SentinelOne White Paper

SentinelOne

MITRE ENGENUITY

MITRE Engenuity™ ATT&CK® Evaluation

SentinelOne Participates for the Fourth Year with Record Performance

April 2022

Table of Contents

Introduction	**3**
2022 Enterprise ATT&CK Evaluation	**4**
Results	**5**
What the Results Mean for You	**10**
Ready for a Demo?	**10**

01

Introduction

MITRE has become the common language of EDR and is the de facto way to evaluate a product's ability to provide actionable information to the SOC. For three years now, MITRE Engenuity has conducted independent evaluations of cybersecurity products to help the industry and government institutions make better decisions to combat security threats and improve their threat detection capabilities. Leveraging the ATT&CK framework, evaluations assess various vendors on their ability to automatically detect and respond to real-life cyberattacks within the context of the ATT&CK framework. The results indicate a solution's ability to provide security analysts a quick, clear picture of how an attack unfolded. Participating vendors are measured on their ability to detect and address real-world threats through the language and structure of the ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework.

SentinelOne remains a steadfast supporter of MITRE Engenuity's objective approach. They are indeed a catalyst for cybersecurity innovation not only in the vendor community but also within 1000's of organizations that now use ATT&CK as a common lexicon for understanding who the adversaries are and their typical game plans. ATT&CK helps the industry clearly communicate the exact nature of threats and makes it clear how to enhance defenses to blunt the impact. Overall, ATT&CK serves as a flexible model and invaluable tool for applying intelligence to cybersecurity operations.

SentinelOne's stellar performance delivers maximum cybersecurity value for the fourth year running

100% Protection

9 of 9 MITRE ATT&CK Tests

100% Detection

19 of 19 Attack Steps

100% Real-Time Protection

0 Delays

99% Visibility

108 of 109 Attack Sub-Steps

99% Highest Analytic Coverage

108 of 109 Detections

02

2022 Enterprise ATT&CK Evaluation

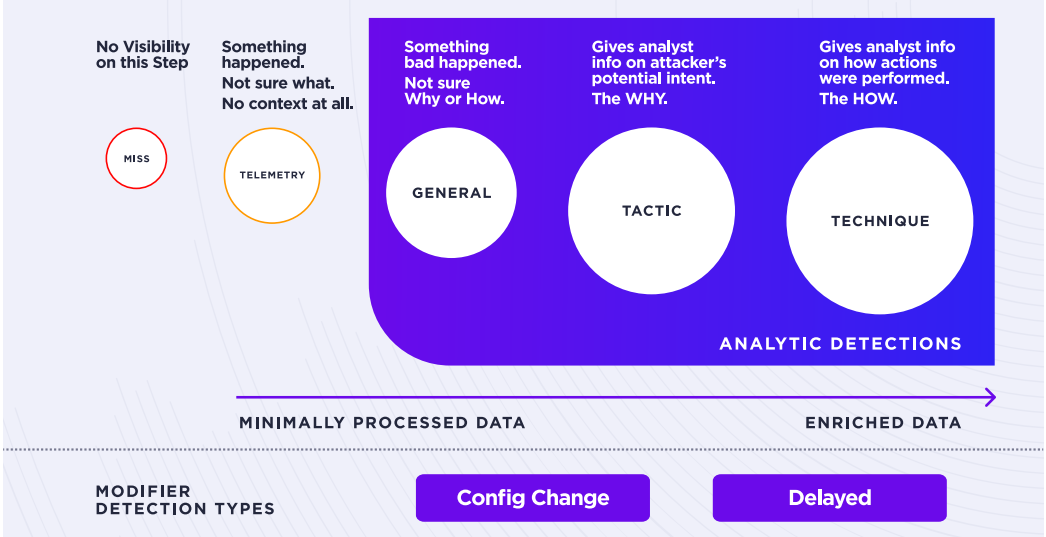
The 2022 Enterprise ATT&CK Evaluation emulates the real attack methods of Wizard Spider and Sandworm, two APT threat groups that conduct ransomware campaigns for financial gain and data destruction. According to MITRE, these two threat actors were chosen based on their complexity, relevancy to the market,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

- Wizard Spider is a financially motivated criminal group that has been conducting ransomware campaigns since August 2018 against a variety of organizations, ranging from major corporations to hospitals.
- Sandworm is a destructive Russian threat group that is known for carrying out notable attacks such as the 2015 and 2016 targeting of Ukrainian electrical companies and 2017's NotPetya attacks.

The Evals team chose to emulate two threat groups that abuse the Data Encrypted For Impact (T1486) technique. In Wizard Spider's case, they have leveraged data encryption for ransomware, including the widely known Ryuk malware (S0446). Sandworm, on the other hand, leveraged encryption for the destruction of data, perhaps most notably with their NotPetya malware (S0368) that disguised itself as ransomware. While the common thread to this year's evaluations is "Data Encrypted for Impact," both groups have substantial reporting on a broad range of post-exploitation tradecraft.

Though the ATT&CK evaluation is not a competition, the results do help organizations understand relative product performance under emulated adversary conditions. The 2022 test takes place over two days and involves 19 distinct steps comprising 109 sub-steps. This year MITRE Engenuity emulates the Wizard Spider adversary group on Day 1 and the Sandworm adversary group on Day 2.

Arm yourself against exaggerated competing vendor claims by taking time to understand the differences among ATT&CK's detection categories. In summary, not all detections have the same level of quality. On one end of the quality, spectrum is "Telemetry" which is simple "minimally processed data." On the other end of quality are "Techniques" that, according to the ATT&CK website, "gives the analyst information on how the action was performed or helps answer the question 'what was done'." The evaluation describes "Analytic Detections" as the sum total of all three higher quality, enriched detection types labeled as General, Tactic, and Technique. Lastly, ATT&CK defines two modifiers, configuration change and delayed. During testing, if the vendor modifies how their product operates to adjust for whatever reason, the evaluation proctors note these as "configuration changes." During testing, if a "detection is not immediately available to the analyst due to additional processing unavailable due to some factor that slows or defers its presentation," this detection is labeled as "delayed."

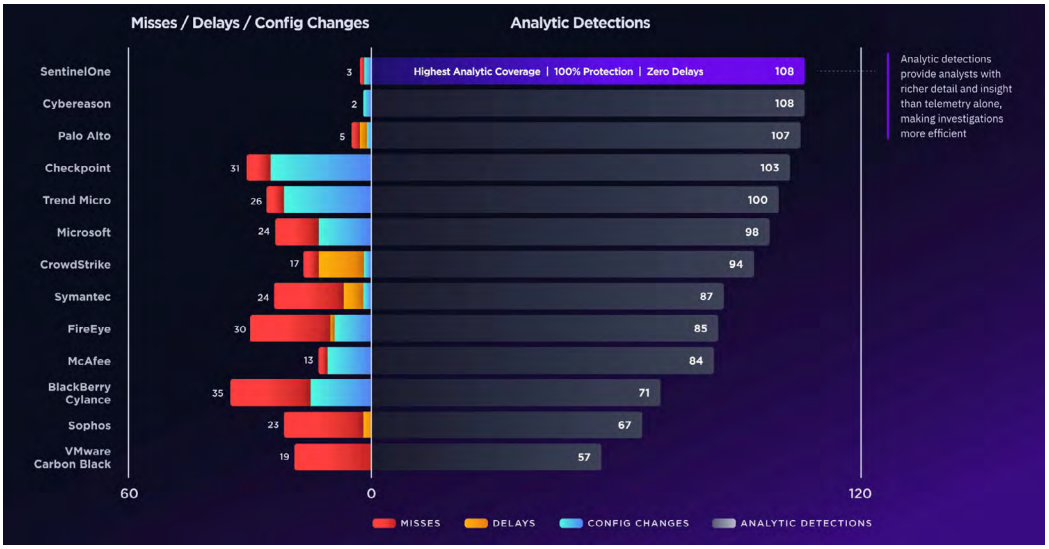


03

Results

SentinelOne had exceptional results in the 2022 ATT&CK evaluation and excelled in every category. SentinelOne's performance in the evaluation demonstrates how we're uniquely positioned to drive business value and help customers excel across major KPIs:

- SentinelOne delivered 100% Protection: (9 of 9 MITRE ATT&CK tests)
- SentinelOne delivered 100% Detection: (19 of 19 attack steps)
- SentinelOne delivered 100% Real-time (0 Delays)
- SentinelOne delivered 99% Visibility: (108 of 109 attack sub-steps)
- SentinelOne delivered 99% - Highest Analytic Coverage: (108 of 109 detections)
- SentinelOne consolidated all the data points over 2 days into only 9 campaign level alerts



SentinelOne's superior visibility, actionable context, the ability to defeat adversaries in real-time, and out-of-the-box efficacy Singularity XDR provides sets us apart from every other vendor on the market.

Other highlights of the evaluation detection results follow.

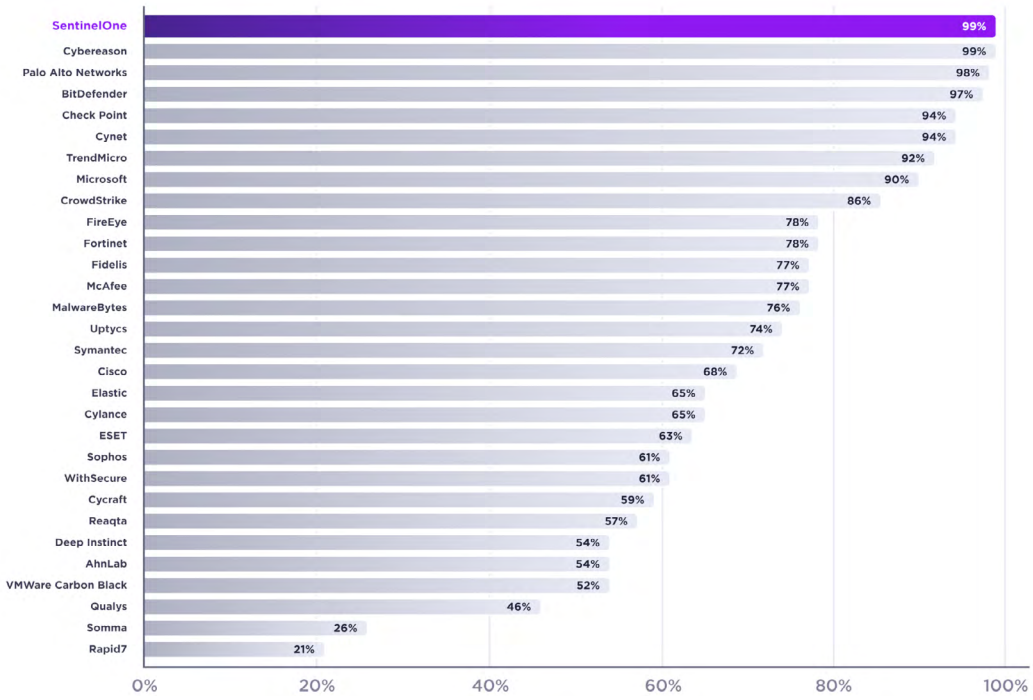
1. SentinelOne Singularity XDR delivered the highest analytic coverage three years in a row. And we do this across all tested operating systems – Windows & Linux.

Analytic detections are contextual detections that are built from a broader data set and are a combination of technique plus tactic detections. This produces a detailed view of what took place, why, and how. Having access to high-fidelity, high-quality detections saves operator time, maximizes response speed, and minimizes dwell time risk.

SOC teams often find themselves with too many alerts and not enough time to investigate, research, and respond. Alerts for the sake of alerts become meaningless: unused and unnoticed. Pinpointed alerts that are actionable with pre-assembled context maximize EDR effectiveness and use.

SentinelOne's patented Storyline technology percolates every event happening in real-time, providing a fulling indexed, prefabricated map for each alert. All this work happens on the agent side, resulting in a massive advantage compared to technology or teams that try to figure out what happened after everything happened – when it's too late. The power of autonomous cybersecurity is that it happens in real-time, where and when the action is taking place, on the attack surface itself.

Analytic detections create context and actionable alerts. SentinelOne Singularity XDR delivered the highest analytic coverage three years in a row.



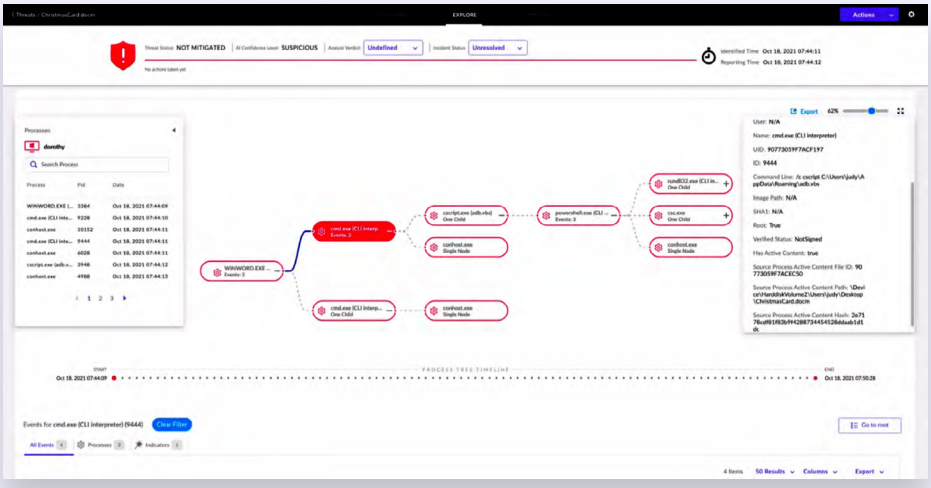
According to MITRE Engenuity's published results, SentinelOne recorded the highest number of analytic detections for this year's evaluation as well as the last three years.

SentinelOne is unique among vendors in that it achieved the highest high-quality "analytic detections" in the last three ATT&CK evaluations.

2. Visibility Ensures That No Threats Go Undetected. SentinelOne delivered 100% detection and flawlessly detected EVERY attack step in the 2022 Enterprise Evaluation.

Visibility is the building block of EDR and is a core metric across MITRE Engenuity results. In order to understand what's going on in the enterprise as well as accurately threat hunt, cybersecurity technology needs to create a visibility aperture. The data needs to be accurate and provide an end-to-end view of what happened, where it happened, and who did the happening regardless of device connectivity or type.

During the ATT&CK Evaluation, the TTPs used by Wizard Spider and Sandworm were grouped into 19 attack steps, and SentinelOne Singularity detected all of them. This allows a comprehensive view of the entire enterprise, minimizing incident dwell time and reducing risk.



SentinelOne Singularity XDR detects malicious file execution and automatically correlates it with other data to provide context.

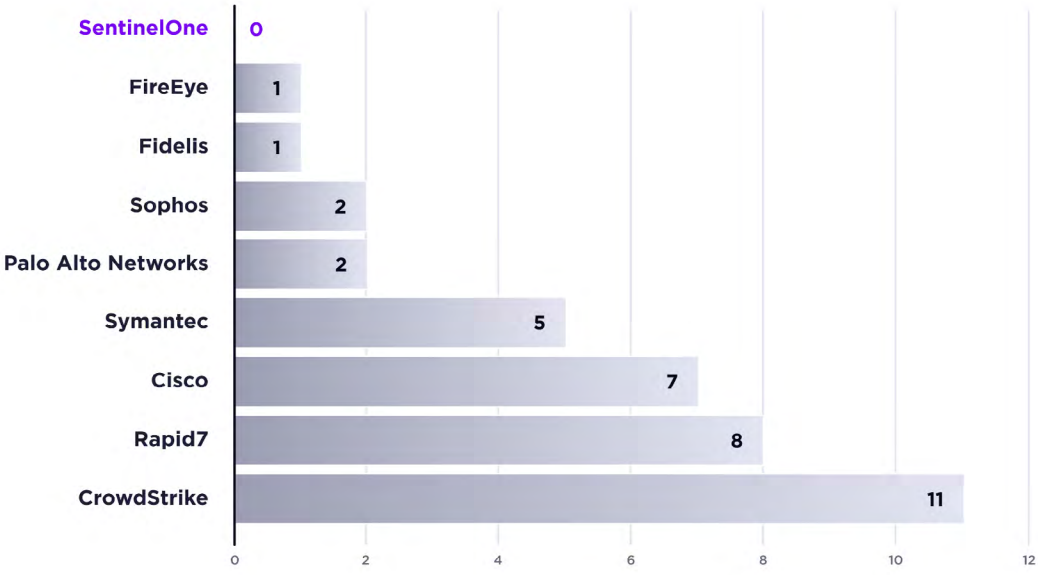
SentinelOne had zero telemetry detections, meaning ALL of the detections were high-quality analytic coverage providing security analysts with automated context.

3. SentinelOne experienced zero delayed detections, making EDR real-time.

Time is a critical factor whether you're detecting an attack or neutralizing it. A delayed detection during the evaluation often means that an EDR solution requires a human analyst to manually confirm suspicious activity due to the inability of the solution to do so on its own. The solution typically needs to send data to the analyst team or third-party services such as sandboxes, which in turn analyzes the data and alerts the customer, if required. However, many critical parts of this process are done manually, resulting in a window of opportunity for the adversary to do real damage.

All SentinelOne detections are real-time, with zero delays, reducing incident dwell time through automation. Vendors that have delays are often far more human/linear/slower behind the scenes and lack automation.

As the ATT&CK evaluation data shows, SentinelOne had zero delayed detections.



4. SentinelOne Singularity delivered 100% Protection Across Operating Systems With the Fastest Threat Containment.

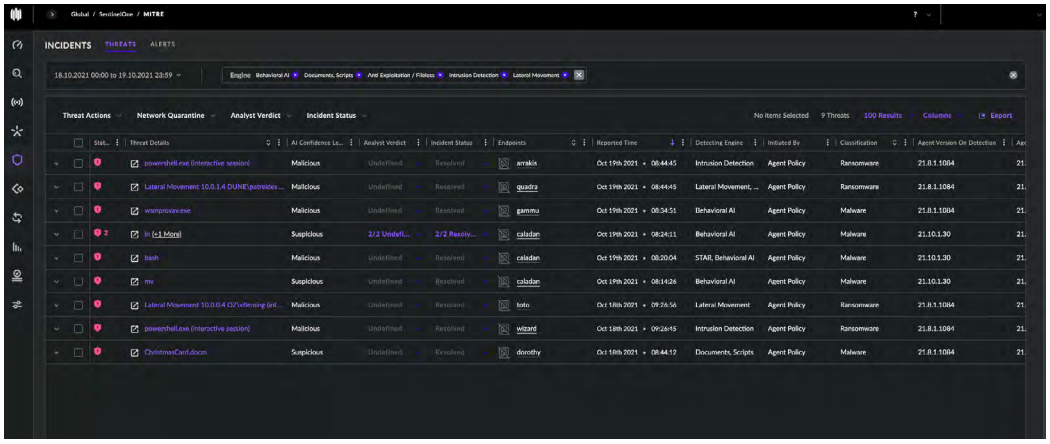
Security teams demand technology that matches the rapid pace at which adversaries operate. MITRE Protection determines the vendor's ability to rapidly analyze detections and execute automated remediation to protect systems.

SentinelOne delivered the fastest protection. With its real-time protection, Singularity XDR provided the MITRE ATT&CK Evaluation with the least amount of permitted actions in the kill-chain for attackers to do damage. The ATT&CK results reveal our commitment to preventing and protecting against every possible threat and keeping our customers safe from most adversaries.

> SentinelOne delivered the fastest and earliest protection with the least amount of permitted actions in the kill-chain for attackers to do damage, dramatically reducing incident dwell time.

5. SentinelOne excels at the analyst user experience, reducing the amount of manual effort required to understand what's happening. It automatically grouped two days of testing into only nine campaign-level console alerts.

Consolidating hundreds of data points across a 48-hour advanced campaign, SentinelOne correlated and crystallized the attack into one complete story. SentinelOne provides instant insights within seconds rather than having analysts spend hours, days, or weeks correlating logs and linking events manually. SentinelOne reduces the amount of manual effort needed, helps with alert fatigue, and significantly lowers the skillset barrier to benefiting from EDR.



04

What the Results Mean for You

As a security leader, it's essential that you look at how you can improve your security posture and reduce risk while reducing the burden on your security team. SentinelOne's exceptional performance in 2022 ATT&CK evaluations once again proves that purpose-built, future-thinking solutions deliver the in-depth visibility, automation, and speed that the modern SOC needs to combat adversaries. As evidenced by the results data, SentinelOne excels at visibility and detection and, even more importantly, in the autonomous mapping and correlating of data into fully indexed and correlated stories through Storyline™ technology. This technology advantage sets us apart from every other vendor on the market.

Ready for a Demo?

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

sentinelone.com

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

Gartner peerinsights™ 4.9 ★★★★★

98% of Gartner Peer Insights™

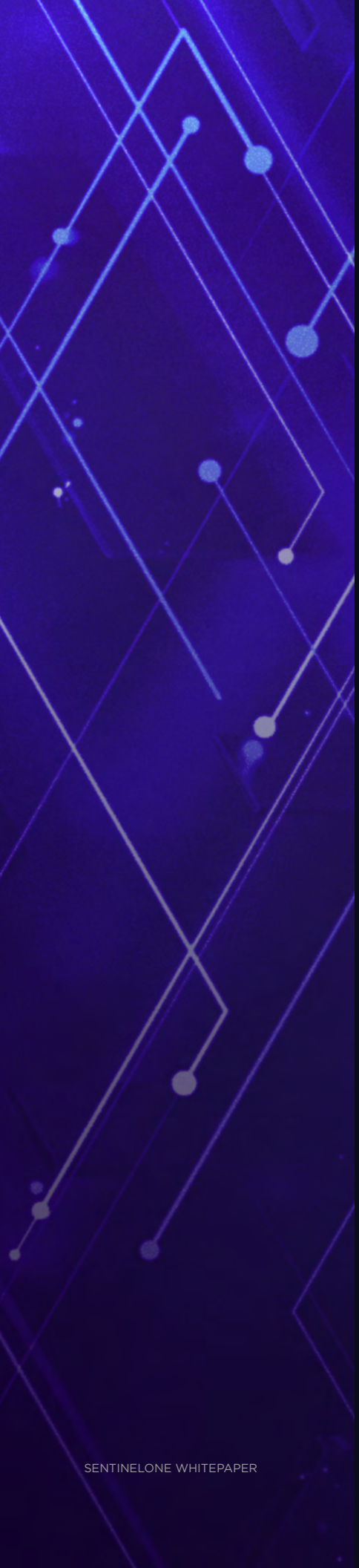
Voice of the Customer Reviewers recommend SentinelOne

FedRAMP

ISO 27001 CERTIFIED by schellman

TEVORA

PCI DSS Attestation
HIPAA Attestation



SentinelOne

Contact us

sales@sentinelone.com

+1-855-868-3733

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

sentinelone.com

2022_MITRE_Engenuity_ATT&CK_Evaluation_04272022

© SentinelOne 2022