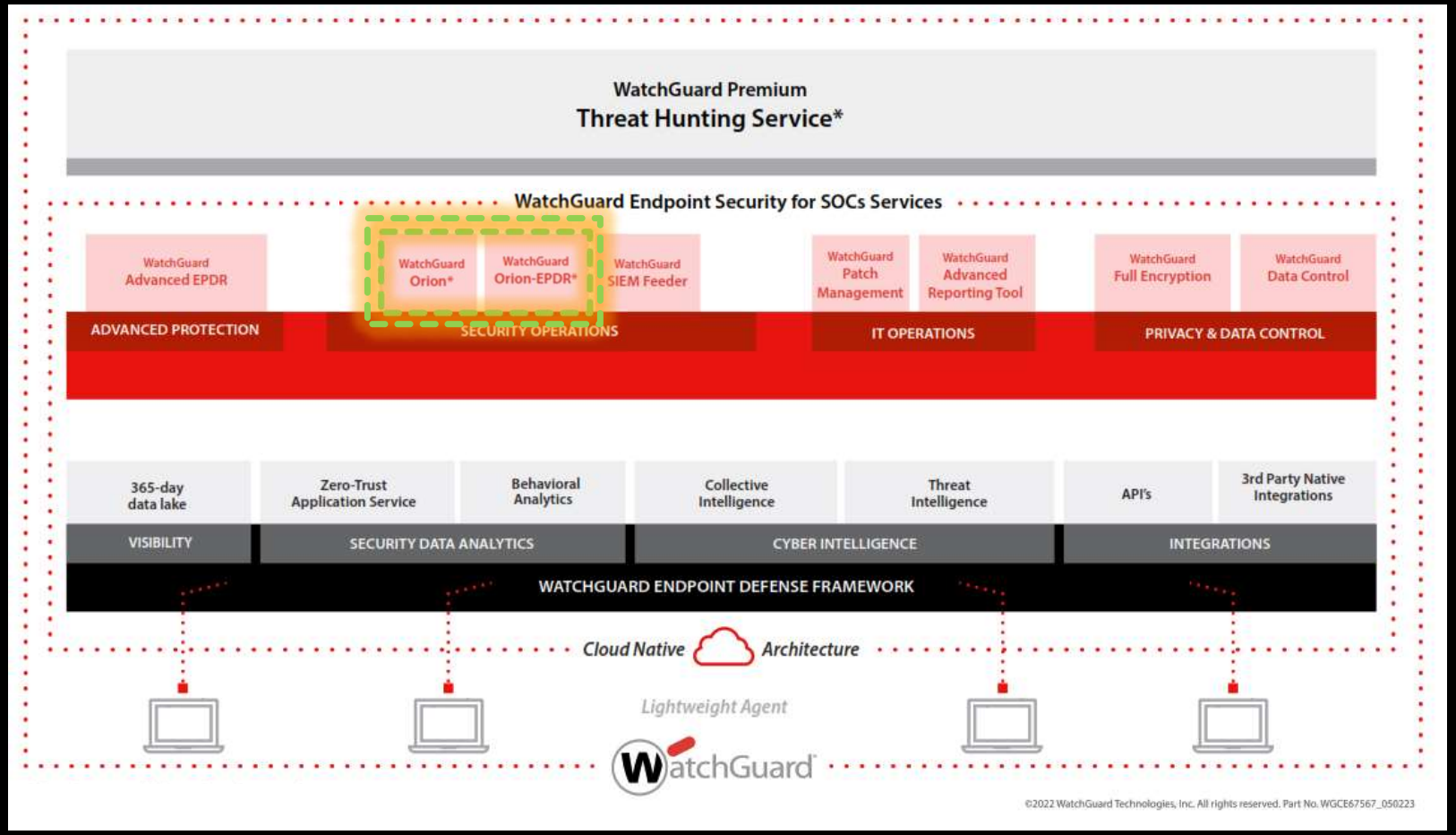
IDEAS > CREATE REALITY

WatchGuard | ORION
Security operation Center

WatchGuard

WatchGuard Endpoint Solution & Services for SOCs



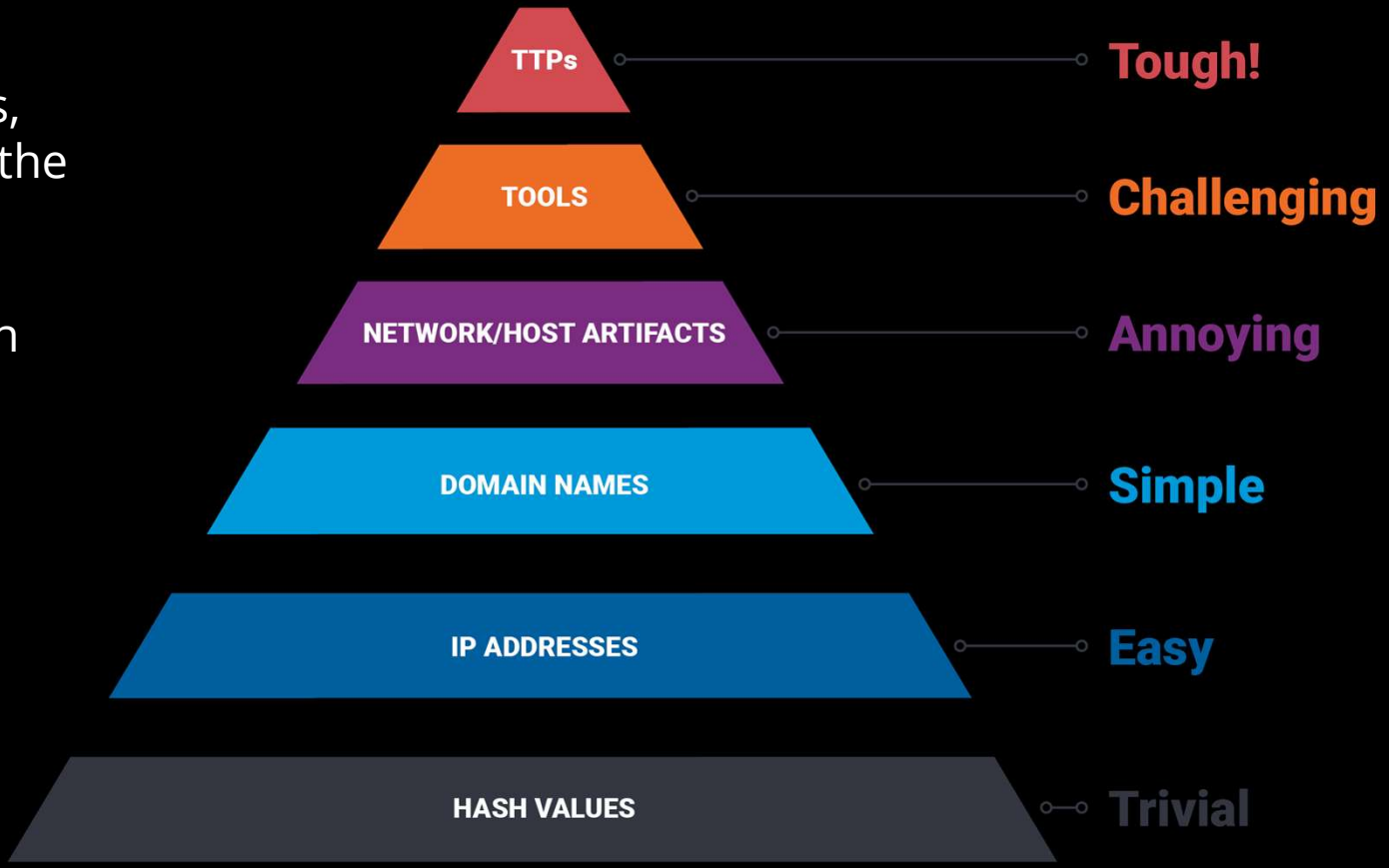
WatchGuard

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

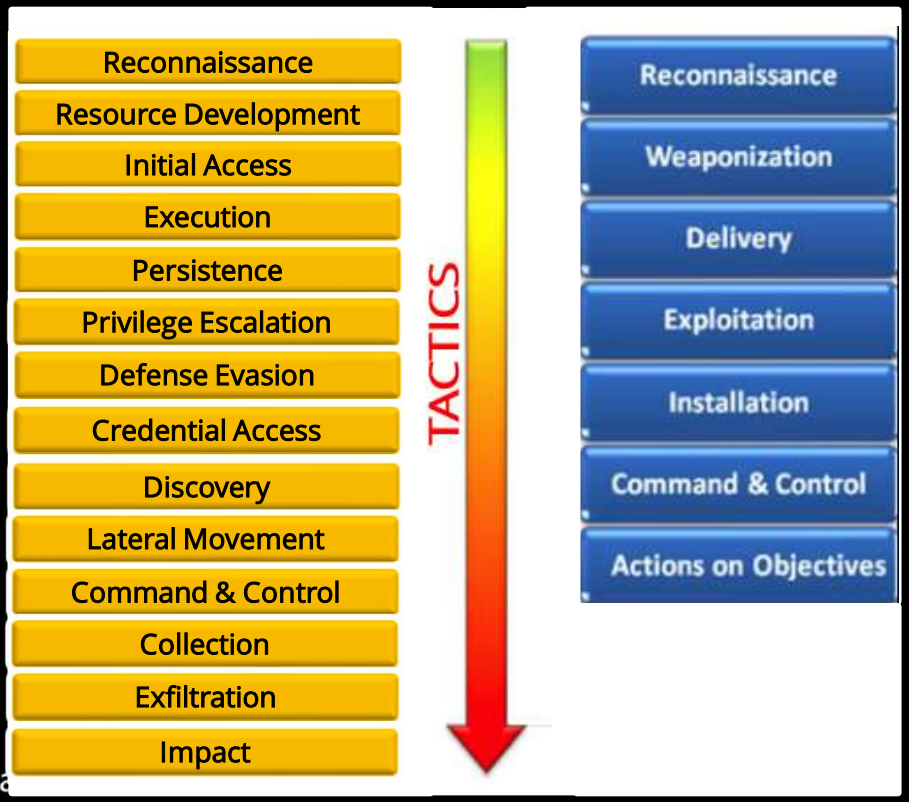


The Cyber Kill Chain and The MITRE ATT&CK

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

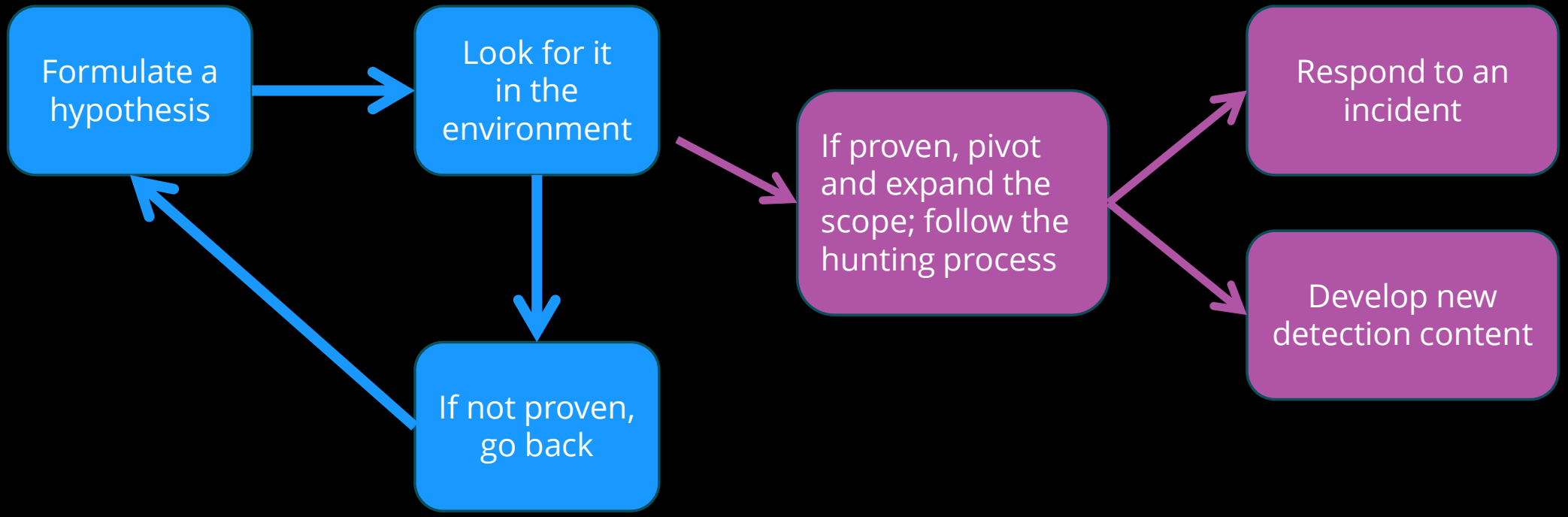
The Enterprise ATT&CK matrix

The CKC



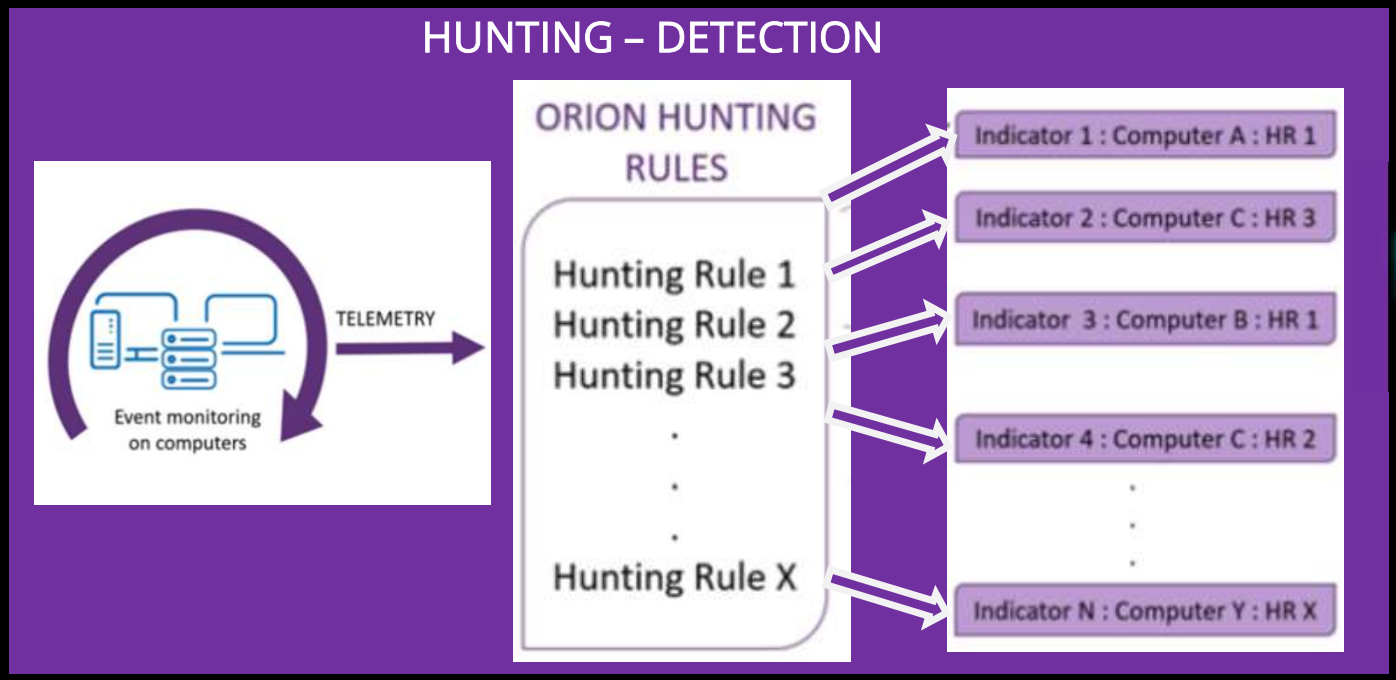
- Orion can stop attacks in any of the phases defined in the CKC and MITRE ATT&CK frameworks
- Most attacks use combination of several tactics and techniques
- Orion downloads the MITRE tactic, technique, and sub-technique knowledge base twice a day
- The key is the ability to detect and prevent attacks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

THREAT HUNTING



- Proactive: Investigate from a hypothesis of an attack

ORION – key points



INVESTIGATIONS

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

RESPOND

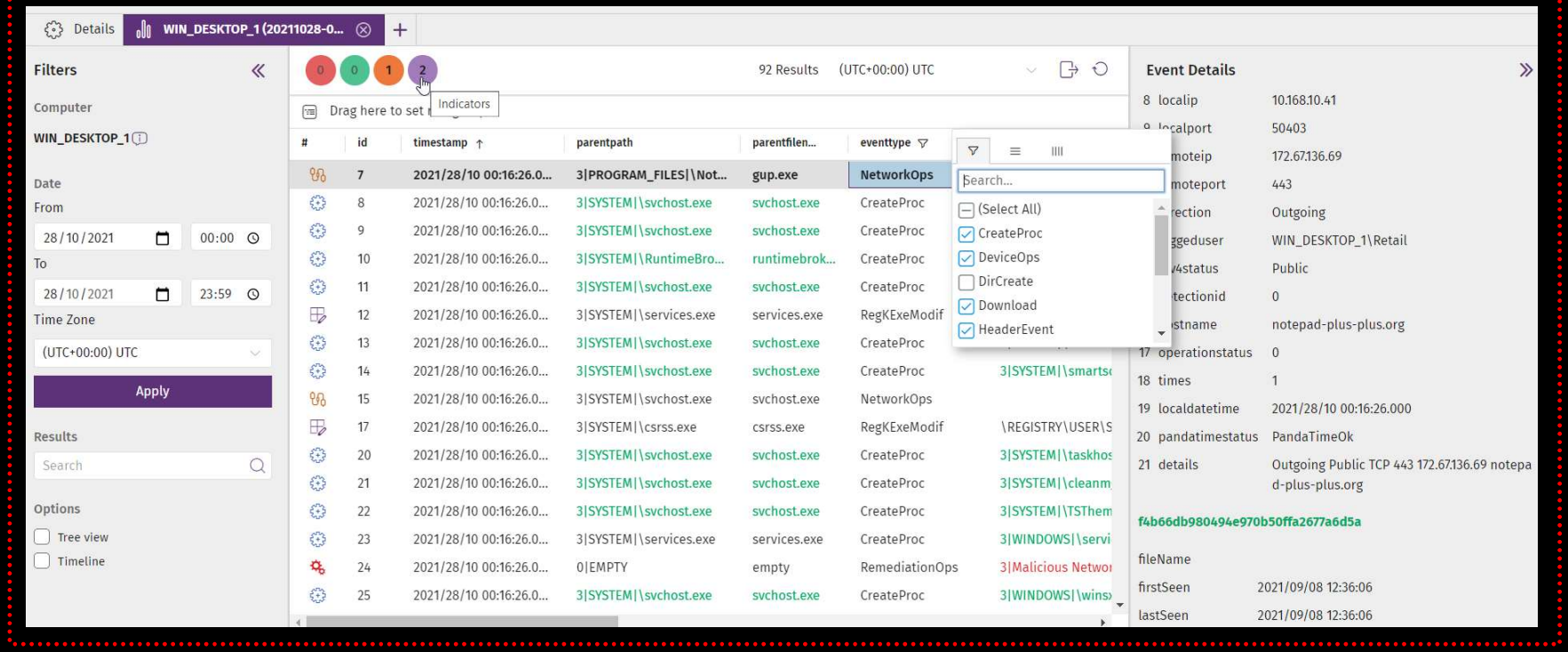
- containment and remediation actions
- robust set of APIs and plugins

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

WatchGuard

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

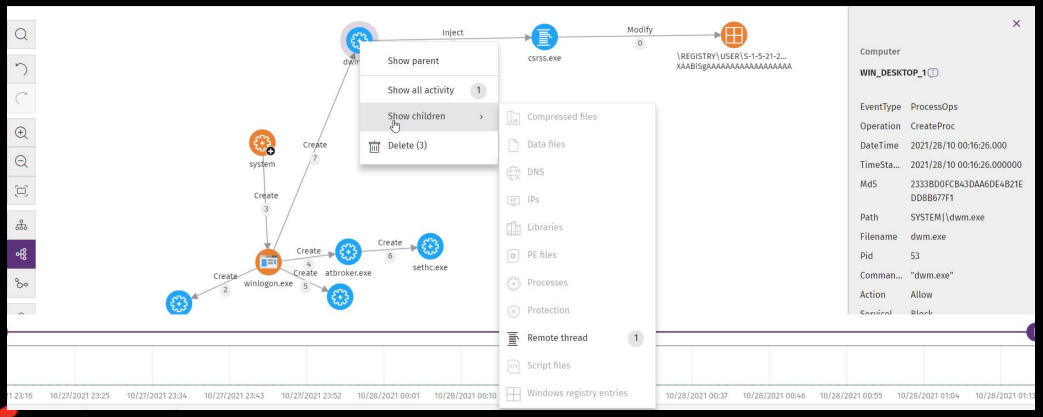


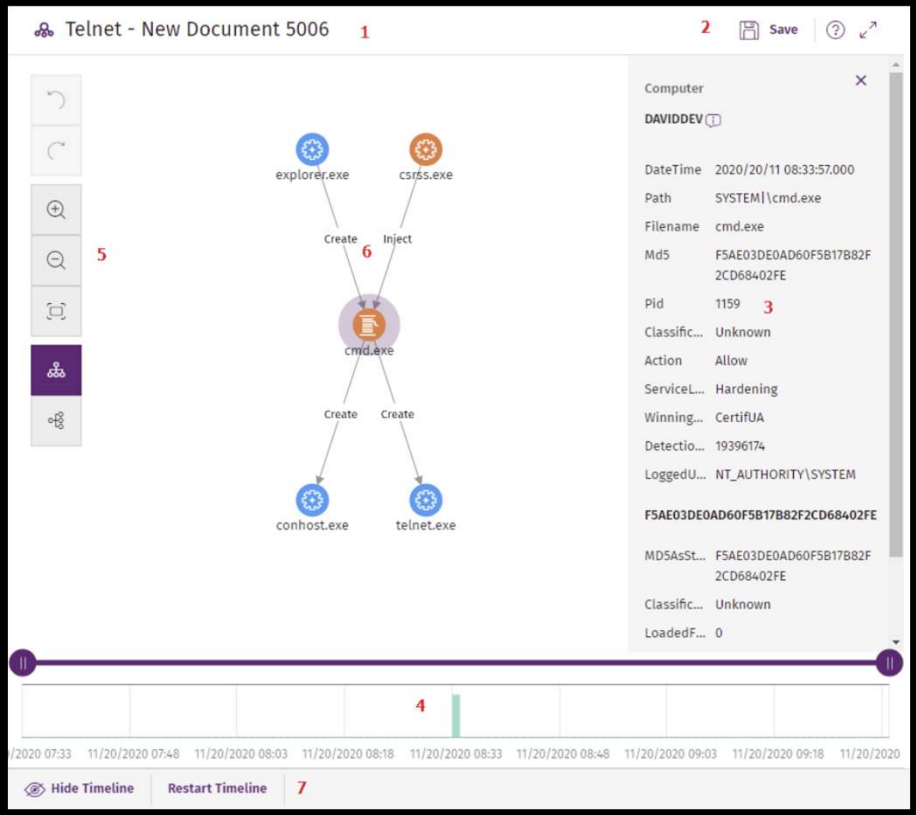
Investigation Graphs in WatchGuard Orion

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.



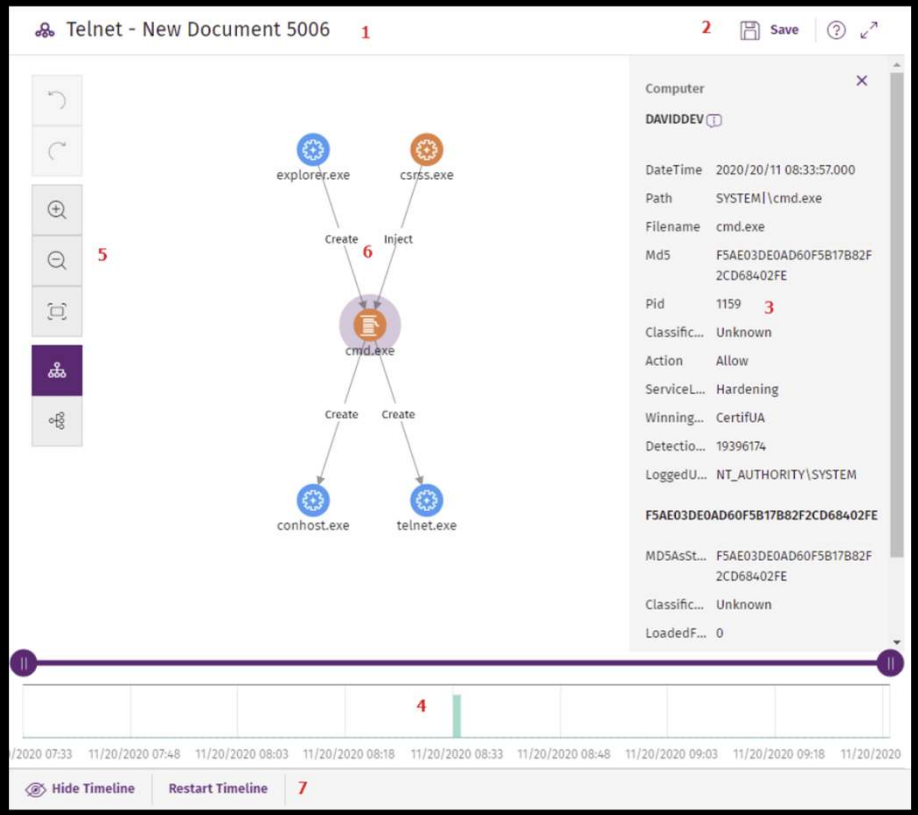


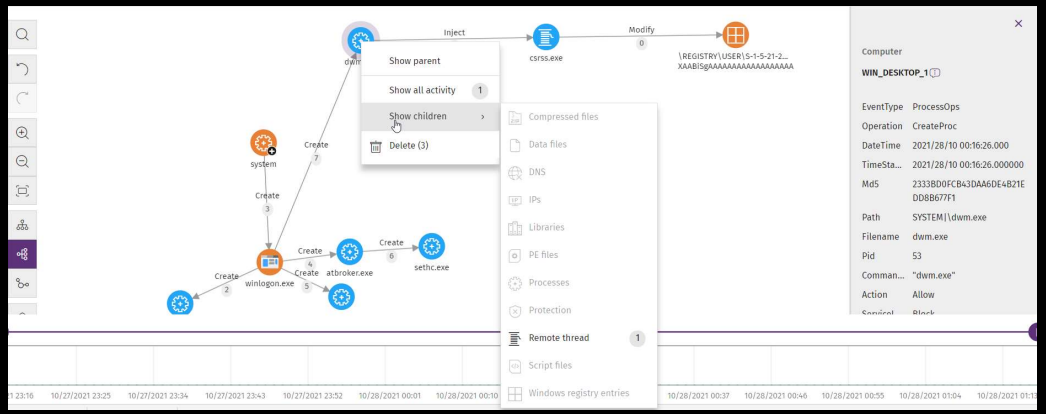
Investigation Graphs in WatchGuard Orion

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