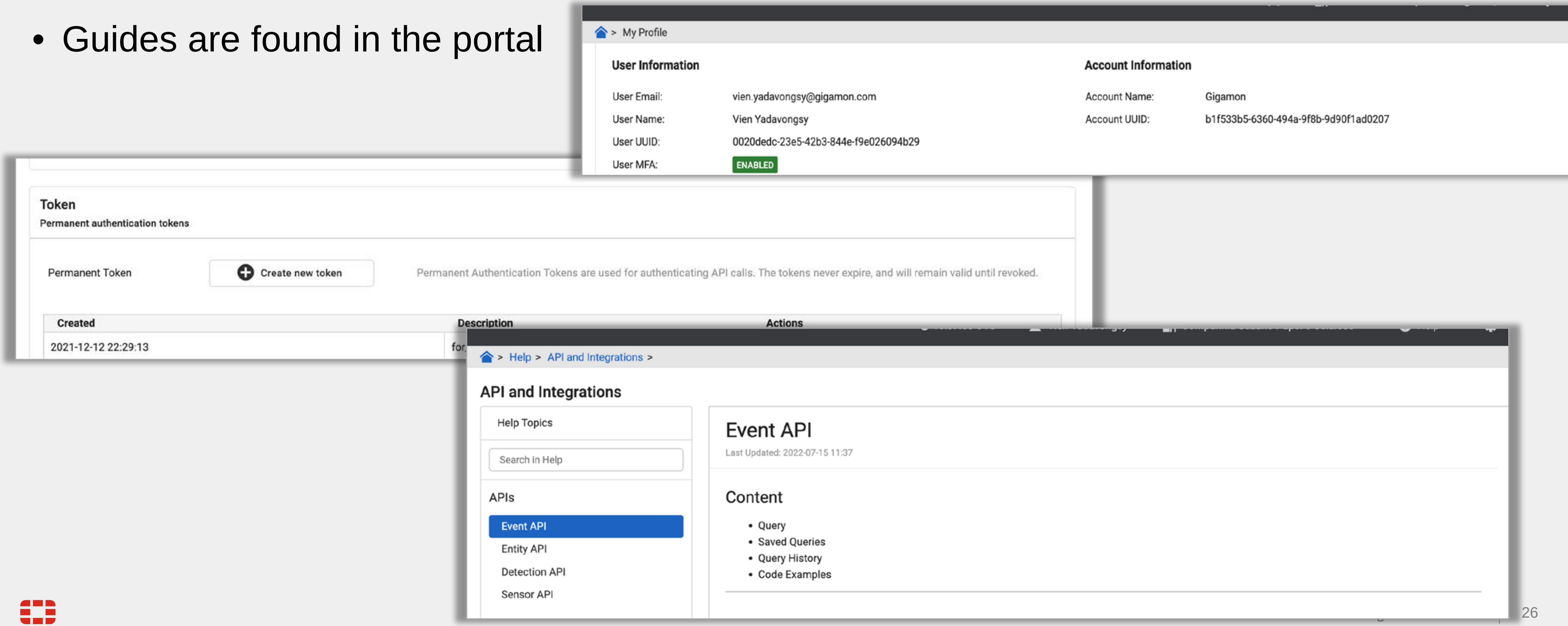
10
Devices with Detections

FortiNDR Cloud provides detailed reports on detections in your environment.

API

Working with API’s

- Gather your personal token from My Profile page
- Guides are found in the portal



> My Profile

User Information

User Email:	vien.yadavongsy@gigamon.com
User Name:	Vien Yadavongsy
User UUID:	0020dedc-23e5-42b3-844e-f9e026094b29
User MFA:	ENABLED

Account Information

Account Name:	Gigamon
Account UUID:	b1f533b5-6360-494a-9f8b-9d90f1ad0207

Token

Permanent authentication tokens

Permanent Token — Create new token

Permanent Authentication Tokens are used for authenticating API calls. The tokens never expire, and will remain valid until revoked.

Created	Description	Actions
2021-12-12 22:29:13	for,	

> Help > API and Integrations >

API and Integrations

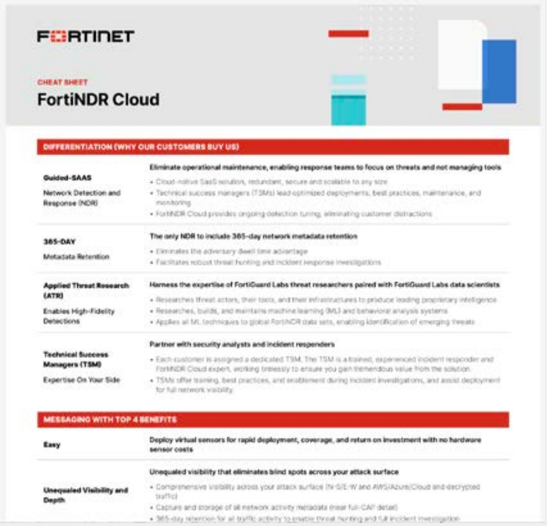
Event API

Last Updated: 2022-07-15 11:37

Content

- Query
- Saved Queries
- Query History
- Code Examples

Available Resources



FORTINET

CHEAT SHEET

FortiNDR Cloud

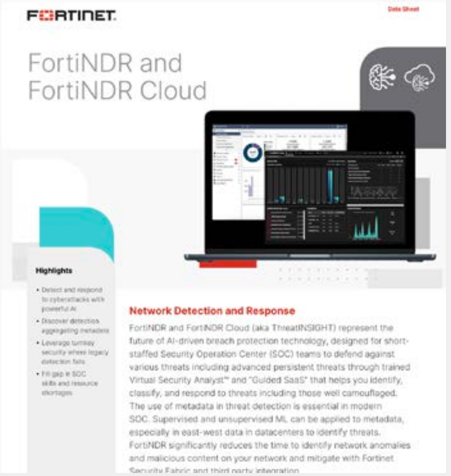
DIFFERENTIATION (WHY OUR CUSTOMERS BUY US)

Guided-SAAS **Network Detection and Response (NDR)**	**Eliminate operational maintenance, enabling response teams to focus on threats and not managing tools** - Cloud-native SaaS solution, redundant, secure and scalable to any size - Technical success managers (TSMs) lead optimized deployments, best practices, maintenance, and monitoring - FortiNDR Cloud provides ongoing detection tuning, eliminating customer distractions
365-DAY **Metadata Retention**	**The only NDR to include 365-day network metadata retention** - Eliminates the adversary dwell time advantage - Facilitates robust threat hunting and incident response investigations
Applied Threat Research (ATR) **Enables High-Fidelity Detections**	**Harness the expertise of FortiGuard Labs threat researchers paired with FortiGuard Labs data scientists** - Researches threat actors, their tools, and their infrastructures to produce leading proprietary intelligence - Researches, builds, and maintains machine learning (ML) and behavioral analysis systems - Applies all ML techniques to global FortiNDR data sets, enabling identification of emerging threats
Technical Success Managers (TSM) **Expertise On Your Side**	**Partner with security analysts and incident responders** - Each customer is assigned a dedicated TSM. The TSM is a trained, experienced incident responder and FortiNDR Cloud expert, working tirelessly to ensure you gain tremendous value from the solution. - TSMs offer training, best practices, and enablement during incident investigations, and assist deployment for full network visibility

MESSAGING WITH TOP 4 BENEFITS

Easy	**Deploy virtual sensors for rapid deployment, coverage, and return on investment with no hardware sensor costs**
Unequaled Visibility and Depth	**Unequaled visibility that eliminates blind spots across your attack surface** - Comprehensive visibility across your attack surface (N-S/E-W and AWS/Azure/Cloud and decrypted traffic) - Capture and storage of all network activity metadata (near full-CAP detail) - 365-day retention for all traffic activity to enable threat hunting and full incident investigation

FortiNDR Cloud Cheat Sheet



FORTINET

Data Sheet

FortiNDR and FortiNDR Cloud

Highlights

- Detect and respond to cyberattacks with powerful AI
- Discover detection aggregating metadata
- Leverage turnkey security where legacy detection fails
- Fill gap in SOC skills and resource shortages

Network Detection and Response

FortiNDR and FortiNDR Cloud (aka ThreatINSIGHT) represent the future of AI-driven breach protection technology, designed for short-staffed Security Operation Center (SOC) teams to defend against various threats including advanced persistent threats through trained Virtual Security Analyst™ and "Guided SaaS" that helps you identify, classify, and respond to threats including those well camouflaged. The use of metadata in threat detection is essential in modern SOC. Supervised and unsupervised ML can be applied to metadata, especially in east-west data in datacenters to identify threats. FortiNDR significantly reduces the time to identify network anomalies and malicious content on your network and mitigate with Fortinet Security Fabric and third party integration.

FortiNDR Data Sheet

ORDERING GUIDE

FORTINET

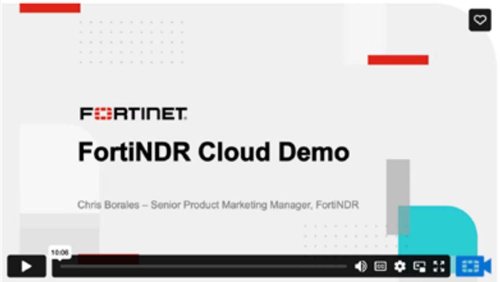
FortiNDR

Product Offerings

FortiNDR and FortiNDR Cloud (aka ThreatINSIGHT) represents the future of artificial intelligence-driven breach protection technology, designed for short-staffed Security Operation Center (SOC) teams to defend against various threats including advanced persistent threats through trained Virtual Security AnalystTM and "Guided SaaS" that helps you identify, classify, and respond to threats including those well camouflaged. The use of metadata in detection of threats is essential in modern SOC. Supervised and unsupervised ML can be applied to metadata, especially in East-West data in datacentres to identify threats.

	FORTINDR 3500F	FORTINDR VM16/32	FORTINDRCLOUD-100F (SMALL SENSORS)	FORTINDR CLOUD 1000F (LARGE SENSORS)	FORTINDRCLOUD VIRTUAL SENSORS
Features					
Sniffer/SPAN/RSS Support	✓	✓	✓	✓	✓
SaaS Portal with Sensors			✓	✓	✓
Local Deployment (No Data Offshore)	✓	✓			
Security Services					
NDR Throughput	[illegible]	Hypervisor dependent	2 Gbps (metadata processing)	10 Gbps (metadata processing)	Hypervisor dependent
Malware Analysis Throughput	100K files per hour	[illegible]	Hash lookup (ITI in SaaS)	Hash lookup (ITI in SaaS)	Hash lookup (ITI in SaaS)
Artificial Neural Networks (ANN) Engine Update	✓	✓	N/A	N/A	N/A
FortiNDR Updates	✓	✓	✓	✓	✓
Attack Scenarios Detection (Malware)	✓	✓	N/A	N/A	N/A
Data Retention	Local (HDD dependent)	Local (HDD dependent)	365 days in cloud	365 days in cloud	365 days in cloud
Investigation/Threat Hunting	Limited	Limited	Full featured	Full featured	Full featured
Additional Services					
24x7 Support	Included	Included	Included	Included	Included
Technical Service Manager (TSM) guided SaaS	N/A	N/A	Included	Included	Included

FortiNDR Ordering Guide



FORTINET

FortiNDR Cloud Demo

Chris Borales – Senior Product Marketing Manager, FortiNDR

FortiNDR Cloud High Level Demo

FORTINET®