

Singularity | HOLOGRAM

Angreifer mit Täuschungstechnologien enttarnen

Wer spioniert und was will er? Angreifer, die sich bereits Zugang zur Umgebung verschafft haben, werden an einem bestimmten Punkt versuchen, zu lateralen Bewegungen überzugehen. Gleichzeitig können Mitarbeiter mit privilegiertem Zugriff und entsprechenden Motiven eine Insider-Bedrohung darstellen.

Singularity Hologram, eine Komponente der SentinelOne Singularity XDR-Plattform bringt netzwerkinterne Angreifer und böswillige Insider mit modernen interaktiven Täuschungs- und Ködertechologien dazu, aktiv zu werden und sich zu zeigen. Dazu imitiert Singularity Hologram Produktionsbetriebssysteme, Anwendungen, Daten usw. Diese Lösung erfasst detaillierte Telemetriedaten und speichert verwertbare Informationen, damit Sie Ihre Verteidigung organisieren können.



Ein weites Netz

Durch Imitieren von Produktions-Betriebssystemen, Anwendungen, Daten, Industriesteuersystemen, IoT, Cloud-Funktionen und mehr können Sie Bedrohungsakteure anlocken, die Erkundungsaktivitäten durchführen.



Identifizierung aktiver Kompromittierungen

Sie können überall im Netzwerk befindliche Bedrohungsakteure und Insider überführen, die sich lateral bewegen und mit Täuschungs-Assets und Ködern interagieren.



Visualisierung und Stärkung

Angriffe auf das Netzwerk können schnell visualisiert und ihr zeitlicher Ablauf angezeigt werden. Mit den daraus gewonnenen Erkenntnissen können Sie Ihre Schutzmaßnahmen verstärken.



Erweiterung und Erfassung

Die Integration mit der Bedrohungserkennung und Reaktion von Singularity Identity™ (ITDR) ermöglicht umfassenden Schutz für Endpunkte und Active Directory.

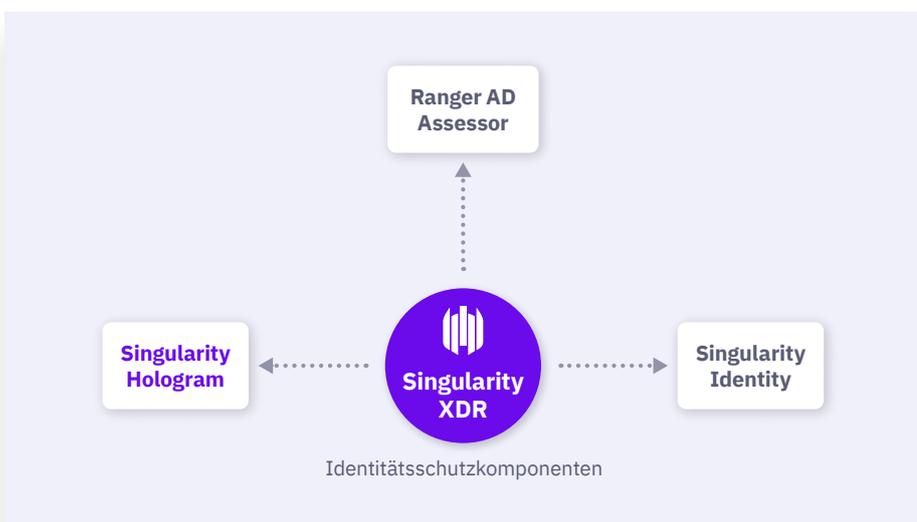
84 % der Unternehmen haben bereits eine identitätsbezogene Sicherheitsverletzung verzeichnet. Singularity Hologram deckt Angriffsversuche in Echtzeit auf.

WICHTIGE FUNKTIONEN UND VORTEILE

- + Enttarnung verdeckter Angreifer mit interaktiven Ködern, die Produktionsressourcen imitieren
- + Gewinnung verwertbarer TTP-Daten und Forensiken für Untersuchungen
- + Verfolgung von Netzwerkangriffen im Zeitverlauf und Erstellung wiederholbarer Prozesse sowie Szenarien für künftige Reaktionen
- + Verkürzung des Zeitaufwands für die Erkennung, Analyse und Abwehr von Angriffen
- + Flexible Bereitstellung und schnelle Einsatzbereitschaft

Singularity Hologram bildet mit Singularity Identity™ eine komplette Täuschungs- und Identitätslösung.

Weitere Informationen unter s1.ai/hologram



Auch hervorragend getarnte Angreifer gehen in die Falle

Singularity Hologram-Netzwerkköder erkennen und warnen Sie vor imminenter Gefahren und Aktivitäten in Ihrer Umgebung, denen heute vorwiegend Unternehmen ausgesetzt sind. Dazu gehören:

- MitM-Aktivitäten (Man-in-the-Middle)
- Ransomware und andere Malware
- Hochentwickelte dauerhafte Bedrohungen (APTs)
- Erkundungsaktivitäten
- Insider-Bedrohungen

Singularity Hologram-Köder lassen sich nicht von Produktionsressourcen unterscheiden und sind dazu gedacht, Angreifer von den echten Systemen und Daten wegzulocken. Alle Köder passen sich an eine breite Palette von Formfaktoren und an verschiedenste geschäftlichen und organisatorische Anforderungen an, zum Beispiel:

- ICS-SCADA-Industriesteuersysteme
- Emulationen für SWIFT-Terminals, Kassensysteme (Point-of-Sale, POS), VoIP-Telekommunikationssysteme, Netzwerkrouter und Switches sowie IoT-Spezialgeräte
- Windows- und Linux-Betriebssysteme
- Serverlose und Storage-Cloud-Technologien

So viele Informationen möglich über die Angreifer wie möglich

Mit der Täuschungstechnologie von Singularity Hologram können Sie nicht nur aktive Angreifer in Ihrer Umgebung erkennen und bekämpfen, sondern Ihr Sicherheitsprogramm auch langfristig mit Informationen versorgen und stärken.

Wenn Sie Angriffe mithilfe von Singularity Hologram ablenken, gewinnen Sie verwertbare TTP-Informationen sowie gesicherte und fundierte Angriffsforensiken, die Untersuchungen unterstützen können. Angriffe lassen sich auch grafisch darstellen, im Zeitverlauf verfolgen und die zugehörigen Ereignisse der MITRE ATT&CK D3FEND™-Matrix zuordnen. Außerdem können Sie durch automatisierte, wiederholbare Prozesse und Szenarien die mittlere Reaktionszeit verkürzen.

SCHNELLE EINSATZBEREITSCHAFT

- + Ihnen stehen flexible Bereitstellungsoptionen zur Verfügung, z. B. eine optionale Integration in Singularity Identity.
- + Machine-Learning-Technologie vereinfacht die Bereitstellung.
- + Hardware- und virtuelle Hologram-Köder können für beliebige Standorte und Rechenzentren erstellt werden.
- + Bedrohungsinformationen von verteilten Ködern werden im Hologram Central Manager erfasst, der beliebige Implementierungen wie Google Cloud, AWS, Azure und OpenStack unterstützt.

WEITERE INFORMATIONEN

Besuchen Sie uns unter s1.ai/hologram.

Innovativ. Vertrauenswürdig. Anerkannt.

Gartner

Führender Anbieter im 2021 Magic Quadrant für Endpoint Protection-Plattformen

**MITRE
GENUINITY.**

Rekordergebnis bei der ATT&CK-Bewertung

- 100 % Schutz. 100 % Erkennung.
- Höchste analytische Abdeckung 3 Jahre in Folge
- 100 % Echtzeit und keinerlei Verzögerungen

**Gartner
peerinsights.**
4,9 ★★★★★

99 % BEI GARTNER PEER INSIGHTS™

EDR-Analysten empfehlen SentinelOne Singularity

FR
FedRAMP

**AICPA
SOC**

TEVORA
PCI DSS Attestation
HIPAA Attestation

**vb
100
VIRUS**
viruslist.com

AVAA

SE Labs
BEST
Innovator
WINNER 2021

Informationen zu SentinelOne

SentinelOne (NYSE:S) ist ein Vorreiter auf dem Gebiet der autonomen Cybersicherheit und verhindert, erkennt und stoppt Cyberangriffe schneller und genauer als je zuvor. Unsere Singularity XDR-Plattform schützt und stärkt weltweit führende Unternehmen mit einem Echtzeitüberblick über Angriffsflächen sowie mit plattformübergreifender Korrelation und KI-gestützten Reaktionen. Nutzen Sie mehr Optionen mit geringerer Komplexität.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733