SentinelOne

Singularity | IDENTITY

Identity Security Questionnaire

As identity-based attack surfaces become common targets for threat actors, more enterprises are turning to identity security solutions to provide the prevention, detection, and response capabilities their teams need to catch and neutralize indicators of credential misuse or theft, entitlement overprovisioning, and attacks based on privilege escalation or lateral movements.

Enterprise CISOs are invited to leverage this questionnaire to understand and get visibility into the identity and entitlement risks across their environments, from endpoints and networks to Active Directory and cloud-based surfaces or assets.

Visibility to Exposures and Risks

- How does your security team gain visibility into identity-related risks (such as risk related to credentials, entitlements, privileges)?
- Consider how your team assesses these risks at the endpoint, Active Directory, and cloud levels.
- How much effort is involved in identifying these identity-related risks?
- What level of visibility do you have into attack paths for attack surface management?
- What level of visibility do your identity security solutions provide at the user, device, and domain levels?
- What issues can your solutions identify relating to accounts, policies, groups, infrastructures, Kerberos security, or dangerous delegations, among other issues?
- How often do you re-evaluate these risks?
- How do you track these risks?
- How do you visualize your results and the risk associated with those results?
- How often does this information get updated?

Attack Detection

- How do you detect identity-based attacks at the endpoint, Active Directory, and cloud-based levels?
- How much manual work or effort goes into detecting identity-based attacks?
- How quickly can your security team detect and respond to identity-based attacks?
- How much data-sharing occurs between different security solutions regarding identity-based attacks?
- How do you address identity-based attacks related to lateral movement, credential theft, or privilege escalation?

Remediation and Mitigation

- ✓ What remediation options do your identity security solutions offer?
- ✓ How much automation do your tools provide for remediation?
- ✓ What mitigation information does the solution provide if remediation is not an option?

Analysis

- ✓ How actionable are your solution's alerts? Does the vendor provide mapping to the MITRE ATT&CK framework or another security framework?
- ✓ How does your identity security solution present its findings?
- ✓ What analysis tools does it provide? How much data sharing does it offer?

Once a CISO understands the strengths and process gaps related to their existing identity security stack, they can use this information to qualify the capabilities of competing security offerings. We encourage security teams to look at the depth of visibility and detection a solution provides, as well as the ability to provide comprehensive coverage from endpoints to Active Directory and multi-cloud environments.

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 peerinsights 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

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