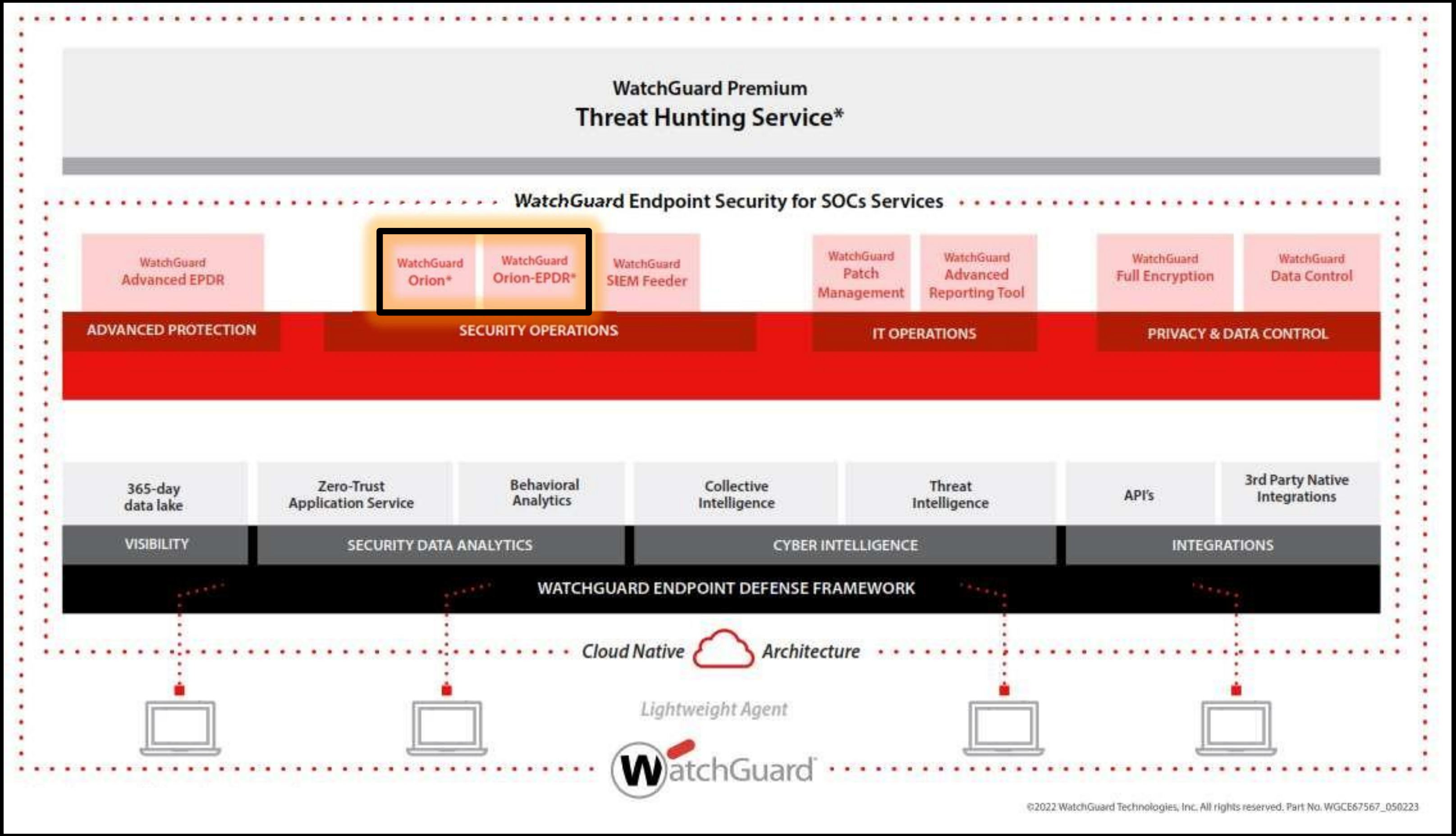
WatchGuard | ORION Security operation Center

WatchGuard Endpoint Solution & Services for SOCs



WatchGuard Premium
Threat Hunting Service*

WatchGuard Endpoint Security for SOCs Services

WatchGuard Advanced EPDR

WatchGuard Orion*

WatchGuard Orion-EPDR*

WatchGuard SIEM Feeder

WatchGuard Patch Management

WatchGuard Advanced Reporting Tool

WatchGuard Full Encryption

WatchGuard Data Control

ADVANCED PROTECTION

SECURITY OPERATIONS

IT OPERATIONS

PRIVACY & DATA CONTROL

365-day data lake

Zero-Trust Application Service

Behavioral Analytics

Collective Intelligence

Threat Intelligence

API's

3rd Party Native Integrations

VISIBILITY

SECURITY DATA ANALYTICS

CYBER INTELLIGENCE

INTEGRATIONS

WATCHGUARD ENDPOINT DEFENSE FRAMEWORK

Cloud Native Architecture

Lightweight Agent

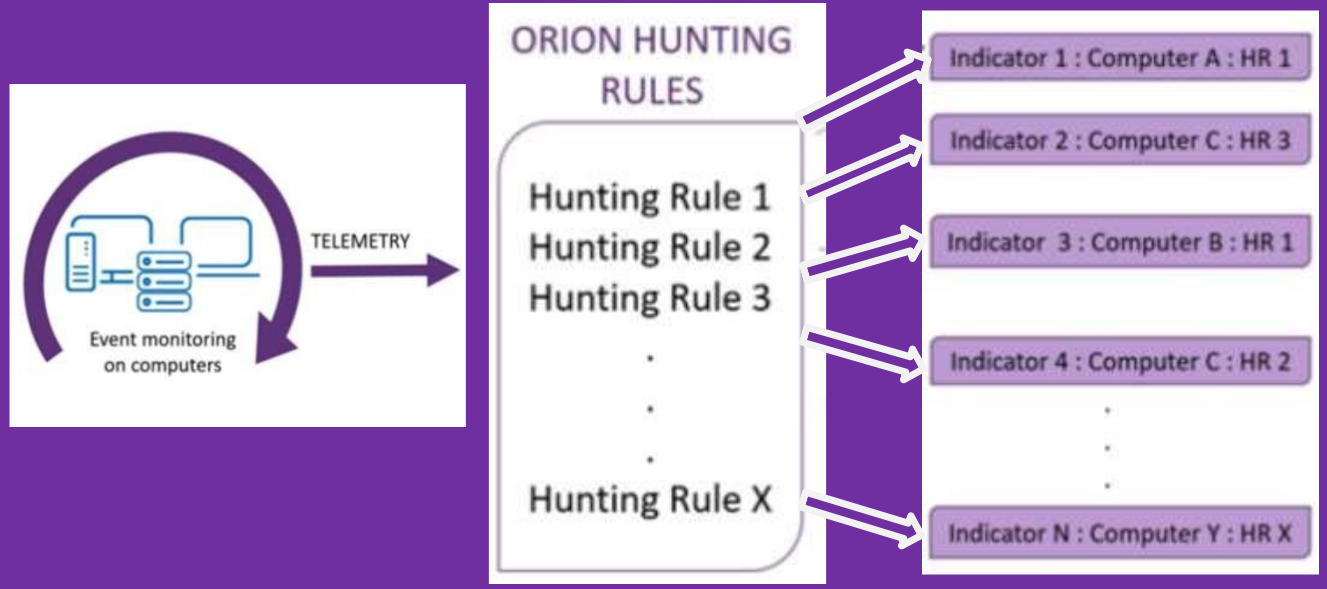
WatchGuard

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 techniques (LOTL)
- **reduces both the Mean Time to Detect (MTTD=212) and Mean Time to Respond (MTTR=75)**

ORION – key points

HUNTING – DETECTION


Event monitoring on computers
TELEMETRY
ORION HUNTING RULES
Hunting Rule 1
Hunting Rule 2
Hunting Rule 3
.
.
.
Hunting Rule X
Indicator 1 : Computer A : HR 1
Indicator 2 : Computer C : HR 3
Indicator 3 : Computer B : HR 1
Indicator 4 : Computer C : HR 2
.
.
.
Indicator N : Computer Y : HR X

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

INVESTIGATIONS

- Jupyter notebooks
- SQL queries
- Computer investigations
- Graphs

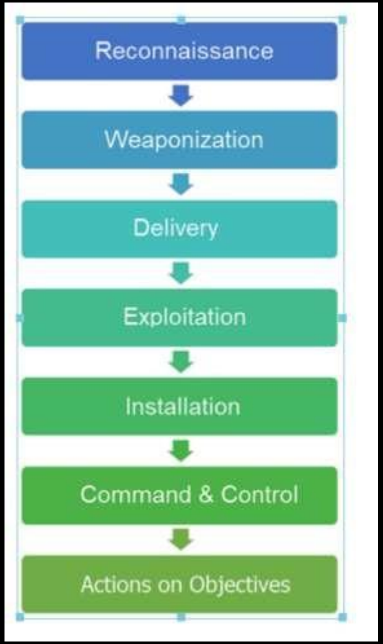
RESPOND

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

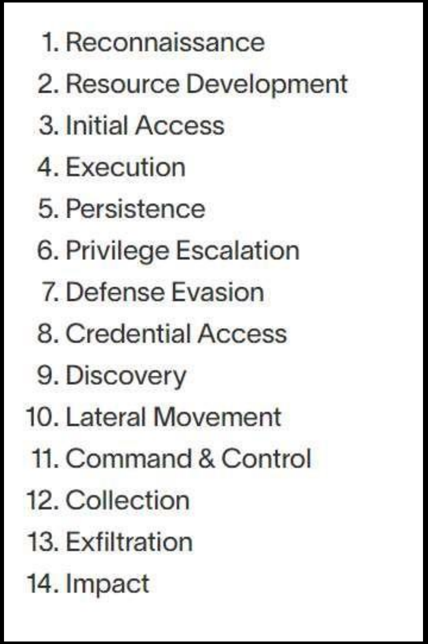
The Cyber Kill Chain and The MITRE ATT&CK

- **Models for identification and prevention of cyber intrusions activity**

The CKC



The Enterprise ATT&CK matrix



1. Reconnaissance
2. Resource Development
3. Initial Access
4. Execution
5. Persistence
6. Privilege Escalation
7. Defense Evasion
8. Credential Access
9. Discovery
10. Lateral Movement
11. Command & Control
12. Collection
13. Exfiltration
14. Impact

- It's important to have multiple layers of protection to ensure that if one of the defenses is bypassed there is another line of defense to protect organization's assets

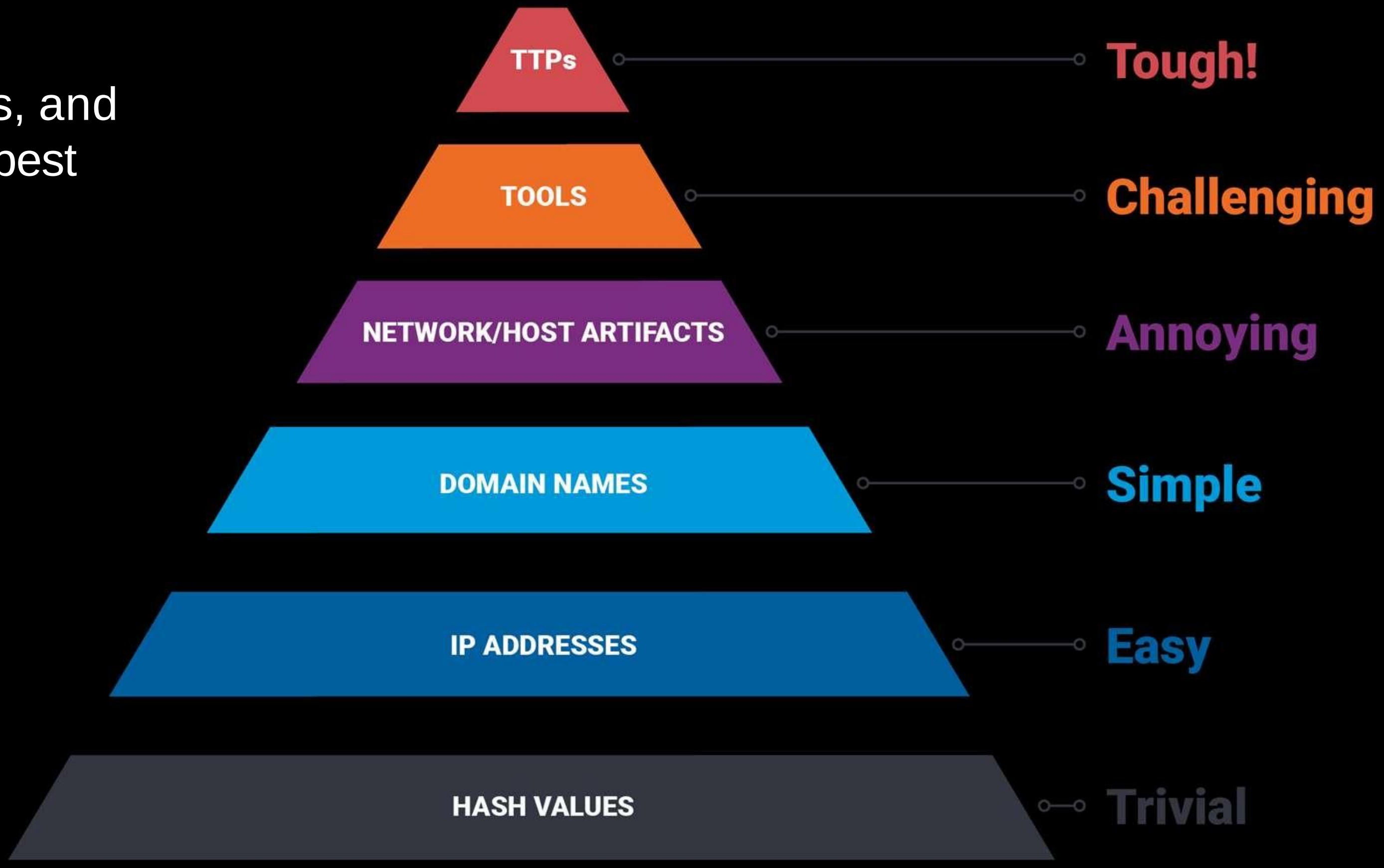
- Orion can stop attacks in any of the phases defined in the CKC and ATT&CK frameworks

- Orion downloads the MITRE tactic, technique, and sub-technique knowledge base twice a day

WatchGuard

The Pyramid of Pain

WHY searching for Tactics, Techniques, and Procedures is the best prevention?



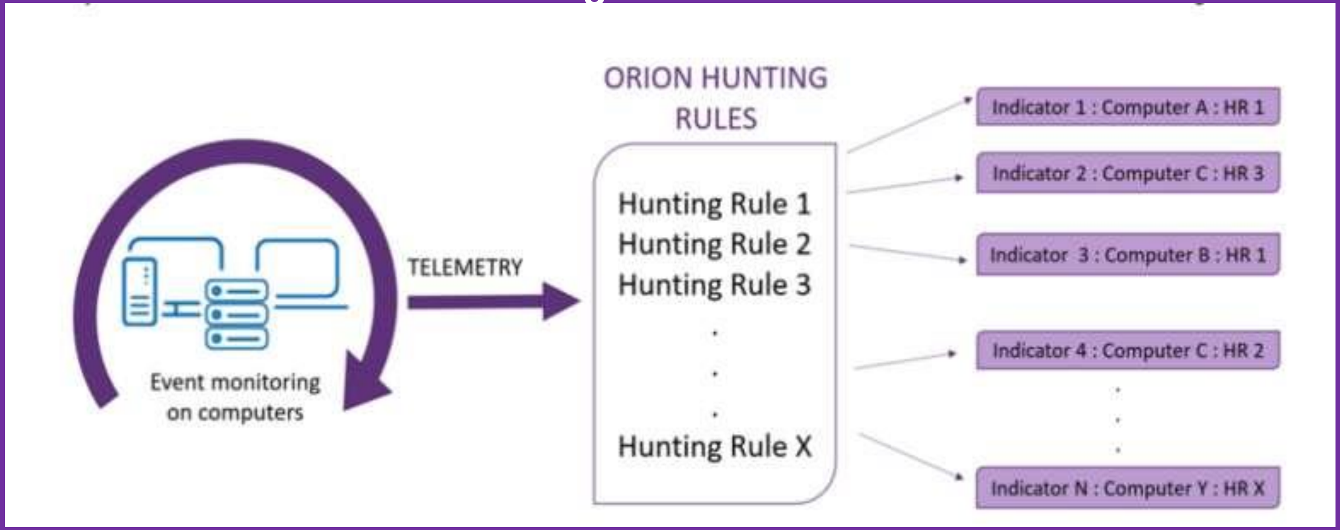
WHY SOC, WHY ORION?

Preventing incidents can be painful,

but responding to them is usually worse!

LIVE DEMO

Hunting – Detection


Event monitoring on computers
TELEMETRY
ORION HUNTING RULES
Hunting Rule 1
Hunting Rule 2
Hunting Rule 3
Hunting Rule X
Indicator 1 : Computer A : HR 1
Indicator 2 : Computer C : HR 3
Indicator 3 : Computer B : HR 1
Indicator 4 : Computer C : HR 2
Indicator N : Computer Y : HR X