Check Point®
SOFTWARE TECHNOLOGIES LTD

INTRODUCING CLOUDGUARD NDR

FULL PREVENTION CYCLE:
Network Detection and Response

Network Detection and Response

Uses non-signature-based techniques to detect suspicious traffic on enterprise networks

Models normal network traffic and highlight suspicious traffic that falls outside the normal range

Monitors and analyzes north/south traffic, as well as east/west traffic (as it moves laterally throughout the network).

Provides automatic or manual response capabilities to react to the detection of suspicious network traffic

Definition source: Gartner
(Previous name: Network Traffic Analysis)

Gartner Analysis of The Market

TBD

Jonathan

CloudGuard NDR

Security

Security that creates security – Context based Prevention!

Automated

Automated tailored security and full automation for the NDR closed cycle

Everywhere

Network, Cloud, Endpoints, Mobile, IoT, and More – on a Single-pane-of-glass

01

Recurrent Connections

Use time to find devices repeatedly connecting to a rare external destinations hosted on suspicious infrastructure

02

Geo Anomalies

Use out of ordinary connections to detect potential attacks

03

Behavioral Anomalies

Find spikes in regular daily work to detect abnormal behavior, unsolicited network reconnaissance and lateral movement attempts

04

Vulnerability Sonar

(Patent)

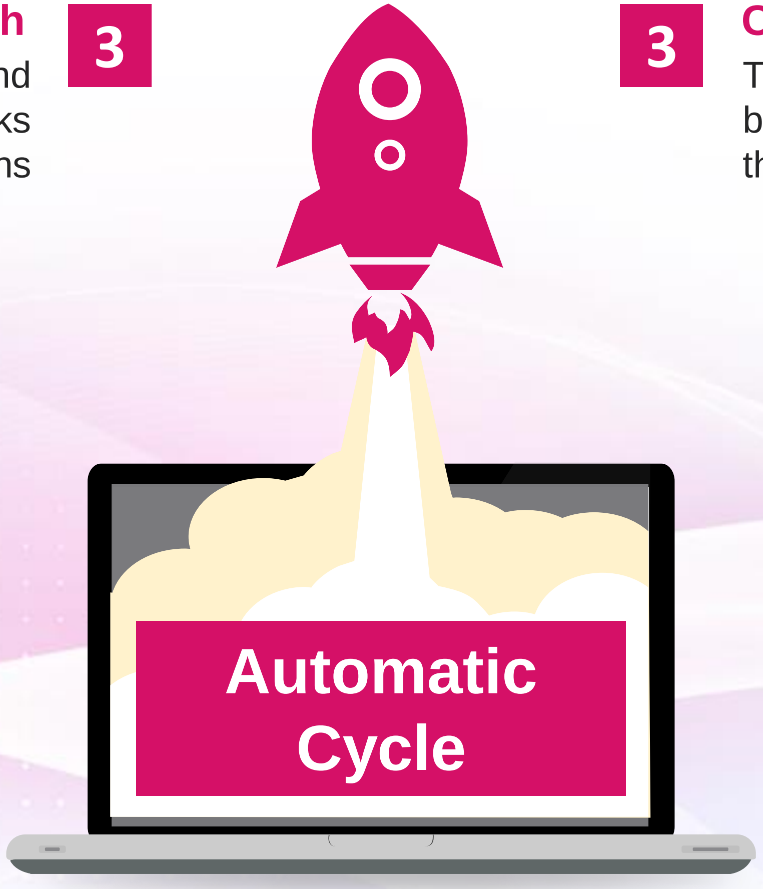
Analyze the response given to external scanners and deduces which of the scans actually found a vulnerability, and to which servers

05

User behavioral anomalies

Find anomalies in user behavior to detect escalation of privilege and credential compromise attempts

The Full Cycle



Automatic Cycle

1 **Aggregate customer’s logs**

Select and group logs into desired features.

2 **Find Spikes**

Find spikes in the data, by configurable order of magnitude

3 **Correlate and Enrich**

Use reputation, white listing, and more data to distil potential attacks from benign connections

1 **Create Indicators for Each Suspicious Connection**

Automatic feed creation

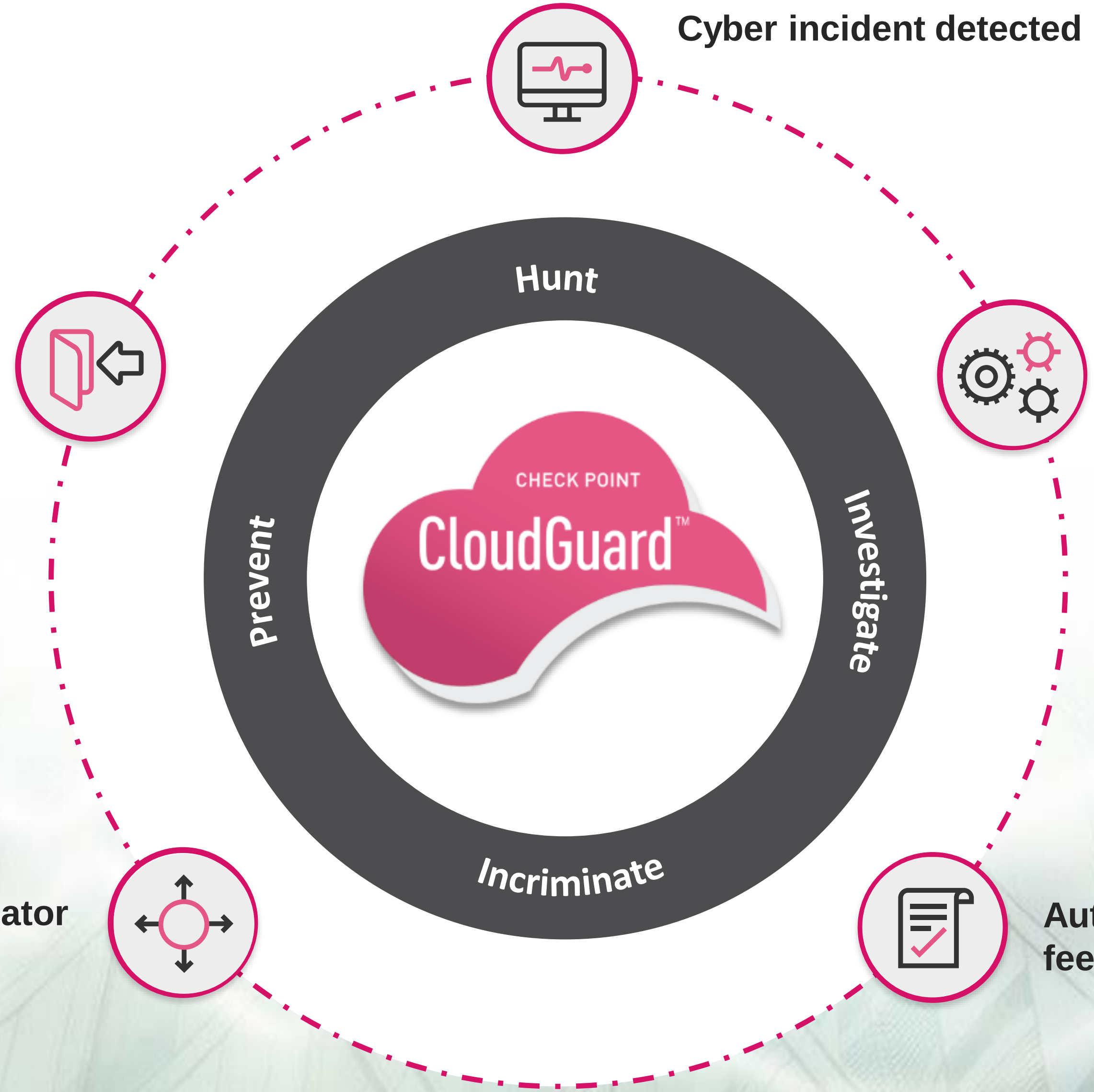
2 **Log and Alert**

Maintain dashboards, reports and alerts to communicate the detection to the customer

3 **Consume The Feed**

The created feed can be consumed by any Check Point product – so the attack is prevented.

Cloudguard NDR Closed-Loop Cycle



Cyber incident detected

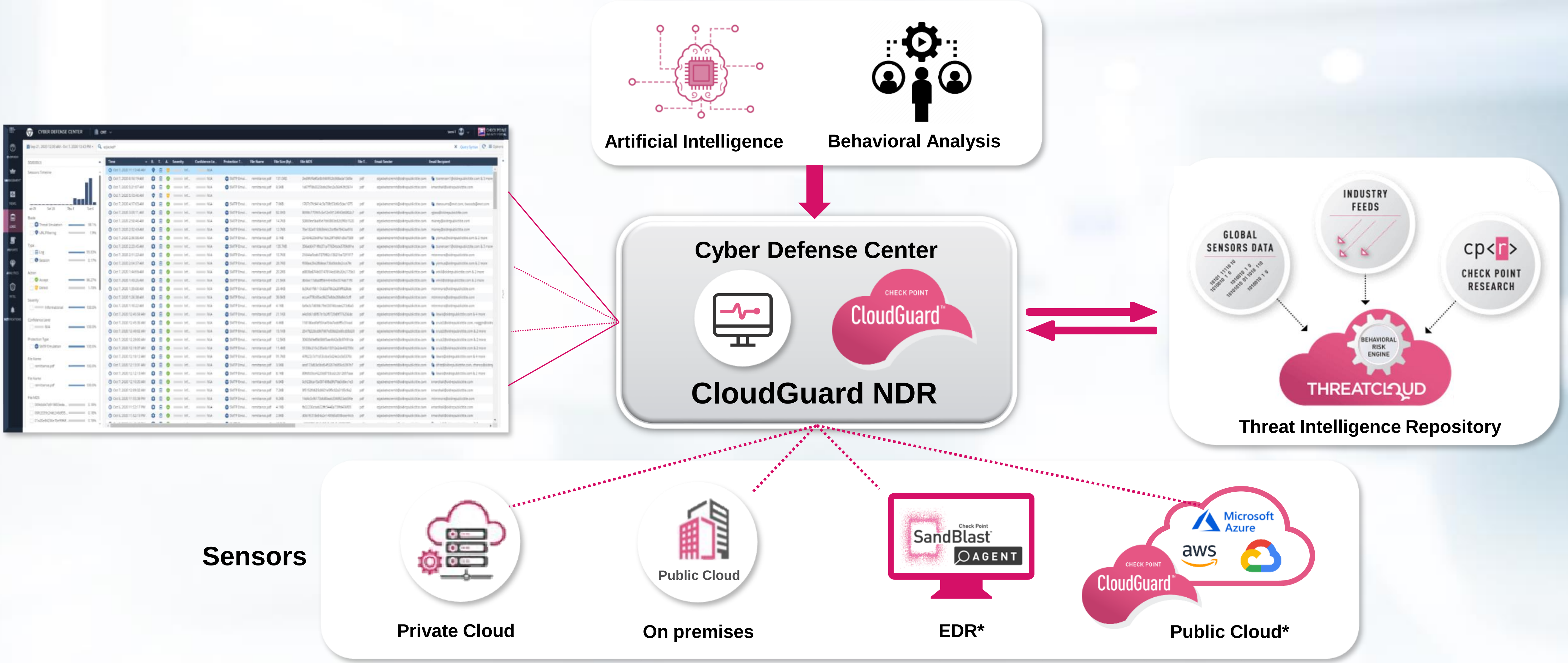
Automated triage, pivoting and enrichment of attack data

Automated and manual indicator feeds creation and publication

Automated distribution of threat indicator feeds across all security solutions

- Threat prevented by inline solutions
- “Red Button” - Prevent mode*

Cloudguard NDR High Level Architecture



Artificial Intelligence

Behavioral Analysis

Cyber Defense Center

CloudGuard NDR

Threat Intelligence Repository

Sensors

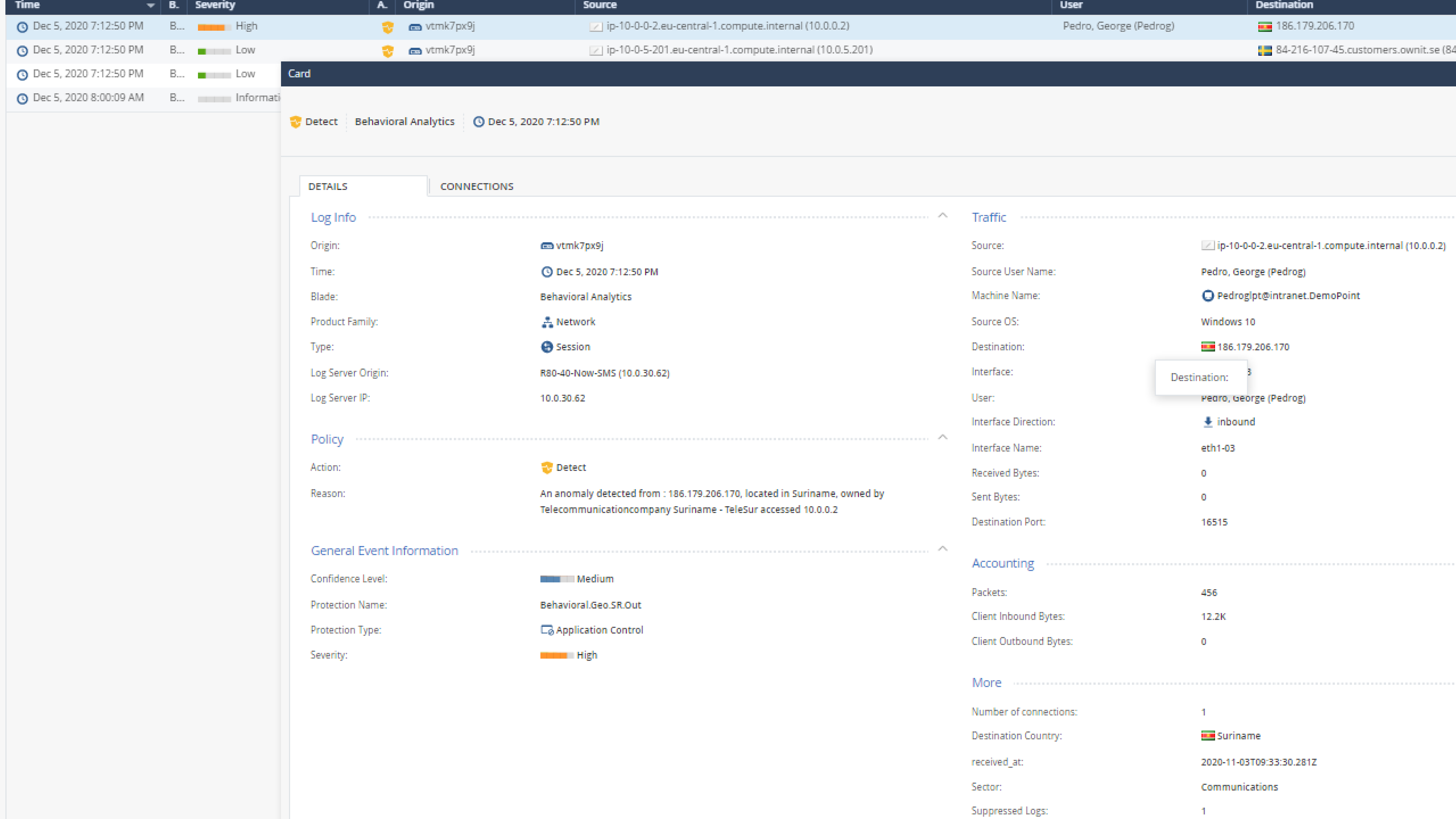
Private Cloud

On premises

EDR*

Public Cloud*

* Azure and Endpoint are roadmap



Time	B.	Severity	A.	Origin	Source	User	Destination
Dec 5, 2020 7:12:50 PM	B...	High		vtmk7px9j	ip-10-0-0-2.eu-central-1.compute.internal (10.0.0.2)	Pedro, George (Pedrog)	186.179.206.170
Dec 5, 2020 7:12:50 PM	B...	Low		vtmk7px9j	ip-10-0-5-201.eu-central-1.compute.internal (10.0.5.201)		84-216-107-45.customers.ownit.se (84
Dec 5, 2020 7:12:50 PM	B...	Low					
Dec 5, 2020 8:00:09 AM	B...	Informati					

Card

Detect | Behavioral Analytics | Dec 5, 2020 7:12:50 PM

Log Info

Origin: vtmk7px9j
Time: Dec 5, 2020 7:12:50 PM
Blade: Behavioral Analytics
Product Family: Network
Type: Session
Log Server Origin: R80-40-Now-SMS (10.0.30.62)
Log Server IP: 10.0.30.62

Policy

Action: Detect
Reason: An anomaly detected from : 186.179.206.170, located in Suriname, owned by Telecommunicationcompany Suriname - TeleSur accessed 10.0.0.2

General Event Information

Confidence Level: Medium
Protection Name: Behavioral.Geo.SR.Out
Protection Type: Application Control
Severity: High

Traffic

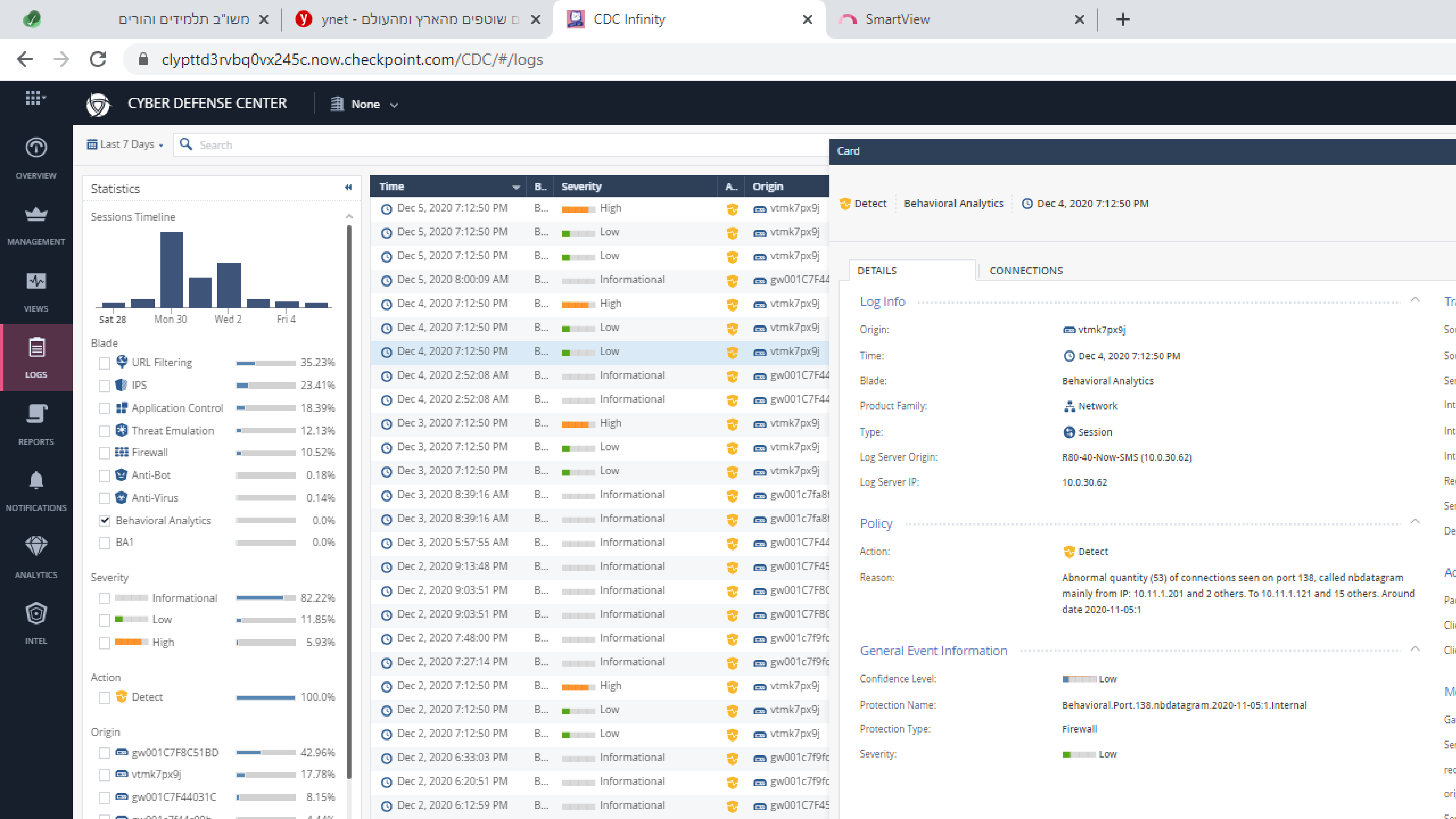
Source: ip-10-0-0-2.eu-central-1.compute.internal (10.0.0.2)
Source User Name: Pedro, George (Pedrog)
Machine Name: Pedroglpt@intranet.DemoPoint
Source OS: Windows 10
Destination: 186.179.206.170
Interface: 3
Destination:
User: Pedro, George (Pedrog)
Interface Direction: inbound
Interface Name: eth1-03
Received Bytes: 0
Sent Bytes: 0
Destination Port: 16515

Accounting

Packets: 456
Client Inbound Bytes: 12.2K
Client Outbound Bytes: 0

More

Number of connections: 1
Destination Country: Suriname
received_at: 2020-11-03T09:33:30.281Z
Sector: Communications
Suppressed Logs: 1



משו"ב תלמידים והורים ✕ | ynet - שוטפים מהארץ ומהעולם ✕ | CDC Infinity ✕ | SmartView ✕ | +

clypttd3rvbq0vx245c.now.checkpoint.com/CDC/#/logs

CYBER DEFENSE CENTER | None

Last 7 Days | Search

Statistics

Sessions Timeline

Sat 28 | Mon 30 | Wed 2 | Fri 4

Blade

□ URL Filtering		35.23%
□ IPS		23.41%
□ Application Control		18.39%
□ Threat Emulation		12.13%
□ Firewall		10.52%
□ Anti-Bot		0.18%
□ Anti-Virus		0.14%
☑ Behavioral Analytics		0.0%
□ BA1		0.0%

Severity

□ Informational		82.22%
□ Low		11.85%
□ High		5.93%

Action

□ Detect		100.0%

Origin

□ gw001C7F8C51BD		42.96%
□ vtmk7px9j		17.78%
□ gw001C7F44031C		8.15%

Time	B..	Severity	A..	Origin
Dec 5, 2020 7:12:50 PM	B...	High		vtmk7px9j
Dec 5, 2020 7:12:50 PM	B...	Low		vtmk7px9j
Dec 5, 2020 7:12:50 PM	B...	Low		vtmk7px9j
Dec 5, 2020 8:00:09 AM	B...	Informational		gw001C7F44
Dec 4, 2020 7:12:50 PM	B...	High		vtmk7px9j
Dec 4, 2020 7:12:50 PM	B...	Low		vtmk7px9j
Dec 4, 2020 7:12:50 PM	B...	Low		vtmk7px9j
Dec 4, 2020 2:52:08 AM	B...	Informational		gw001C7F44
Dec 4, 2020 2:52:08 AM	B...	Informational		gw001C7F44
Dec 3, 2020 7:12:50 PM	B...	High		vtmk7px9j
Dec 3, 2020 7:12:50 PM	B...	Low		vtmk7px9j
Dec 3, 2020 7:12:50 PM	B...	Low		vtmk7px9j
Dec 3, 2020 8:39:16 AM	B...	Informational		gw001c7fa8
Dec 3, 2020 8:39:16 AM	B...	Informational		gw001c7fa8
Dec 3, 2020 5:57:55 AM	B...	Informational		gw001C7F44
Dec 2, 2020 9:13:48 PM	B...	Informational		gw001C7F45
Dec 2, 2020 9:03:51 PM	B...	Informational		gw001C7F8C
Dec 2, 2020 9:03:51 PM	B...	Informational		gw001C7F8C
Dec 2, 2020 7:48:00 PM	B...	Informational		gw001c7f9fc
Dec 2, 2020 7:27:14 PM	B...	Informational		gw001c7f9fc
Dec 2, 2020 7:12:50 PM	B...	High		vtmk7px9j
Dec 2, 2020 7:12:50 PM	B...	Low		vtmk7px9j
Dec 2, 2020 7:12:50 PM	B...	Low		vtmk7px9j
Dec 2, 2020 6:33:03 PM	B...	Informational		gw001c7f9fc
Dec 2, 2020 6:20:51 PM	B...	Informational		gw001c7f9fc
Dec 2, 2020 6:12:59 PM	B...	Informational		gw001C7F45

Card

Detect | Behavioral Analytics | Dec 4, 2020 7:12:50 PM

DETAILS | CONNECTIONS

Log Info

Origin:	vtmk7px9j
Time:	Dec 4, 2020 7:12:50 PM
Blade:	Behavioral Analytics
Product Family:	Network
Type:	Session
Log Server Origin:	R80-40-Now-SMS (10.0.30.62)
Log Server IP:	10.0.30.62

Policy

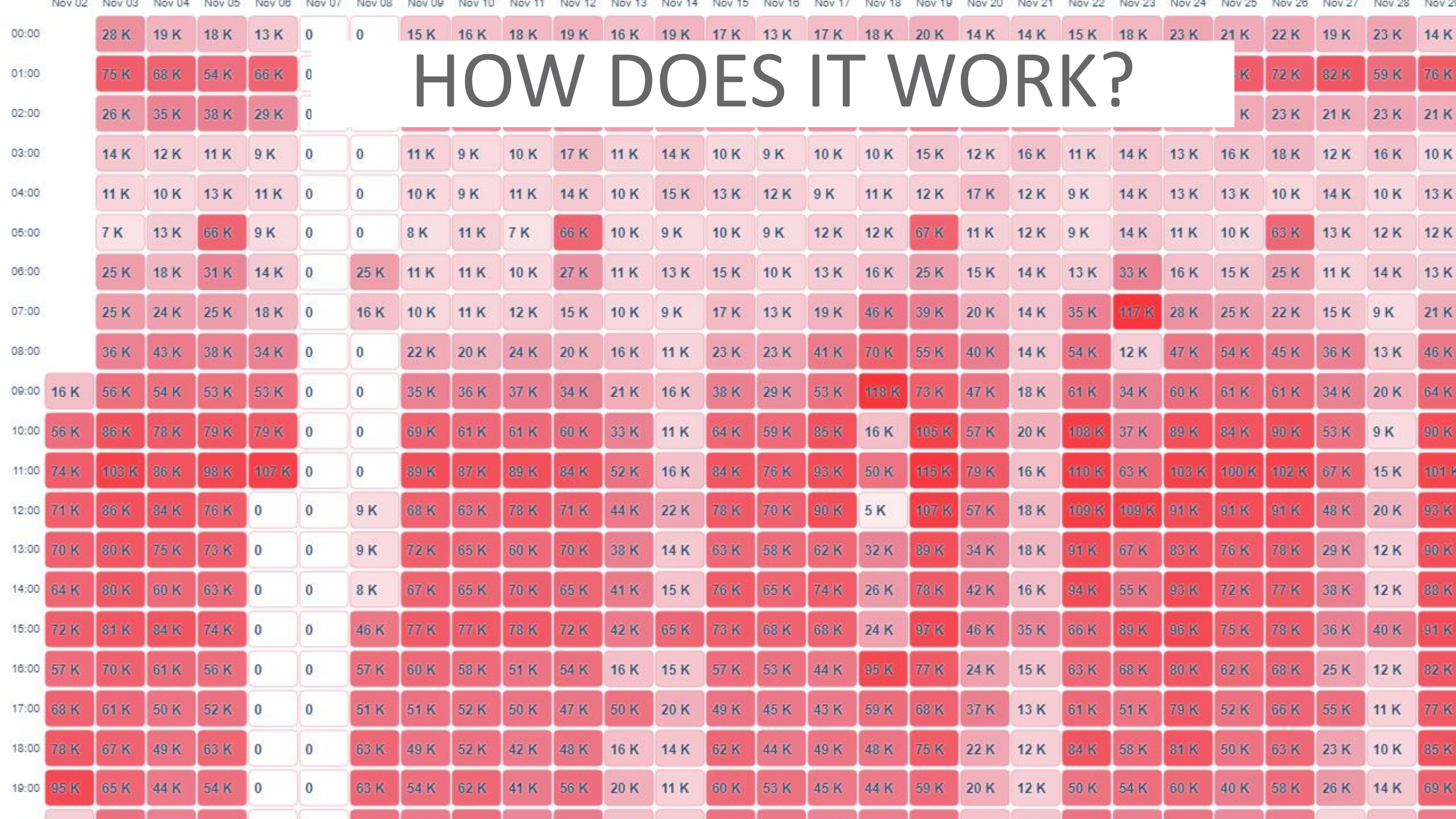
Action:	Detect
Reason:	Abnormal quantity (53) of connections seen on port 138, called nbdatagram mainly from IP: 10.11.1.201 and 2 others. To 10.11.1.121 and 15 others. Around date 2020-11-05:1

General Event Information

Confidence Level:	Low
Protection Name:	Behavioral.Port.138.nbdatagram.2020-11-05:1.Internal
Protection Type:	Firewall
Severity:	Low

Tr
So
So
Se
Int
Int
Int
Re
Se
De
Ac
Pa
Cli
Cli
M
Ga
Se
rec
ori

HOW DOES IT WORK?



	Nov 02	Nov 03	Nov 04	Nov 05	Nov 06	Nov 07	Nov 08	Nov 09	Nov 10	Nov 11	Nov 12	Nov 13	Nov 14	Nov 15	Nov 16	Nov 17	Nov 18	Nov 19	Nov 20	Nov 21	Nov 22	Nov 23	Nov 24	Nov 25	Nov 26	Nov 27	Nov 28	Nov 2
00:00		28 K	19 K	18 K	13 K	0	0	15 K	16 K	18 K	19 K	16 K	19 K	17 K	13 K	17 K	18 K	20 K	14 K	14 K	15 K	18 K	23 K	21 K	22 K	19 K	23 K	14 K
01:00		75 K	68 K	54 K	66 K	0																		K	72 K	82 K	59 K	76 K
02:00		26 K	35 K	38 K	29 K	0																		K	23 K	21 K	23 K	21 K
03:00		14 K	12 K	11 K	9 K	0	0	11 K	9 K	10 K	17 K	11 K	14 K	10 K	9 K	10 K	10 K	15 K	12 K	16 K	11 K	14 K	13 K	16 K	18 K	12 K	16 K	10 K
04:00		11 K	10 K	13 K	11 K	0	0	10 K	9 K	11 K	14 K	10 K	15 K	13 K	12 K	9 K	11 K	12 K	17 K	12 K	9 K	14 K	13 K	13 K	10 K	14 K	10 K	13 K
05:00		7 K	13 K	66 K	9 K	0	0	8 K	11 K	7 K	66 K	10 K	9 K	10 K	9 K	12 K	12 K	67 K	11 K	12 K	9 K	14 K	11 K	10 K	63 K	13 K	12 K	12 K
06:00		25 K	18 K	31 K	14 K	0	25 K	11 K	11 K	10 K	27 K	11 K	13 K	15 K	10 K	13 K	16 K	25 K	15 K	14 K	13 K	33 K	16 K	15 K	25 K	11 K	14 K	13 K
07:00		25 K	24 K	25 K	18 K	0	16 K	10 K	11 K	12 K	15 K	10 K	9 K	17 K	13 K	19 K	46 K	39 K	20 K	14 K	35 K	117 K	28 K	25 K	22 K	15 K	9 K	21 K
08:00		36 K	43 K	38 K	34 K	0	0	22 K	20 K	24 K	20 K	16 K	11 K	23 K	23 K	41 K	70 K	55 K	40 K	14 K	54 K	12 K	47 K	54 K	45 K	36 K	13 K	46 K
09:00	16 K	56 K	54 K	53 K	53 K	0	0	35 K	36 K	37 K	34 K	21 K	16 K	38 K	29 K	53 K	118 K	73 K	47 K	18 K	61 K	34 K	60 K	61 K	61 K	34 K	20 K	64 K
10:00	56 K	86 K	78 K	79 K	79 K	0	0	69 K	61 K	61 K	60 K	33 K	11 K	64 K	59 K	85 K	16 K	105 K	57 K	20 K	108 K	37 K	89 K	84 K	90 K	53 K	9 K	90 K
11:00	74 K	103 K	86 K	98 K	107 K	0	0	89 K	87 K	89 K	84 K	52 K	16 K	84 K	76 K	93 K	50 K	115 K	79 K	16 K	110 K	63 K	103 K	100 K	102 K	67 K	15 K	101 K
12:00	71 K	86 K	84 K	76 K	0	0	9 K	68 K	63 K	78 K	71 K	44 K	22 K	78 K	70 K	90 K	5 K	107 K	57 K	18 K	109 K	109 K	91 K	91 K	91 K	48 K	20 K	93 K
13:00	70 K	80 K	75 K	73 K	0	0	9 K	72 K	65 K	60 K	70 K	38 K	14 K	63 K	58 K	62 K	32 K	89 K	34 K	18 K	91 K	67 K	83 K	76 K	78 K	29 K	12 K	90 K
14:00	64 K	80 K	60 K	63 K	0	0	8 K	67 K	65 K	70 K	65 K	41 K	15 K	76 K	65 K	74 K	26 K	78 K	42 K	16 K	94 K	55 K	93 K	72 K	77 K	38 K	12 K	88 K
15:00	72 K	81 K	84 K	74 K	0	0	46 K	77 K	77 K	78 K	72 K	42 K	65 K	73 K	68 K	68 K	24 K	97 K	46 K	35 K	66 K	89 K	96 K	75 K	78 K	36 K	40 K	91 K
16:00	57 K	70 K	61 K	56 K	0	0	57 K	60 K	58 K	51 K	54 K	16 K	15 K	57 K	53 K	44 K	95 K	77 K	24 K	15 K	63 K	68 K	80 K	62 K	68 K	25 K	12 K	82 K
17:00	68 K	61 K	50 K	52 K	0	0	51 K	51 K	52 K	50 K	47 K	50 K	20 K	49 K	45 K	43 K	59 K	68 K	37 K	13 K	61 K	51 K	79 K	52 K	66 K	55 K	11 K	77 K
18:00	78 K	67 K	49 K	63 K	0	0	63 K	49 K	52 K	42 K	48 K	16 K	14 K	62 K	44 K	49 K	48 K	75 K	22 K	12 K	84 K	58 K	81 K	50 K	63 K	23 K	10 K	85 K
19:00	95 K	65 K	44 K	54 K	0	0	63 K	54 K	62 K	41 K	56 K	20 K	11 K	60 K	53 K	45 K	44 K	59 K	20 K	12 K	50 K	54 K	60 K	40 K	58 K	26 K	14 K	69 K

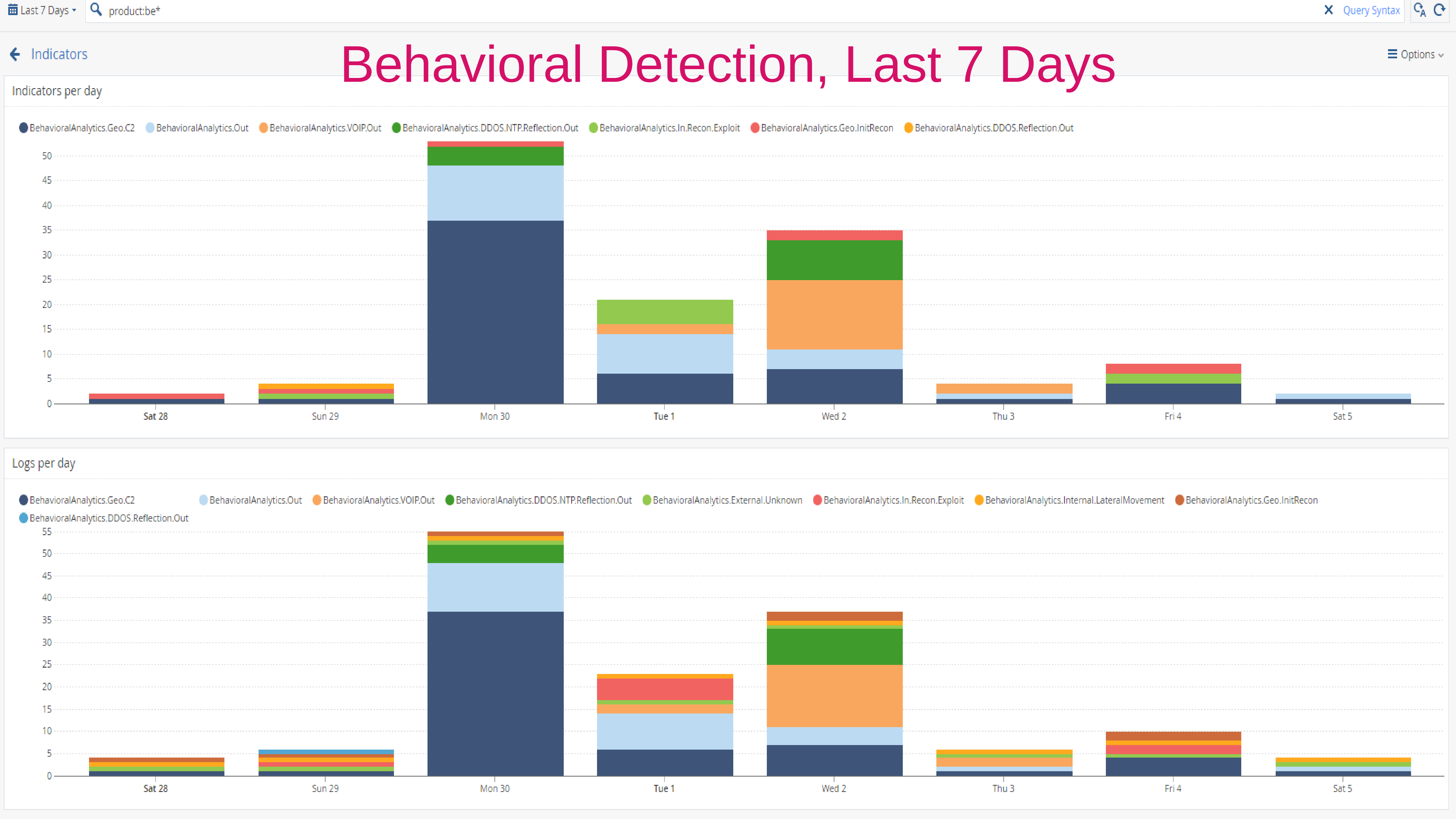
False Positive Cleanup

TBD Tami

How Do The Engines Work?

TBD Tami

Behavioral Detection, Last 7 Days



Last 7 Days
product:be*
Query Syntax
Indicators
Options

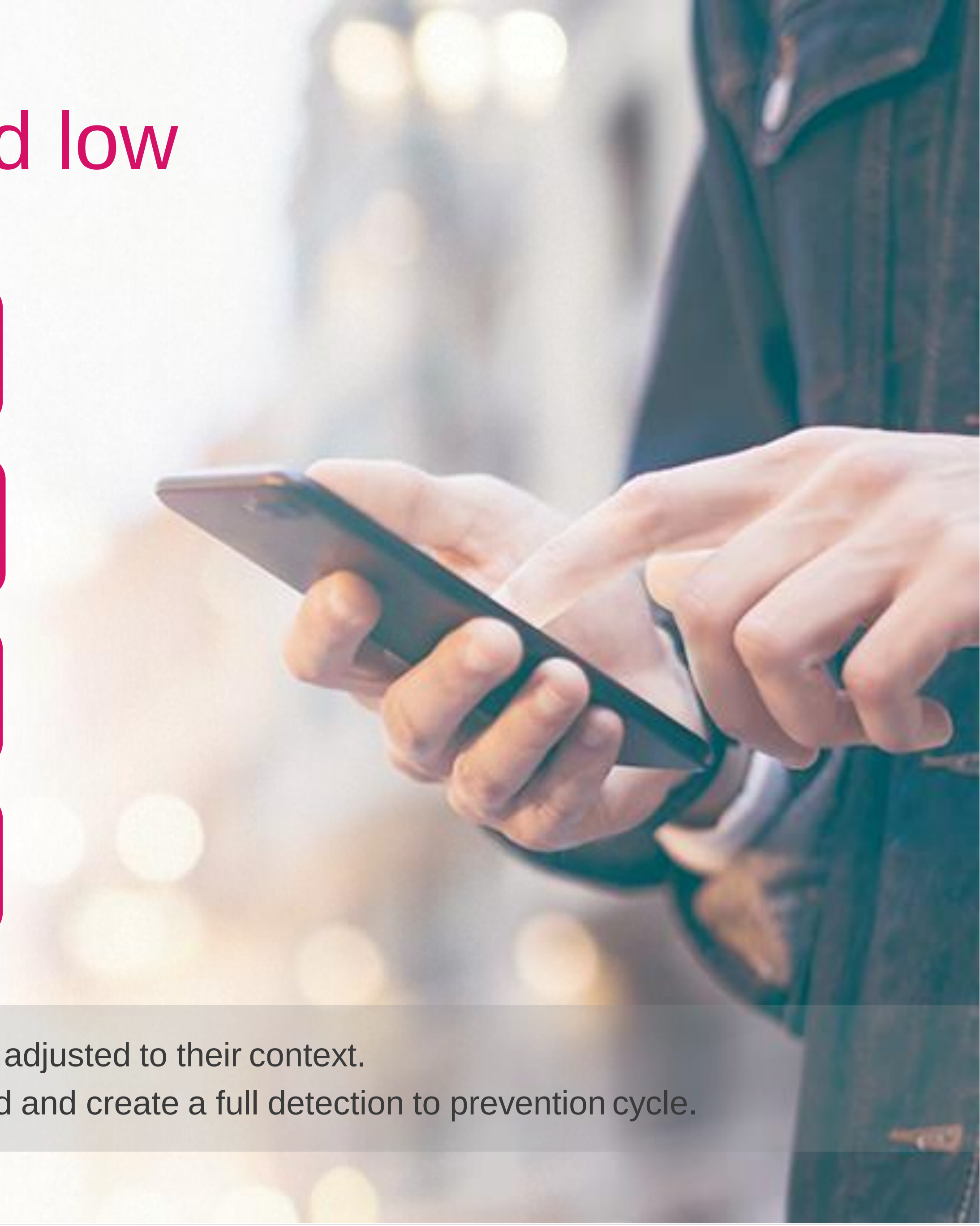
Indicators per day

● BehavioralAnalytics.Geo.C2
● BehavioralAnalytics.Out
● BehavioralAnalytics.VOIP.Out
● BehavioralAnalytics.DDOS.NTP.Reflection.Out
● BehavioralAnalytics.In.Recon.Exploit
● BehavioralAnalytics.Geo.InitRecon
● BehavioralAnalytics.DDOS.Reflection.Out
50
45
40
35
30
25
20
15
10
5
0
Sat 28
Sun 29
Mon 30
Tue 1
Wed 2
Thu 3
Fri 4
Sat 5

Logs per day

● BehavioralAnalytics.Geo.C2
● BehavioralAnalytics.Out
● BehavioralAnalytics.VOIP.Out
● BehavioralAnalytics.DDOS.NTP.Reflection.Out
● BehavioralAnalytics.External.Unknown
● BehavioralAnalytics.In.Recon.Exploit
● BehavioralAnalytics.Internal.LateralMovement
● BehavioralAnalytics.Geo.InitRecon
● BehavioralAnalytics.DDOS.Reflection.Out
55
50
45
40
35
30
25
20
15
10
5
0
Sat 28
Sun 29
Mon 30
Tue 1
Wed 2
Thu 3
Fri 4
Sat 5

Results for 50 customers – Tuned low



~300 distilled new indicators per week

20% recurrent across different customers in different geographical areas

40% repetition in the same geographical area

80% True Positives

Customers can create their own intelligence feed, automatically adjusted to their context.
Other Check Point products can automatically consume the feed and create a full detection to prevention cycle.

Examples

Financial Company – US

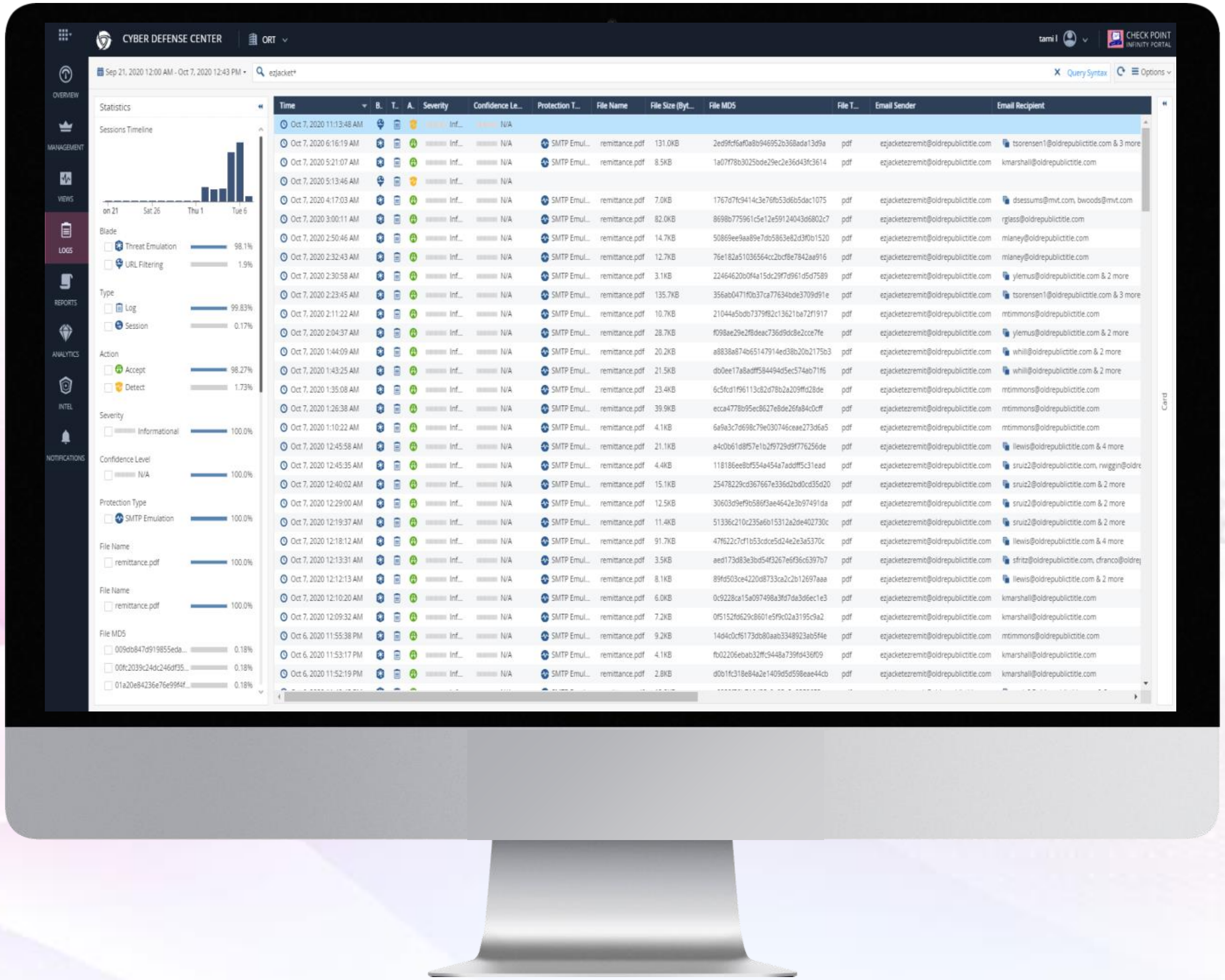
E-mail Phishing Campaign

01 **Behavioral Alert**
Anomalous activity on mail port 25

02 **Suspicious pdf attachment**
Tons of mails were sent to recipients in the company with similar title

03 **Different hashes**
Each attachment with different hash

04 **TE verdict**
TE verdict: Benign



Sep 21, 2020 12:00 AM - Oct 7, 2020 12:43 PM

ezjacket*

Statistics

Sessions Timeline

Blade
- Threat Emulation 98.1%
- URL Filtering 1.9%

Type
- Log 99.83%
- Session 0.17%

Action
- Accept 98.27%
- Detect 1.73%

Severity
- Informational 100.0%

Confidence Level
- N/A 100.0%

Protection Type
- SMTP Emulation 100.0%

File Name
- remittance.pdf 100.0%

File Name
- remittance.pdf 100.0%

File MD5
- 009db847d919855eda... 0.18%
- 00fc2039c24dc246df35... 0.18%
- 01a20e84236e76e99f4f... 0.18%

Time	B.	T..	A.	Severity	Confidence Le...	Protection T...	File Name	File Size (Byt...	File MD5	File T...	Email Sender	Email Recipient
Oct 7, 2020 11:13:48 AM				Inf...	N/A							
Oct 7, 2020 6:16:19 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	131.0KB	2ed9fcf6af0a8b946952b368ada13d9a	pdf	ezjacketezremit@oldrepublictitle.com	tsorensen1@oldrepublictitle.com & 3 more
Oct 7, 2020 5:21:07 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	8.5KB	1a07f78b3025bde29ec2e36d43fc3614	pdf	ezjacketezremit@oldrepublictitle.com	kmarshall@oldrepublictitle.com
Oct 7, 2020 5:13:46 AM				Inf...	N/A							
Oct 7, 2020 4:17:03 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	7.0KB	1767d7fc9414c3e76fb53d6b5dac1075	pdf	ezjacketezremit@oldrepublictitle.com	dsessums@mvt.com, bwoods@mvt.com
Oct 7, 2020 3:00:11 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	82.0KB	8698b775961c5e12e59124043d6802c7	pdf	ezjacketezremit@oldrepublictitle.com	rglass@oldrepublictitle.com
Oct 7, 2020 2:50:46 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	14.7KB	50869ee9aa89e7db5863e82d3f0b1520	pdf	ezjacketezremit@oldrepublictitle.com	mlaney@oldrepublictitle.com
Oct 7, 2020 2:32:43 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	12.7KB	76e182a51036564cc2bcf8e7842aa916	pdf	ezjacketezremit@oldrepublictitle.com	mlaney@oldrepublictitle.com
Oct 7, 2020 2:30:58 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	3.1KB	22464620b0f4a15dc29f7d961d5d7589	pdf	ezjacketezremit@oldrepublictitle.com	ylemus@oldrepublictitle.com & 2 more
Oct 7, 2020 2:23:45 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	135.7KB	356ab0471f0b37ca77634bde3709d91e	pdf	ezjacketezremit@oldrepublictitle.com	tsorensen1@oldrepublictitle.com & 3 more
Oct 7, 2020 2:11:22 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	10.7KB	21044a5bdb7379f82c13621ba72f1917	pdf	ezjacketezremit@oldrepublictitle.com	mtimmons@oldrepublictitle.com
Oct 7, 2020 2:04:37 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	28.7KB	f098ae29e2f8deac736d9dc8e2cce7fe	pdf	ezjacketezremit@oldrepublictitle.com	ylemus@oldrepublictitle.com & 2 more
Oct 7, 2020 1:44:09 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	20.2KB	a8838a874b65147914ed38b20b2175b3	pdf	ezjacketezremit@oldrepublictitle.com	whill@oldrepublictitle.com & 2 more
Oct 7, 2020 1:43:25 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	21.5KB	db0ee17a8adff584494d5ec574ab71f6	pdf	ezjacketezremit@oldrepublictitle.com	whill@oldrepublictitle.com & 2 more
Oct 7, 2020 1:35:08 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	23.4KB	6c5fcd1f96113c82d78b2a209ffd28de	pdf	ezjacketezremit@oldrepublictitle.com	mtimmons@oldrepublictitle.com
Oct 7, 2020 1:26:38 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	39.9KB	ecca4778b95ec8627e8de26fa84c0cff	pdf	ezjacketezremit@oldrepublictitle.com	mtimmons@oldrepublictitle.com
Oct 7, 2020 1:10:22 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	4.1KB	6a9a3c7d698c79e030746ceae273d6a5	pdf	ezjacketezremit@oldrepublictitle.com	mtimmons@oldrepublictitle.com
Oct 7, 2020 12:45:58 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	21.1KB	a4c0b61d8f57e1b2f9729d9f776256de	pdf	ezjacketezremit@oldrepublictitle.com	llewis@oldrepublictitle.com & 4 more
Oct 7, 2020 12:45:35 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	4.4KB	118186ee8bf554a454a7addff5c31ead	pdf	ezjacketezremit@oldrepublictitle.com	sruiz2@oldrepublictitle.com, rwiggin@oldre
Oct 7, 2020 12:40:02 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	15.1KB	25478229cd367667e336d2bd0cd35d20	pdf	ezjacketezremit@oldrepublictitle.com	sruiz2@oldrepublictitle.com & 2 more
Oct 7, 2020 12:29:00 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	12.5KB	30603d9ef9b586f3ae4642e3b97491da	pdf	ezjacketezremit@oldrepublictitle.com	sruiz2@oldrepublictitle.com & 2 more
Oct 7, 2020 12:19:37 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	11.4KB	51336c210c235a6b15312a2de402730c	pdf	ezjacketezremit@oldrepublictitle.com	sruiz2@oldrepublictitle.com & 2 more
Oct 7, 2020 12:18:12 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	91.7KB	47f622c7cf1b53cdce5d24e2e3a5370c	pdf	ezjacketezremit@oldrepublictitle.com	llewis@oldrepublictitle.com & 4 more
Oct 7, 2020 12:13:31 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	3.5KB	aed173d83e3bd54f3267e6f36c6397b7	pdf	ezjacketezremit@oldrepublictitle.com	sfritz@oldrepublictitle.com, cfranco@oldre
Oct 7, 2020 12:12:13 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	8.1KB	89fd503ce4220d8733ca2c2b12697aaa	pdf	ezjacketezremit@oldrepublictitle.com	llewis@oldrepublictitle.com & 2 more
Oct 7, 2020 12:10:20 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	6.0KB	0c9228ca15a097498a3fd7da3d6ec1e3	pdf	ezjacketezremit@oldrepublictitle.com	kmarshall@oldrepublictitle.com
Oct 7, 2020 12:09:32 AM				Inf...	N/A	SMTP Emul...	remittance.pdf	7.2KB	0f5152fd629c8601e5f9c02a3195c9a2	pdf	ezjacketezremit@oldrepublictitle.com	kmarshall@oldrepublictitle.com
Oct 6, 2020 11:55:38 PM				Inf...	N/A	SMTP Emul...	remittance.pdf	9.2KB	14d4c0cf6173db80aab3348923ab5f4e	pdf	ezjacketezremit@oldrepublictitle.com	mtimmons@oldrepublictitle.com
Oct 6, 2020 11:53:17 PM				Inf...	N/A	SMTP Emul...	remittance.pdf	4.1KB	fb02206ebab32ffc9448a739fd436f09	pdf	ezjacketezremit@oldrepublictitle.com	kmarshall@oldrepublictitle.com
Oct 6, 2020 11:52:19 PM				Inf...	N/A	SMTP Emul...	remittance.pdf	2.8KB	d0b1fc318e84a2e1409d5d598eae44cb	pdf	ezjacketezremit@oldrepublictitle.com	kmarshall@oldrepublictitle.com

Check Point
SOFTWARE TECHNOLOGIES

Hospital In Israel

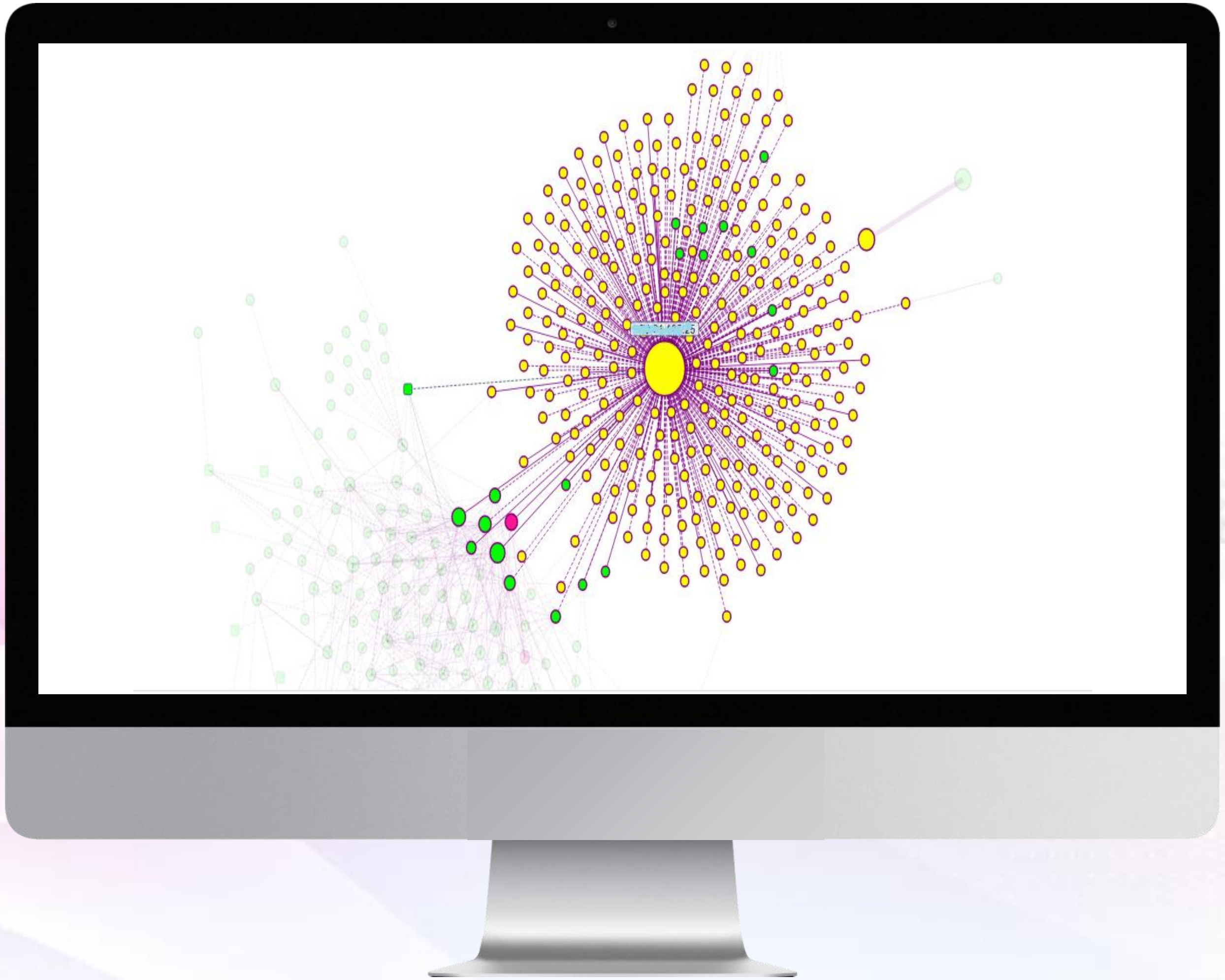
Unsolicited Network Scan

01 **Behavioral Alert**
Regular host (not server) connecting to all machines in the segment

02 **Many ports, many destinations – all internal**
Many detections from IPs

03 **Source immediately identified in the alert**
Employee running ncat inside the company

04 **The scanning was stopped**
No other detection



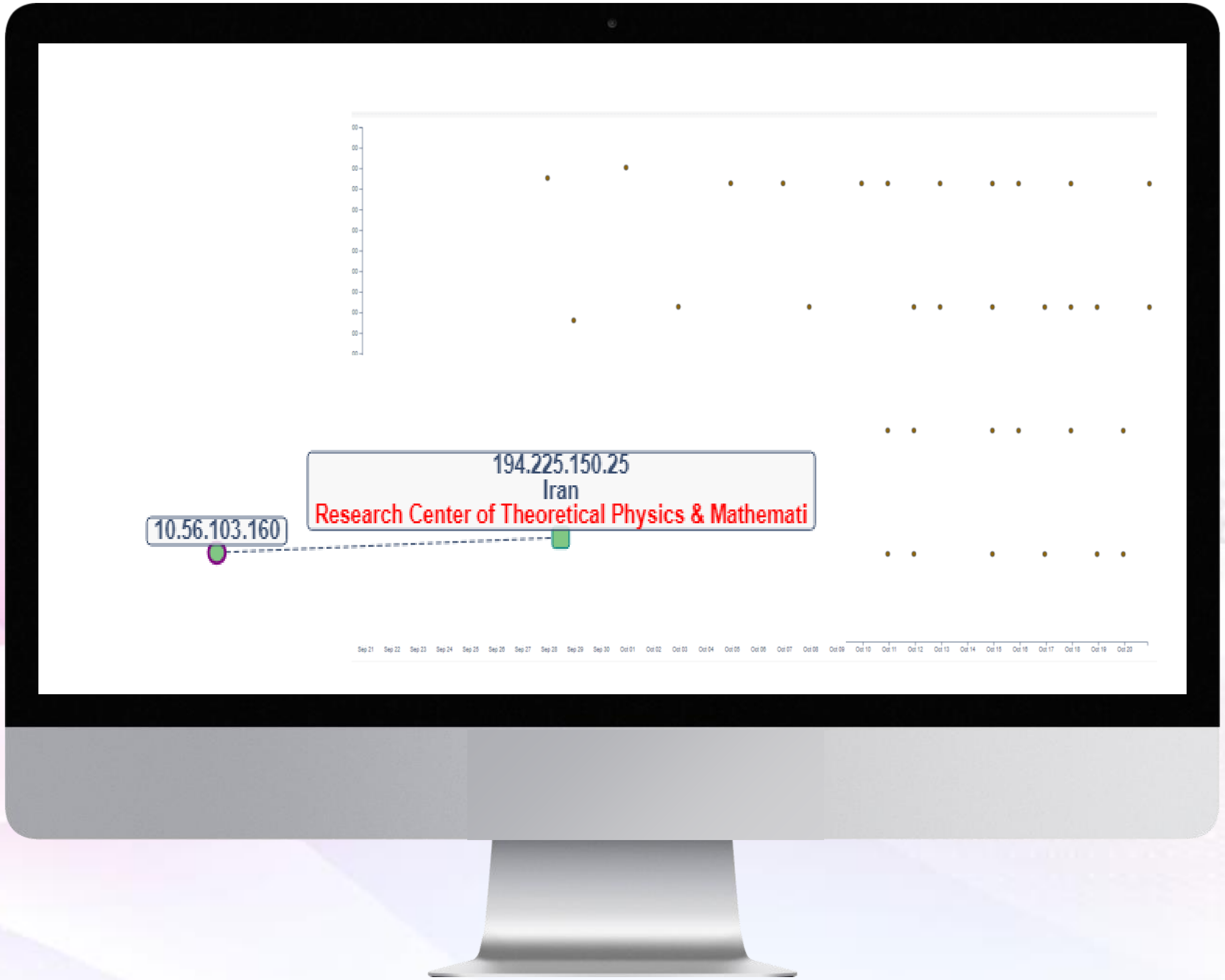
State in US – Iranian Bot

01 **Recurrent Connections Alert**
Recurrent connections from one host to an unclassified IP

02 **Reputation server's verdict is "Unclassified"**
Owned by Iran Research Center of Theoretical Physics and Mathematics

03 **Indicator Created**
For the IP, and added to the feed

04 **No other detections regarding this IP**
Indicator is unique



Trucks Company in Europe

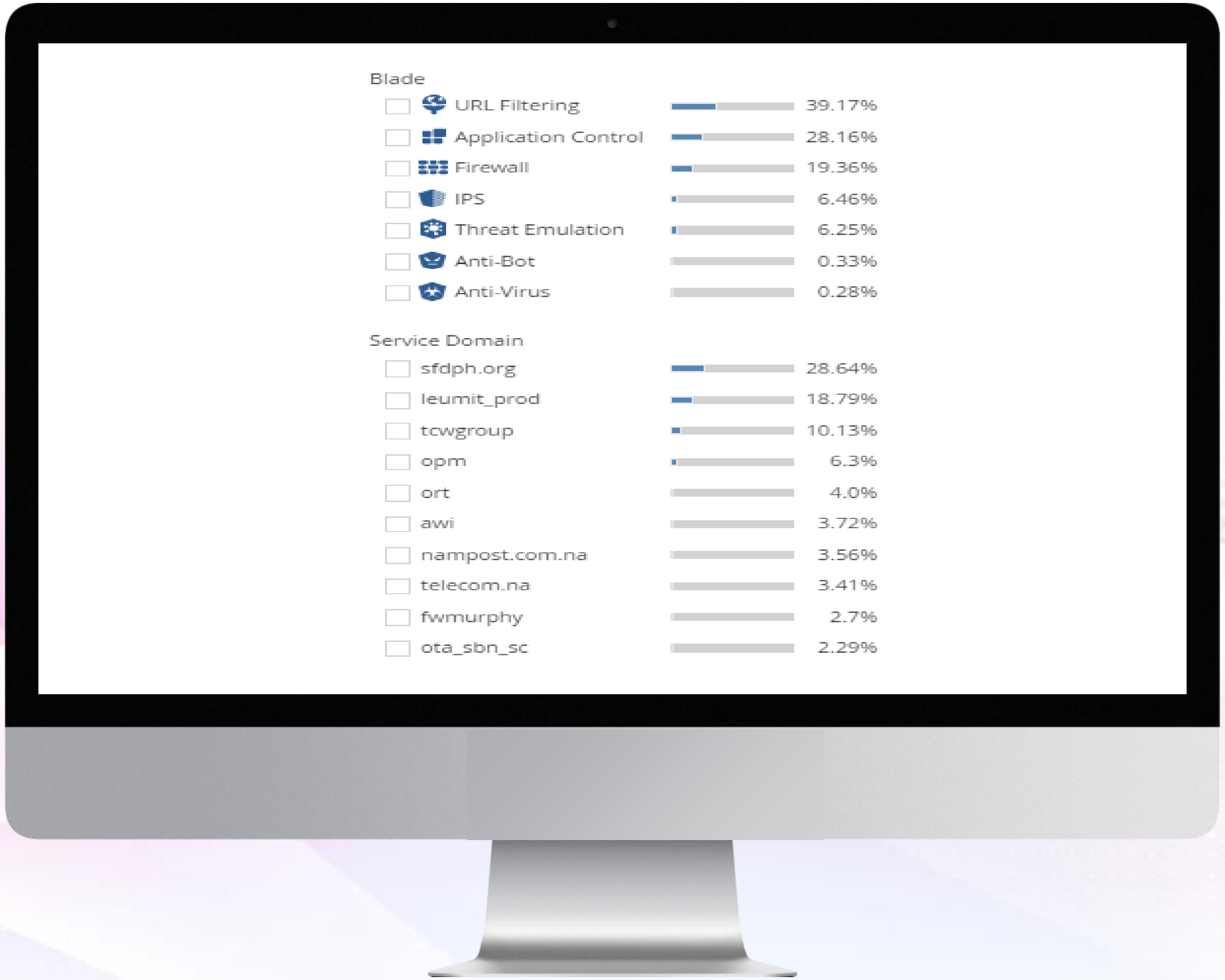
Malvertising

01 **Behavioral Alert**
Abnormal connection to IP located in Kazkhtan

02 **Reputation server’s verdict is “Unclassified”**
Owned by a Kazkhtan host called Kaznic

03 **Same IP being called also by other organizations**
With occasional detections, always from re-directions

04 **Browsing to the resources results on advertising**
Indicator is added to the feed so the firewall can consume it



Blade	
□ URL Filtering	39.17%
□ Application Control	28.16%
□ Firewall	19.36%
□ IPS	6.46%
□ Threat Emulation	6.25%
□ Anti-Bot	0.33%
□ Anti-Virus	0.28%

Service Domain	
□ sfdph.org	28.64%
□ leumit_prod	18.79%
□ tcwgroup	10.13%
□ opm	6.3%
□ ort	4.0%
□ awi	3.72%
□ nampost.com.na	3.56%
□ telecom.na	3.41%
□ fwmurphy	2.7%
□ ota_sbn_sc	2.29%

Check Point®
SOFTWARE TECHNOLOGIES LTD

THANK YOU