



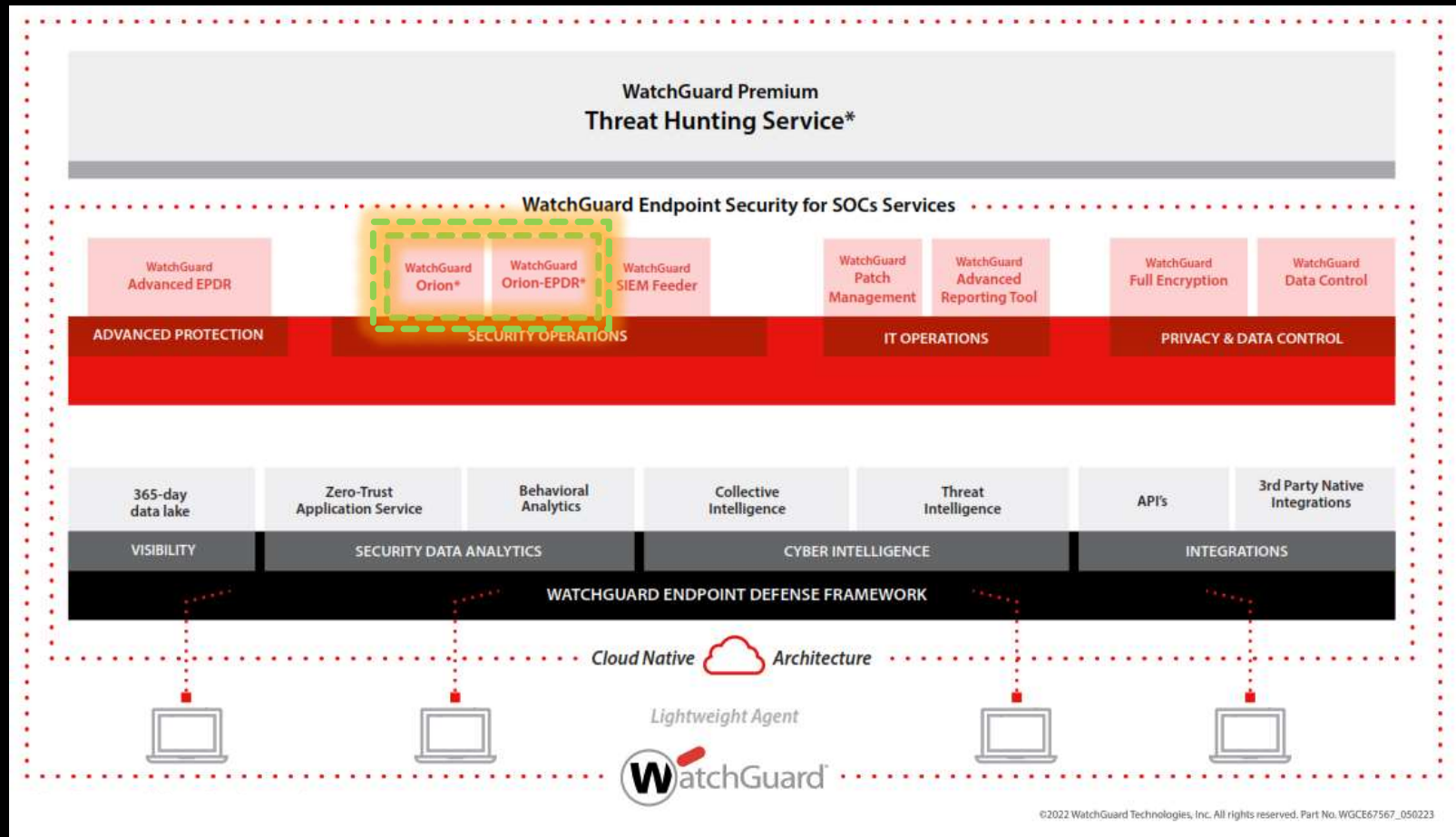
IDEAS >
CREATE
REALITY



WatchGuard[®] | ORION

Security operation Center

WatchGuard Endpoint Solution & Services for SOCs

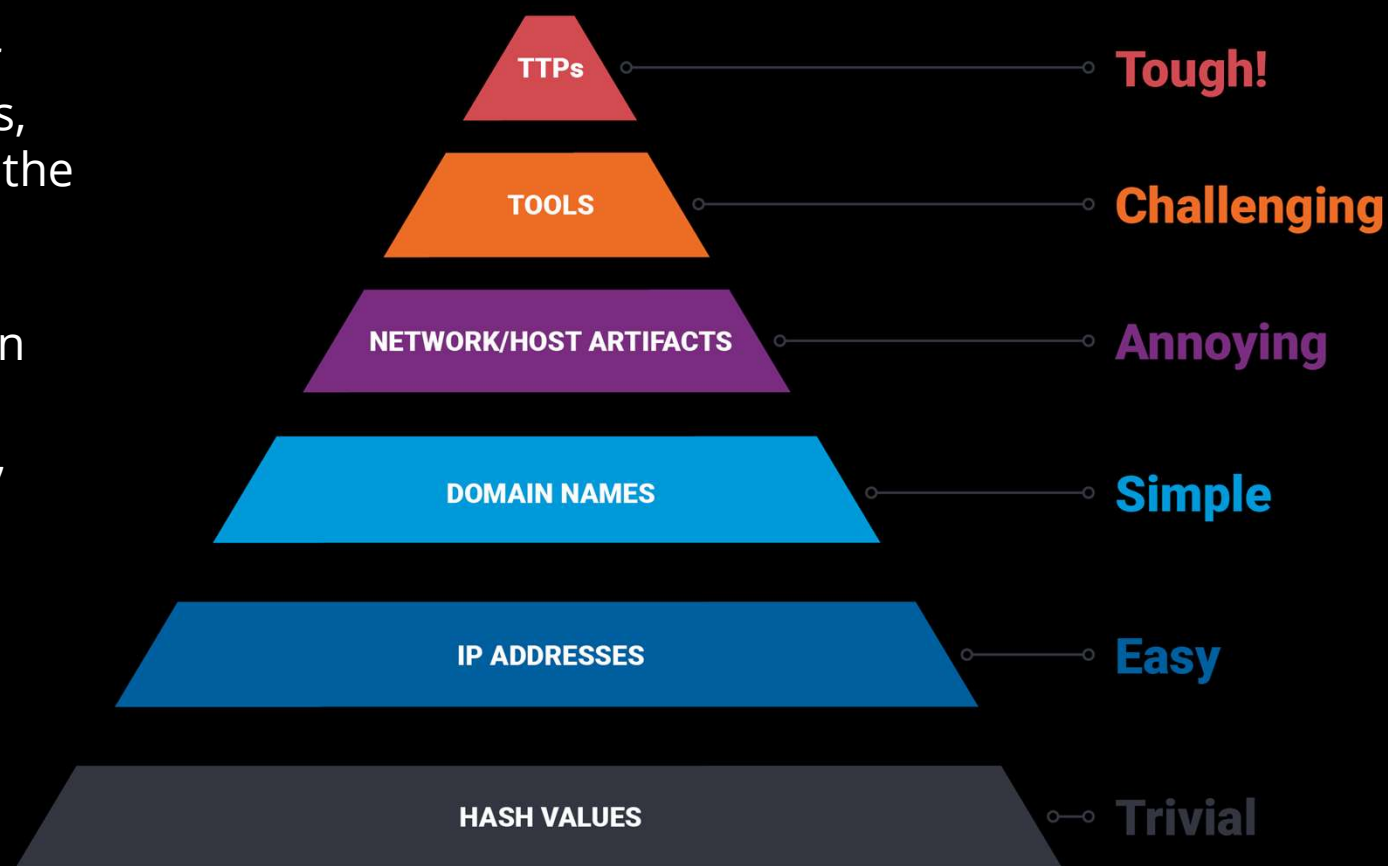


WatchGuard ORION

- multi-tenant cloud **Threat Hunting & Incident Response** platform
- **main goal**: to detect cyberattacks designed to go **undetected by traditional protection systems**: unusual activities, behaviors, suspicious execution patterns that exploit system legitimate tools - known as **Living-off-the-Land (LOTL) or fileless techniques**
- reduces **Dwell Time (MTTD + MTTR) = 11 days** global median (with traditional tools it was more than **200**)
- Real-world events: MTTD can be much longer. For instance, the Microsoft Midnight Blizzard attack in late 2023 had an MTTD of approximately two months

The Pyramid of Pain

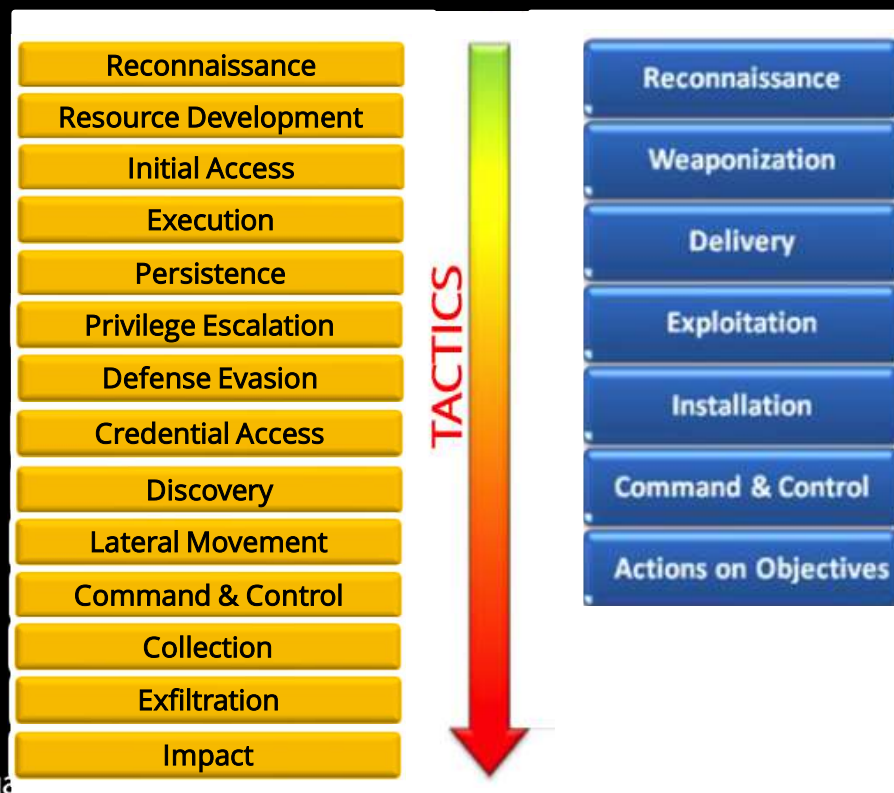
- **WHY** searching for Tactics, Techniques, and Procedures is the best prevention?
- **reduction of 60%** in the frequency and severity of attacks, because the attackers give up



The Cyber Kill Chain and The MITRE ATT&CK

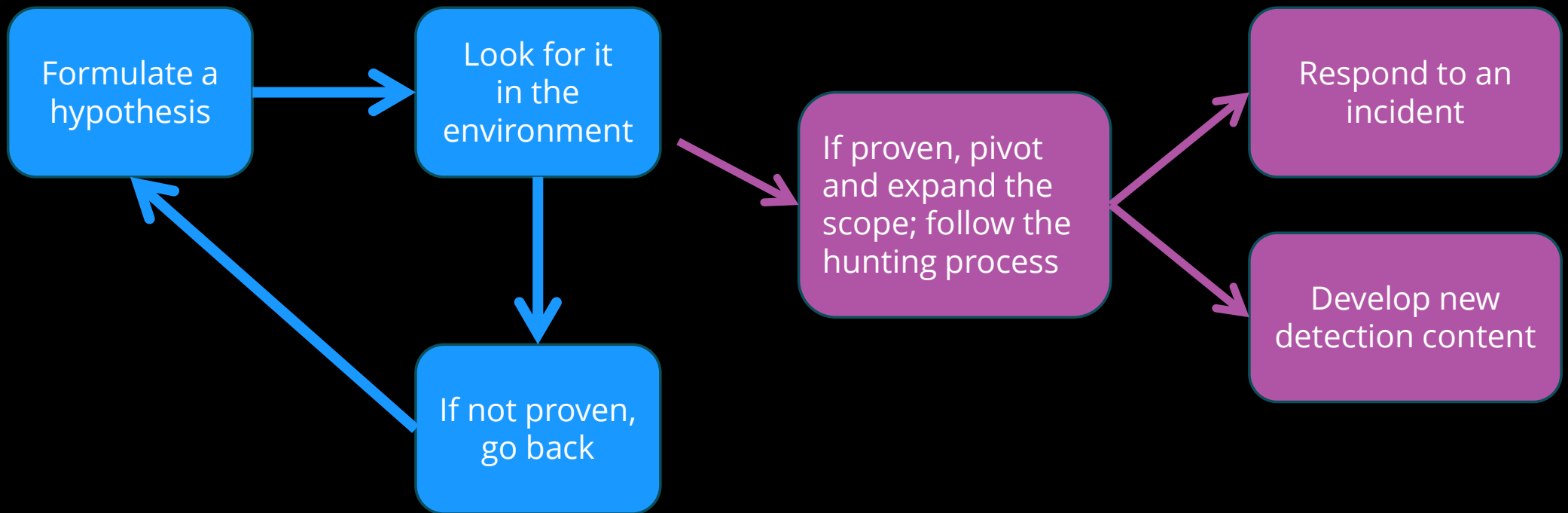
- Models (methodology) for identification and prevention of cyber intrusions activity

The Enterprise ATT&CK matrix



- Orion can stop attacks in any of the phases defined in the CKC and MITRE ATT&CK frameworks
- Most attacks use combination of several tactics and techniques
- Orion downloads the MITRE tactic, technique, and sub-technique knowledge base twice a day
- The key** is the ability to detect and prevent attacks at every phase

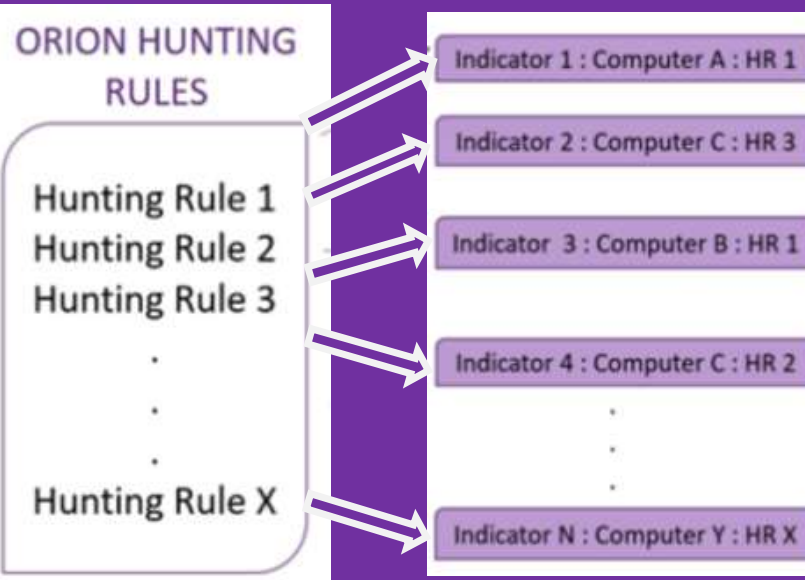
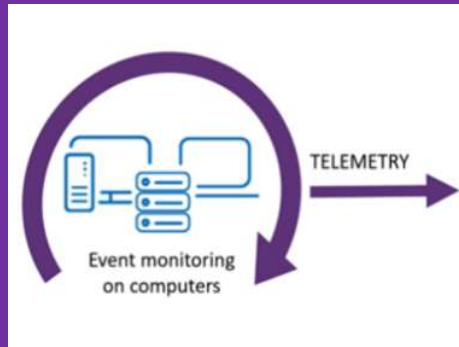
THREAT HUNTING



- Proactive: Investigate from a hypothesis of an attack

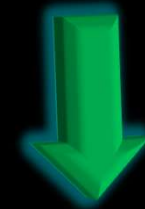
ORION – key points

HUNTING – DETECTION



INVESTIGATIONS

- Jupyter labs
- SQL queries
- Deep Computer investigations
- Graphs



RESPOND

- containment and remediation actions
- robust set of APIs and plugins

- assumption that **the enemy has already entered the system**
- **Focus on discovering Tactics, Techniques, and Procedures (TTPs)**

Deep Investigation in WatchGuard Orion

The investigation console allows in-depth investigation on specific computers and dates. This resource offers all the necessary tools for an analyst to inspect the processes run on a computer in detail

The screenshot displays the WatchGuard Orion investigation console. The top bar shows the selected computer 'WIN_DESKTOP_1 (20211028-0...)' and the number of results '92 Results (UTC+00:00) UTC'. The left sidebar contains filters for Computer, Date, and Time Zone. The main area shows a table of events with columns for #, id, timestamp, parentpath, parentfile, and eventtype. A context menu is open over the 'NetworkOps' event type, showing options like 'CreateProc', 'DeviceOps', 'Download', and 'HeaderEvent'. The right sidebar shows the 'Event Details' for the selected event, including fields like 'localip', 'localport', 'moteip', 'moteport', 'direction', 'loggeduser', '4status', 'tectionid', 'stname', 'operationstatus', 'times', 'localdatetime', 'pandatimestatus', 'details', 'fileName', 'firstSeen', and 'lastSeen'.

#	id	timestamp	parentpath	parentfile	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
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	RegKExeModif
20		2021/28/10 00:16:26.0...	3 SYSTEM svchost.exe	svchost.exe	CreateProc
21		2021/28/10 00:16:26.0...	3 SYSTEM svchost.exe	svchost.exe	CreateProc
22		2021/28/10 00:16:26.0...	3 SYSTEM svchost.exe	svchost.exe	CreateProc
23		2021/28/10 00:16:26.0...	3 SYSTEM services.exe	services.exe	CreateProc
24		2021/28/10 00:16:26.0...	0 EMPTY	empty	RemediationOps
25		2021/28/10 00:16:26.0...	3 SYSTEM svchost.exe	svchost.exe	CreateProc

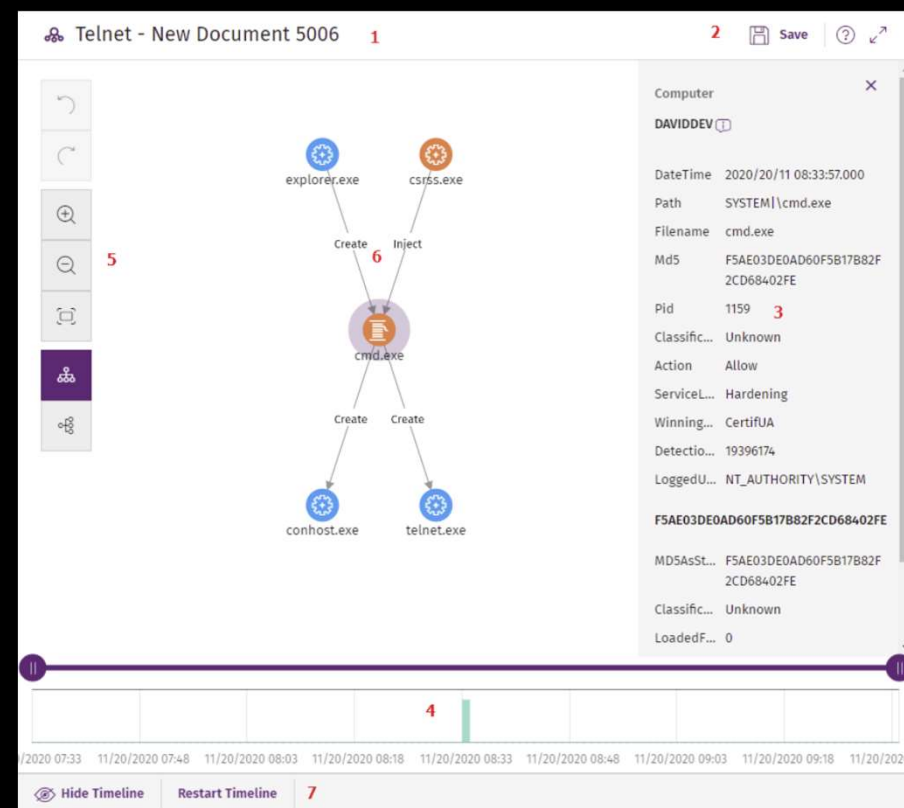
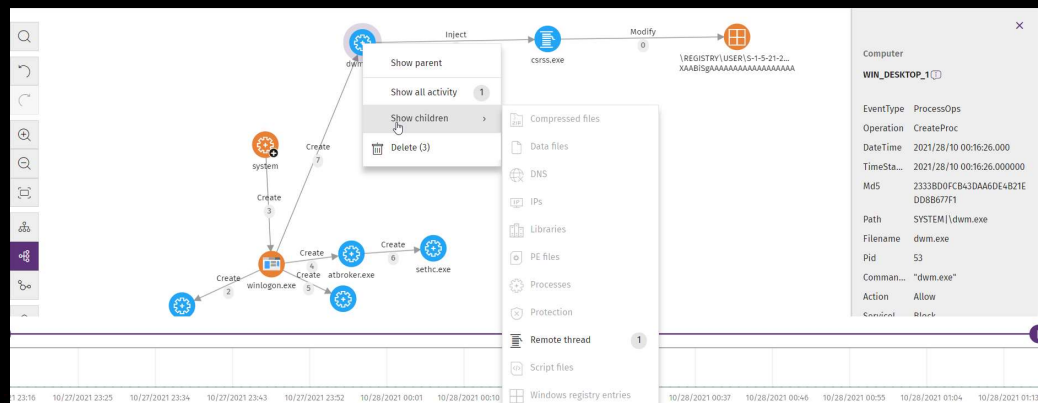
Field	Value
8 localip	10.168.10.41
9 localport	50403
moteip	172.67.136.69
moteport	443
rection	Outgoing
loggeduser	WIN_DESKTOP_1\Retail
4status	Public
tectionid	0
stname	notepad-plus-plus.org
17 operationstatus	0
18 times	1
19 localdatetime	2021/28/10 00:16:26.000
20 pandatimestatus	PandaTimeOk
21 details	Outgoing Public TCP 443 172.67.136.69 notepa d-plus-plus.org
fileName	f4b66db980494e970b50ffa2677a6d5a
firstSeen	2021/09/08 12:36:06
lastSeen	2021/09/08 12:36:06

Investigation Graphs in WatchGuard Orion

The investigation console allows in-depth investigation on specific computers and dates. This resource offers all the necessary tools for an analyst to inspect the processes run on a computer in detail

- Visual context from a suspicious activity
- Entity relationships extracted from the enriched events in the data lake
- Connections across different signals
- Visual access to the telemetry extensible up to 365 days

The information displayed on a graph is equivalent to the one displayed in the investigation console or in advanced queries, but arranged and presented in a clearer, easier-to-interpret way.

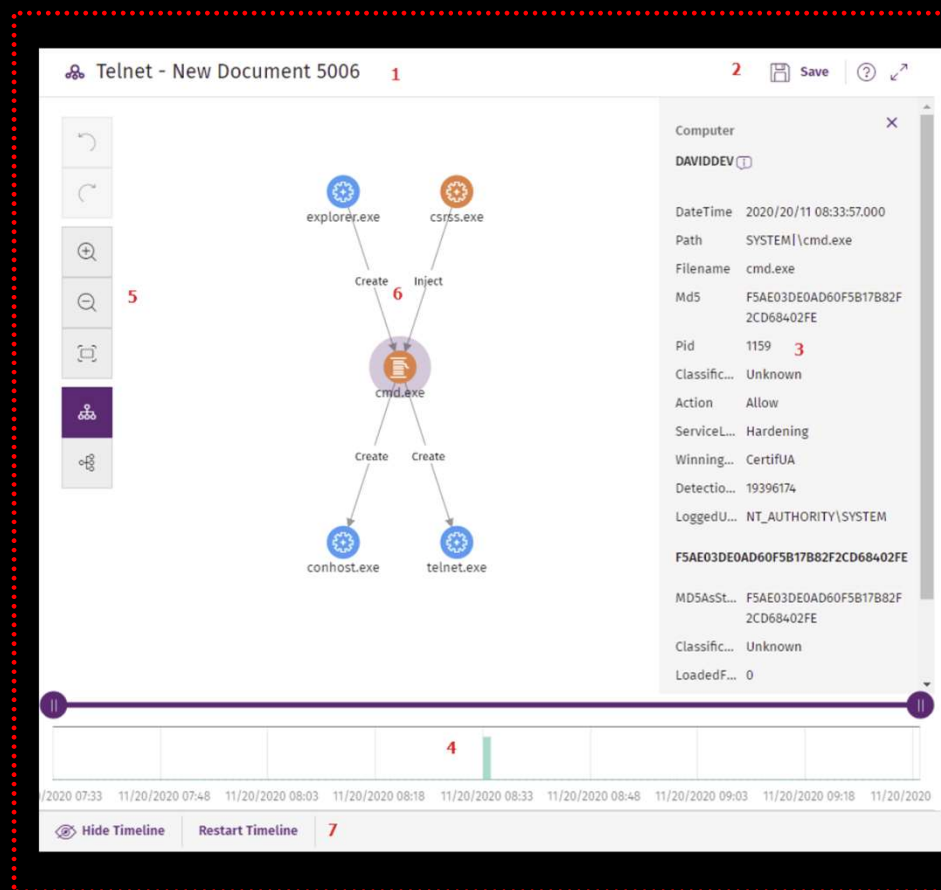
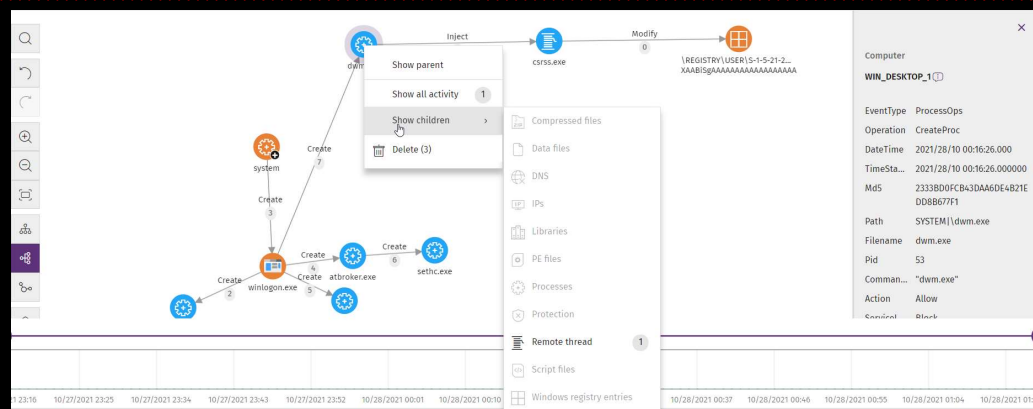


Investigation Graphs in WatchGuard Orion

The investigation graph provides to the analysts:

- Visual context from a suspicious activity
- Entity relationships extracted from the enriched events in the data lake
- Connections across different signals
- Visual access to the telemetry extensible up to 365 days

The information displayed on a graph is equivalent to the one displayed in the investigation console or in advanced queries, but arranged and presented in a clearer, easier-to-interpret way.





LIVE DEMO