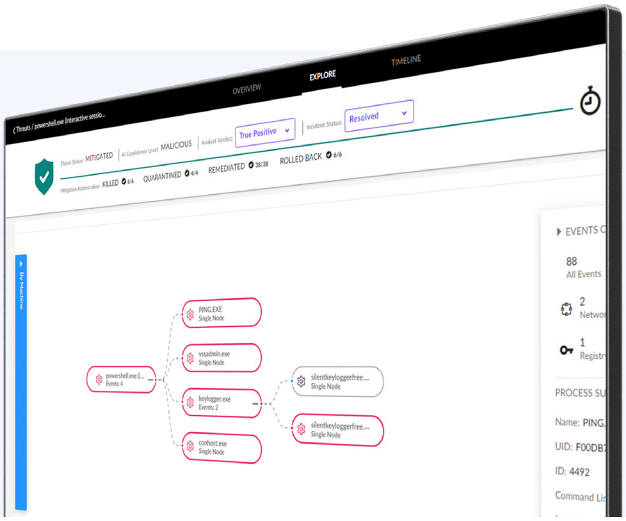
WWCS
World Wide Communication Services
sales@wwcspro.com

Endpoint Detection and Response

Endpoint Detection and Response (EDR) helps prevent, detect, and quickly respond to ever-changing cyberthreats with behavioral AI threat detection, automated remediation, and rollback.


Threats / powershell.exe (interactive sessio...
Threat Status: MITIGATED
AI Confidence Level: MALICIOUS
Analyst Verdict: True Positive
Incident Status: Resolved
Mitigation Actions taken: KILLED 6/6 QUARANTINED 4/4 REMEDIATED 38/38 ROLLED BACK 6/6
88 All Events
2 Netwo
1 Registr
PROCESS SU
Name: PING.
UID: F00DB
ID: 4492
Command Li

Leverage multiple AI detection engines

- Harness AI to analyze new threat patterns and machine learning to evolve response
- Detect malicious activities such as memory exploitation with behavioral AI
- Detect signature-less advanced file-based malware with static AI

Help prevent cyber attacks

- Protect against the latest threats without waiting for recurring scans or malware definition updates
- Enforce policy-driven protection tailored to your users: allow/block USB and device connections as needed

Respond effectively through automation

- Automate quick threat containment, as well as “kill,” quarantine, and remediation actions
- Roll back endpoints and compromised files to their pre-attack healthy state in case of ransomware (Windows OS only)

Accelerate threat investigation

- Investigate using readily available threat intelligence from leading third-party feeds and SentinelOne sources
- Visualize threat activity—the full chain of events making up an attack—to quickly understand its context, root cause, and lateral movements

Powered by SentinelOne®,

leader in the 2022 MITRE Engenuity™ ATT&CK® Evaluation:

- 100% Protection and Detection
- Highest Visibility and Analytic Coverage
- 100% Real-Time. Zero Detection Delays