SentinelOne Delivers Top Coverage For Both Enterprise ATT&CK & Deception ATT&CK Evaluation

2022 Enterprise ATT&CK Evaluation

The 2022 Enterprise ATT&CK Evaluation emulates the real attack methods of Wizard Spider and Sandworm, two APT threat groups that conduct ransomware campaigns for financial gain and data destruction. According to MITRE, these two threat actors were chosen based on their complexity, relevancy to the market, and how well MITRE Engenuity's staff can fittingly emulate the adversary. MITRE Engenuity tested our product, Singularity XDR, evaluating both detection and protection.

2022 Deception ATT&CK Evaluation

Starting this year, MITRE also launched the inaugural MITRE Engenuity ATT&CK Deception Evaluation. This evaluation expands the ATT&CK landscape to test vendors on their deception capabilities. The evaluation can dramatically increase analyst confidence in detection via high fidelity tripwires, causing the adversary to waste time, money, or capability, and potentially provide vendors critical new insights into adversary behavior.

The Results

SentinelOne excelled in delivering top coverage across both the evaluations once again demonstrating its commitment to pushing the boundaries to help enterprises gain control of their dynamic attack surface.

Top Coverage for Both Enterprise ATT&CK and Deception ATT&CK Evaluation

Leader in Enterprise ATT&CK Evaluations 3 Years Running

Leader in Deception ATT&CK Evaluation, Defending Against Identity-based Attacks

Industry-leading Proof That Singularity XDR Reduces Risk Across Various Attack Surfaces

INAUGURAL 2022 DECEPTION ATT&CK EVALUATION HIGHLIGHTS

MITRE ENGENUITY ATT&CK® EVALUATIONS
Trials
DECEPTION 2022

Deliver Real-time Protection Against Active Directory (AD) Compromise

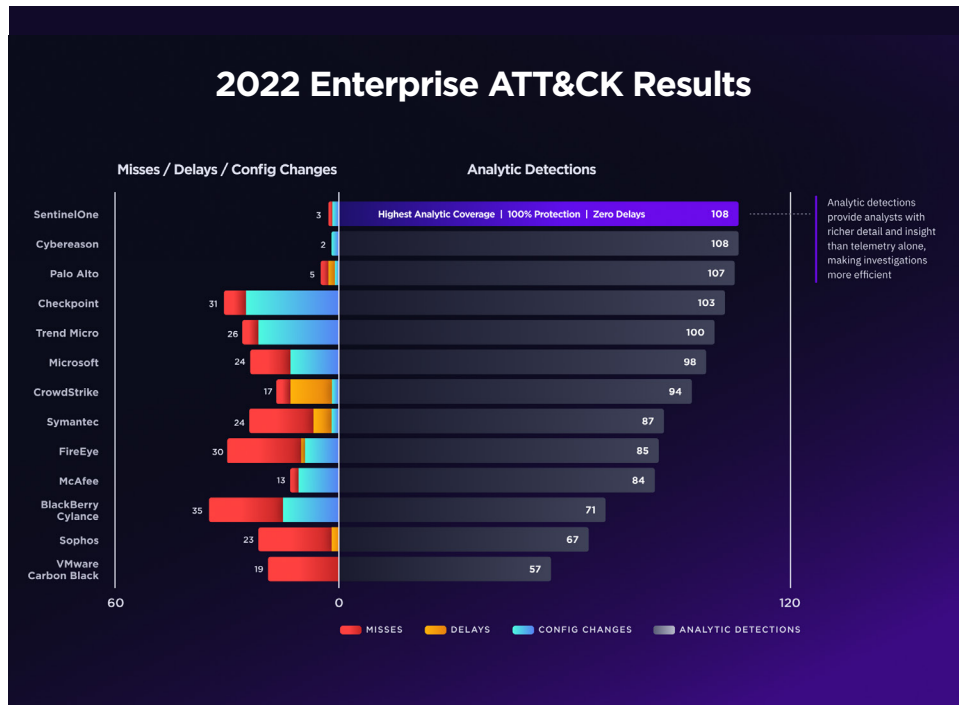Secure Critical Assets With Data Cloaking

Stop Lateral Movement and Privilege Escalation

Maximize Insight Into the Adversary Behavior

As the first and only XDR vendor to participate and lead across both the evaluations, SentinelOne's performance demonstrates how we're uniquely positioned to defend organizations across various attack surfaces and drive business value and help customers excel across major KPIs.

2022 Enterprise ATT&CK Results

Misses / Delays / Config Changes | Analytic Detections

Analytic detections provide analysts with richer detail and insight than telemetry alone, making investigations more efficient

Vendor	Misses/Delays/Config	Analytic Detections
SentinelOne	3	108 (Highest Analytic Coverage | 100% Protection | Zero Delays)
Cybereason	2	108
Palo Alto	5	107
Checkpoint	31	103
Trend Micro	26	100
Microsoft	24	98
CrowdStrike	17	94
Symantec	24	87
FireEye	30	85
McAfee	13	84
BlackBerry Cylance	35	71
Sophos	23	67
VMware Carbon Black	19	57

MISSES DELAYS CONFIG CHANGES ANALYTIC DETECTIONS

Visit **S1.ai/mitre** to learn more about the **ATT&CK Framework.**

READY FOR A DEMO?

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation
- 100% Protection. 100% Detection.
- Top Analytic Coverage 3 Years Running
- 100% Real-time with Zero Delays

Gartner peer insights
4.9 ★★★★★

99% of Gartner Peer Insights™
EDR Reviewers Recommend SentinelOne Singularity

FR FedRAMP
AICPA SOC
TEVORA PCI DSS Attestation HIPAA Attestation
vb 100 VIRUS virusbtn.com
AAA
SE Labs BEST Innovator WINNER 2021

About SentinelOne

SentinelOne is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks at faster speed, greater scale and higher accuracy than human-powered technology alone. The Singularity XDR platform offers real-time visibility and intelligent AI-powered response. Achieve more capability with less complexity.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733