A Roadmap to Resilience: WatchGuard's 2024 Strategy

Alper Onarangil

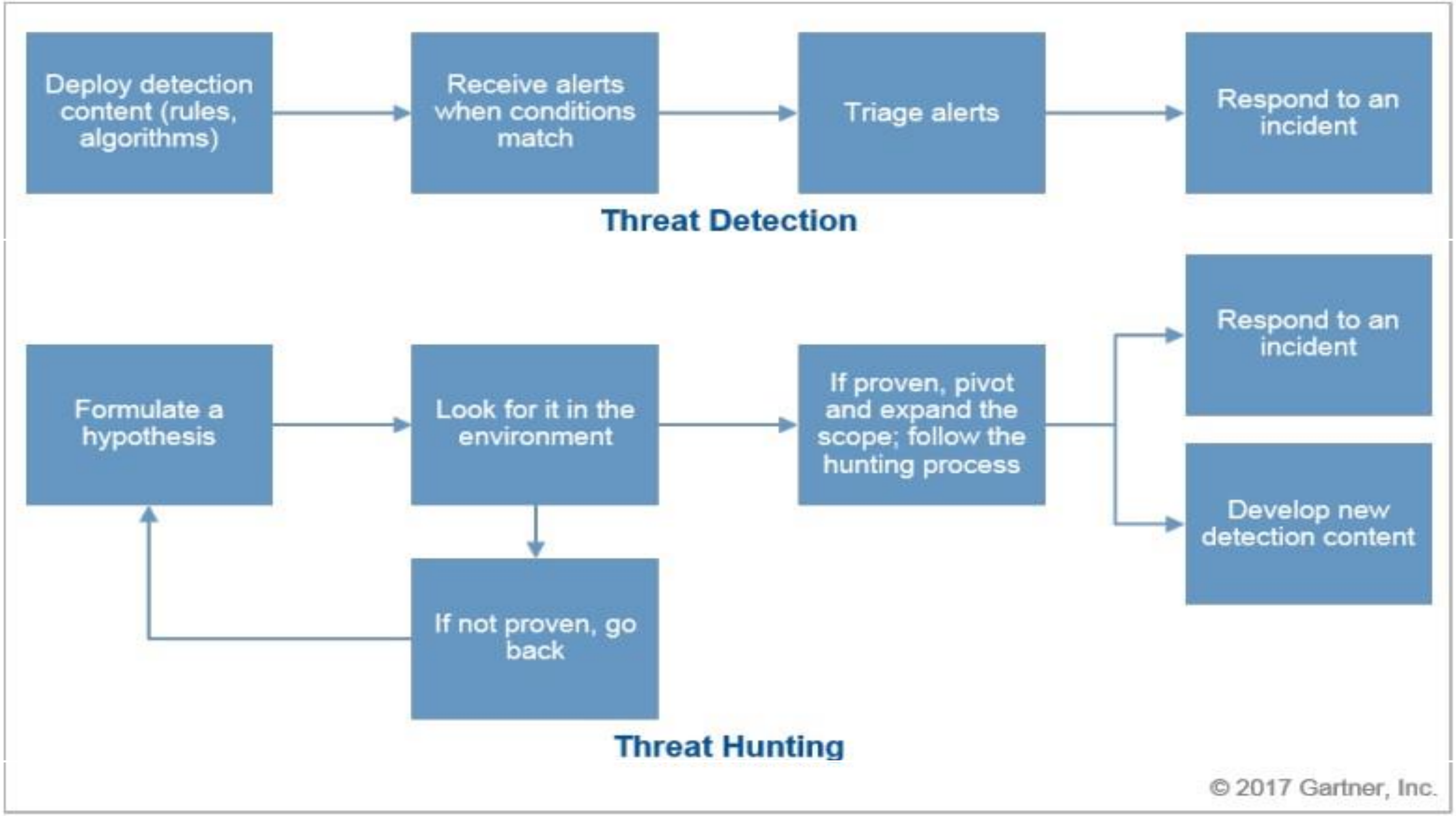
Sales Engineer

Agenda

- MDR Behind the scene
- 2024 Vision and Roadmap
  - Fireware Roadmap
  - FireCloud
  - NDR – Network Detection And Response

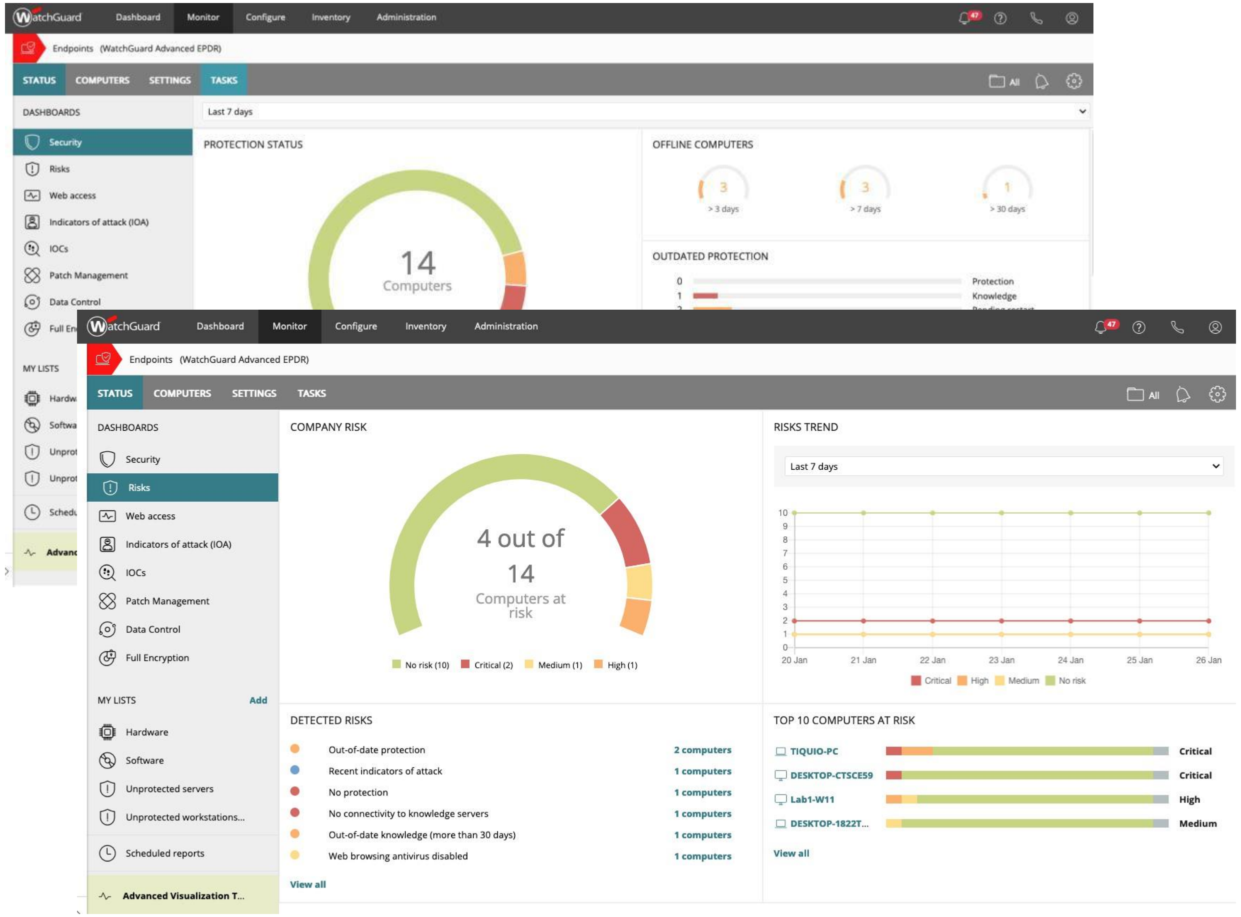
MDR – Behind the scene

Threat Detection vs Threat Hunting



Deploy detection content (rules, algorithms)
Receive alerts when conditions match
Triage alerts
Respond to an incident
Threat Detection
Formulate a hypothesis
Look for it in the environment
If proven, pivot and expand the scope; follow the hunting process
Respond to an incident
Develop new detection content
If not proven, go back
Threat Hunting
© 2017 Gartner, Inc.

Threat Detection vs Threat Hunting



Endpoints (WatchGuard Advanced EPDR)

DASHBOARDS

- Security
- Risks
- Web access
- Indicators of attack (IOA)
- IOCs
- Patch Management
- Data Control
- Full Encryption

MY LISTS Add

- Hardware
- Software
- Unprotected servers
- Unprotected workstations...
- Scheduled reports

Advanced Visualization T...

COMPANY RISK

4 out of 14 Computers at risk

RISKS TREND

Last 7 days

DETECTED RISKS

●	Out-of-date protection	2 computers
●	Recent indicators of attack	1 computers
●	No protection	1 computers
●	No connectivity to knowledge servers	1 computers
●	Out-of-date knowledge (more than 30 days)	1 computers
●	Web browsing antivirus disabled	1 computers

View all

TOP 10 COMPUTERS AT RISK

TIQUIO-PC	Critical
DESKTOP-CTSCE59	Critical
Lab1-W11	High
DESKTOP-1822T...	Medium

View all

PROTECTION STATUS

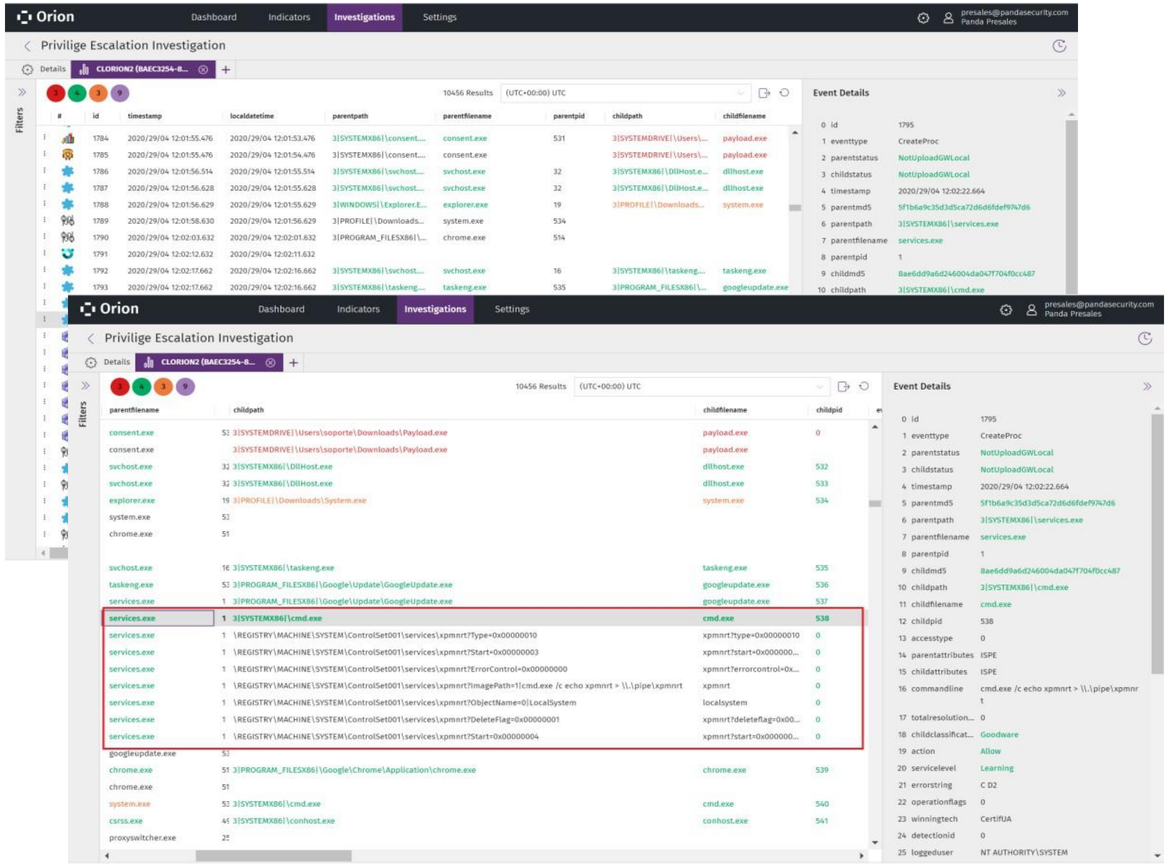
14 Computers

OFFLINE COMPUTERS

3 > 3 days
3 > 7 days
1 > 30 days

OUTDATED PROTECTION

Protection
Knowledge



Privilige Escalation Investigation

Details CLORION2 (BAEC3254-8...

10456 Results (UTC+00:00) UTC

parentfilename		childpath	childfilename	childpid
consent.exe	53	3|SYSTEMDRIVE|\Users\soporte\Downloads\Payload.exe	payload.exe	0
consent.exe		3|SYSTEMDRIVE|\Users\soporte\Downloads\Payload.exe	payload.exe	
svchost.exe	32	3|SYSTEMX86|\DllHost.exe	dllhost.exe	532
svchost.exe	32	3|SYSTEMX86|\DllHost.exe	dllhost.exe	533
explorer.exe	19	3|PROFILE|\Downloads\System.exe	system.exe	534
system.exe	53			
chrome.exe	51			
svchost.exe	16	3|SYSTEMX86|\taskeng.exe	taskeng.exe	535
taskeng.exe	53	3|PROGRAM_FILESX86|\Google\Update\GoogleUpdate.exe	googleupdate.exe	536
services.exe	1	3|PROGRAM_FILESX86|\Google\Update\GoogleUpdate.exe	googleupdate.exe	537
services.exe	1	3|SYSTEMX86|\cmd.exe	cmd.exe	538
services.exe	1	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\xpmnrt?Type=0x00000010	xpmnrt?type=0x00000010	0
services.exe	1	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\xpmnrt?Start=0x00000003	xpmnrt?start=0x000000...	0
services.exe	1	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\xpmnrt?ErrorControl=0x00000000	xpmnrt?errorcontrol=0x...	0
services.exe	1	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\xpmnrt?ImagePath=1|cmd.exe /c echo xpmnrt > \\.\pipe\xpmnrt	xpmnrt	0
services.exe	1	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\xpmnrt?ObjectName=0|LocalSystem	localsystem	0
services.exe	1	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\xpmnrt?DeleteFlag=0x00000001	xpmnrt?deleteflag=0x00...	0
services.exe	1	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\xpmnrt?Start=0x00000004	xpmnrt?start=0x000000...	0
googleupdate.exe	53			
chrome.exe	51	3|PROGRAM_FILESX86|\Google\Chrome\Application\chrome.exe	chrome.exe	539
chrome.exe	51			
system.exe	53	3|SYSTEMX86|\cmd.exe	cmd.exe	540
csrss.exe	49	3|SYSTEMX86|\conhost.exe	conhost.exe	541
proxyswitcher.exe	25			

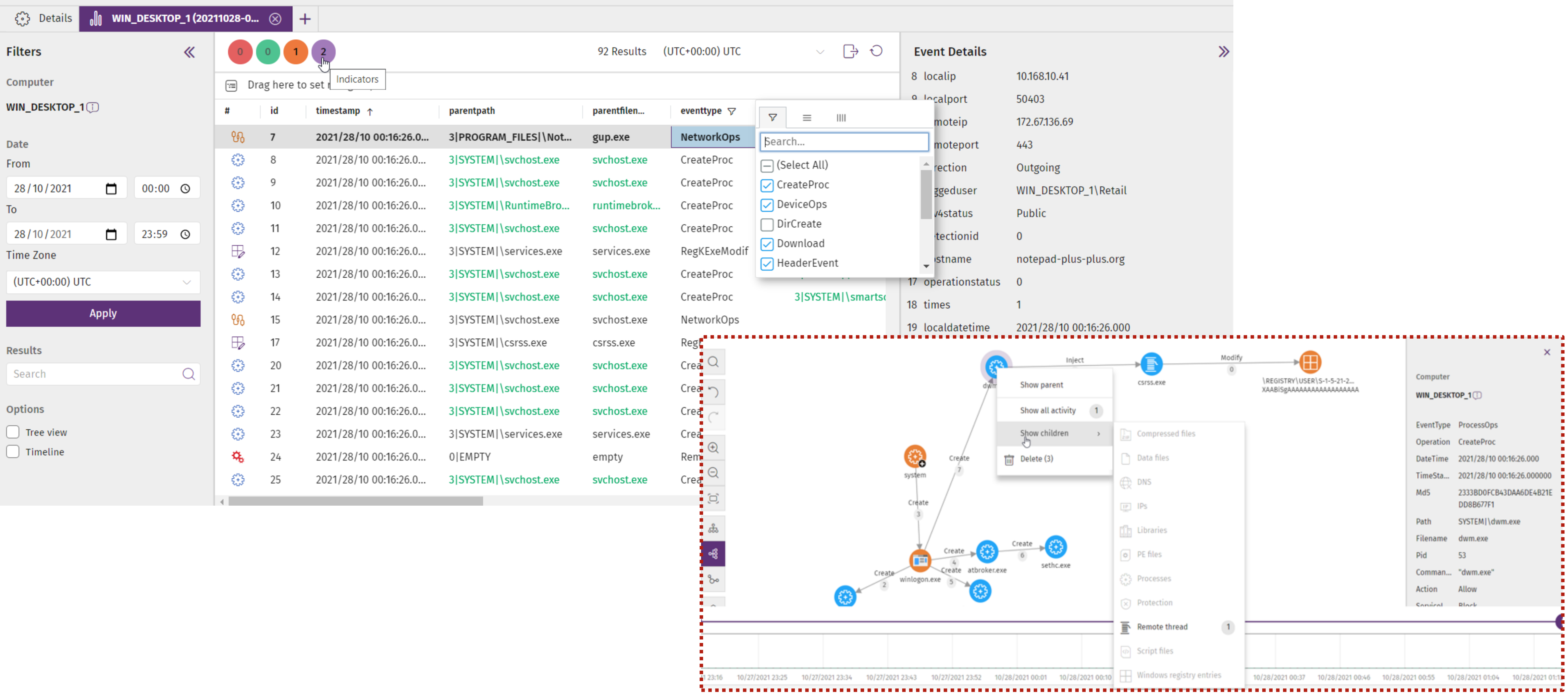
Event Details

0	id	1795
1	eventtype	CreateProc
2	parentstatus	NotUploadGWLocal
3	childstatus	NotUploadGWLocal
4	timestamp	2020/29/04 12:02:22.664
5	parentmd5	5f1b6a9c35d3d5ca72d6d6fdef9747d6
6	parentpath	3|SYSTEMX86|\services.exe
7	parentfilename	services.exe
8	parentpid	1
9	childmd5	8ae6dd9a6d246004da047f704f0cc487
10	childpath	3|SYSTEMX86|\cmd.exe
11	childfilename	cmd.exe
12	childpid	538
13	accesstype	0
14	parentattributes	ISPE
15	childattributes	ISPE
16	commandline	cmd.exe /c echo xpmnrt > \\.\pipe\xpmnrt
17	totalresolution...	0
18	childclassificat...	Goodware
19	action	Allow
20	servicelevel	Learning
21	errorstring	C D2
22	operationflags	0
23	winningtech	CertifUA
24	detectionid	0
25	loggeduser	NT AUTHORITY\SYSTEM

EPDR Console

Orion Console

MDR – Behind the scene



Computer
WIN_DESKTOP_1

Date
From
28 / 10 / 2021 00:00
To
28 / 10 / 2021 23:59
Time Zone
(UTC+00:00) UTC
Apply

Results
Search

Options
☐ Tree view
☐ Timeline

#	id	timestamp ↑	parentpath	parentfilen...	eventtype
	7	2021/28/10 00:16:26.0...	3|PROGRAM_FILES|\Not...	gup.exe	NetworkOps
	8	2021/28/10 00:16:26.0...	3|SYSTEM|\svchost.exe	svchost.exe	CreateProc
	9	2021/28/10 00:16:26.0...	3|SYSTEM|\svchost.exe	svchost.exe	CreateProc
	10	2021/28/10 00:16:26.0...	3|SYSTEM|\RuntimeBro...	runtimebrok...	CreateProc
	11	2021/28/10 00:16:26.0...	3|SYSTEM|\svchost.exe	svchost.exe	CreateProc
	12	2021/28/10 00:16:26.0...	3|SYSTEM|\services.exe	services.exe	RegKExeModif
	13	2021/28/10 00:16:26.0...	3|SYSTEM|\svchost.exe	svchost.exe	CreateProc
	14	2021/28/10 00:16:26.0...	3|SYSTEM|\svchost.exe	svchost.exe	CreateProc 3|SYSTEM|\smartsc
	15	2021/28/10 00:16:26.0...	3|SYSTEM|\svchost.exe	svchost.exe	NetworkOps
	17	2021/28/10 00:16:26.0...	3|SYSTEM|\csrss.exe	csrss.exe	Regl
	20	2021/28/10 00:16:26.0...	3|SYSTEM|\svchost.exe	svchost.exe	Crea
	21	2021/28/10 00:16:26.0...	3|SYSTEM|\svchost.exe	svchost.exe	Crea
	22	2021/28/10 00:16:26.0...	3|SYSTEM|\svchost.exe	svchost.exe	Crea
	23	2021/28/10 00:16:26.0...	3|SYSTEM|\services.exe	services.exe	Crea
	24	2021/28/10 00:16:26.0...	0|EMPTY	empty	Rem
	25	2021/28/10 00:16:26.0...	3|SYSTEM|\svchost.exe	svchost.exe	Crea

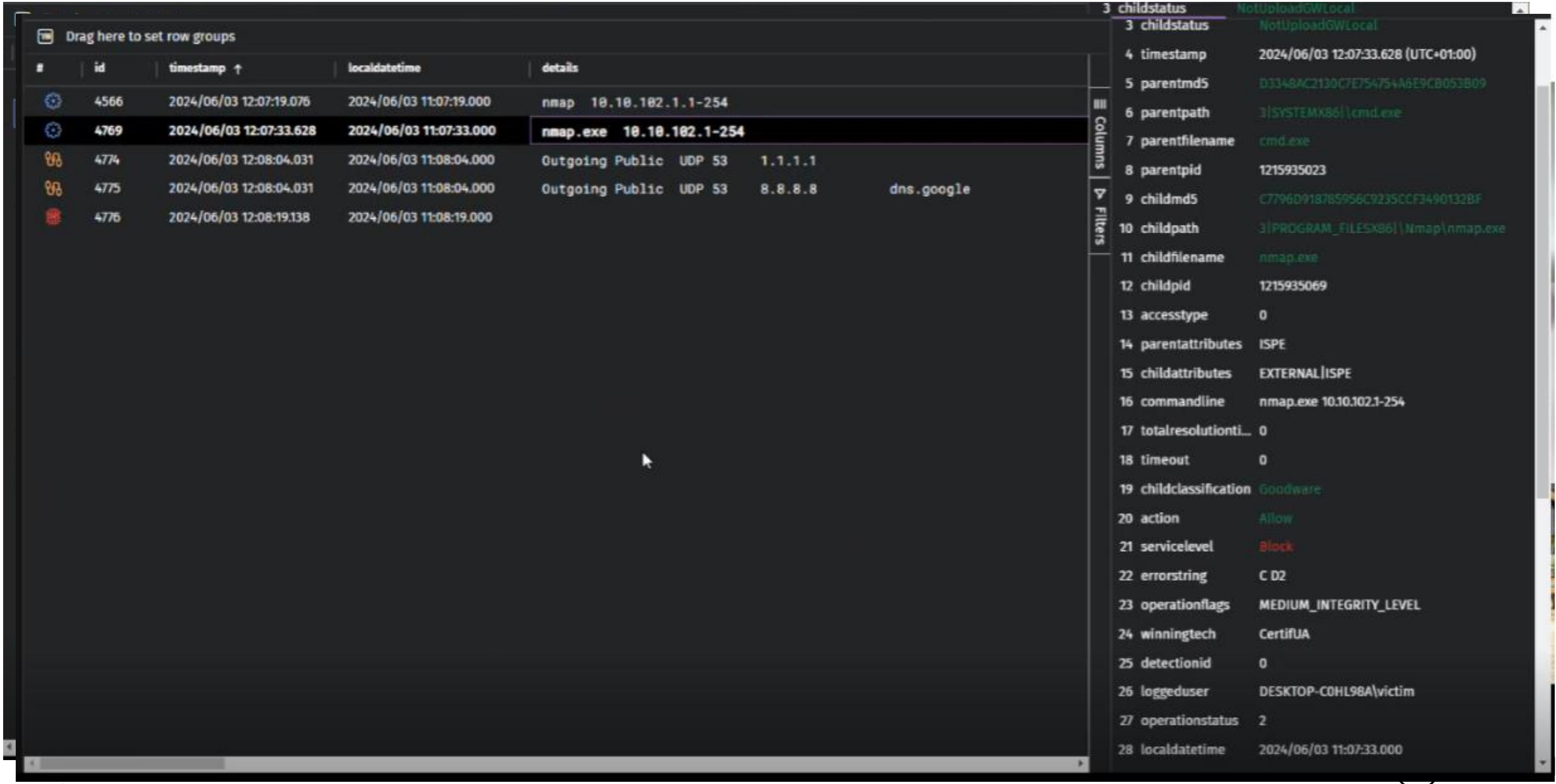
Search...
☐ (Select All)
☑ CreateProc
☑ DeviceOps
☐ DirCreate
☑ Download
☑ HeaderEvent

8	localip	10.168.10.41
9	localport	50403
	moteip	172.67.136.69
	moteport	443
	rection	Outgoing
	ggeduser	WIN_DESKTOP_1\Retail
	v4status	Public
	tectionid	0
	stname	notepad-plus-plus.org
17	operationstatus	0
18	times	1
19	localdatetime	2021/28/10 00:16:26.000

Computer
WIN_DESKTOP_1

EventType	ProcessOps
Operation	CreateProc
DateTime	2021/28/10 00:16:26.000
TimeSta...	2021/28/10 00:16:26.000000
Md5	2333BD0FCB43DAA6DE4B21E DD8B677F1
Path	SYSTEM|\dwm.exe
Filename	dwm.exe
Pid	53
Comman...	"dwm.exe"
Action	Allow
Servicel	Block

MDR – Behind the scene



#	id	timestamp ↑	localdatetime	details
⚙	4566	2024/06/03 12:07:19.076	2024/06/03 11:07:19.000	nmap 10.10.102.1.1-254
⚙	4769	2024/06/03 12:07:33.628	2024/06/03 11:07:33.000	nmap.exe 10.10.102.1-254
	4774	2024/06/03 12:08:04.031	2024/06/03 11:08:04.000	Outgoing Public UDP 53 1.1.1.1
	4775	2024/06/03 12:08:04.031	2024/06/03 11:08:04.000	Outgoing Public UDP 53 8.8.8.8 dns.google
	4776	2024/06/03 12:08:19.138	2024/06/03 11:08:19.000	

3	childstatus	NotUploadGWLocal
3	childstatus	NotUploadGWLocal
4	timestamp	2024/06/03 12:07:33.628 (UTC+01:00)
5	parentmd5	D3348AC2130C7E754754A6E9CB053B09
6	parentpath	3|SYSTEMX86|\cmd.exe
7	parentfilename	cmd.exe
8	parentpid	1215935023
9	childmd5	C7796D918785956C9235CCF3490132BF
10	childpath	3|PROGRAM_FILESX86|\Nmap\nmap.exe
11	childfilename	nmap.exe
12	childpid	1215935069
13	accesstype	0
14	parentattributes	ISPE
15	childattributes	EXTERNAL|ISPE
16	commandline	nmap.exe 10.10.102.1-254
17	totalresolutionti...	0
18	timeout	0
19	childclassification	Goodware
20	action	Allow
21	servicelevel	Block
22	errorstring	C D2
23	operationflags	MEDIUM_INTEGRITY_LEVEL
24	winningtech	CertifUA
25	detectionid	0
26	loggeduser	DESKTOP-C0HL98A\victim
27	operationstatus	2
28	localdatetime	2024/06/03 11:07:33.000

Thank You

WatchGuard
CYBERSECURITY SIMPLIFIED
CLIMATE PLEDGE ARENA
WatchGuard®
CLIMATE PLEDGE ARENA
Official Cybersecurity Partner of the Seattle Kraken
Official Partner of Climate Pledge Arena