

# Extended Detection and Response (XDR) Checklist

Today, threat actors are not just targeting individual, single machines; they are targeting an organization as a whole. The first machine to be compromised is just the starting point. From that initial entry, the attacker can conduct further surveillance and move through the network to identify valuable data before stealing it. Whilst Endpoint Detection and Response (EDR) tools are very effective, there only needs to be one weak link for the attacker to exploit. Extended Detection and Response (XDR) goes beyond just the endpoint and enables security teams to integrate and correlate events and alerts across a wide range

of security tools to improve visibility, reduce the time to detect even further and then respond quickly.

XDR is a strategy that helps organizations broaden their security program while recognizing the need for an expanded scope of visibility, detection, response, and automation. Enterprise CISOs and security practitioners are invited to leverage this questionnaire as they plan their XDR journey to stay ahead of the increasingly complex and constantly evolving cyber threats.

# 9

### **Reduced Security Risk**

- How many core security solutions, including endpoint security, does my team operate today? How well and sustainably do they integrate?
- Do we have cross-stack visibility and actionability of all the different security data streams?
- How many different agents/modules are required to achieve endpoint protection? What is the overhead of all these processes on my systems?
- Are the alerts we receive high-fidelity and actionable across my security stack?
- Are we equally protected from threats across Windows, Linux, MacOS, and Mobile?

- Does my endpoint security solution provide full MITRE coverage?
- Does my endpoint security solution provide full rollback capabilities? How quickly can this action be performed across multiple devices?
- Are we adequately securing cloud workloads with behavioral run time protection and detection?
- Are we protecting and detecting threats against Identity beyond traditional access and rights management? Do our security solutions provide us with the ability to effectively retain years of historical event/alert telemetry, often required for retrospective threat hunting but also for compliance?

# **(③)**

## **Empowered Security Teams**

- How much time does my security team spend manually investigating and triaging alerts?
- How often does my security team have to perform repetitive work in responding to cyber threats?
- How do we automate incident response playbooks today, across our security stack, without analyst intervention in a scalable and efficient manner?
- Are we able to effectively have a concise and converged view of all activities associated with a threat?
- Are we able to make automated remediation decisions without the need for analyst intervention?
- Does my solution provide a single, concise view of all activities associated with a threat, or are we flooded with multiple discrete events about each suspicious activity?

© SentinelOne 2023 S1-XDR-Checklist-0315202



#### **Breaking Data Silos**

- Do we have a single unified data lake that converges across our multiple security products?
- How many resources are dedicated to maintaining my security data platforms?
- Has my SIEM become a 'dumping ground' for security event data with little actionable value?
- Does my existing SIEM provide integrated response capabilities without complex workflow creation?
- How many consoles does my security team operate?
- How easily can my security analysts find critical signals through all the noise?
- Can my security tools automatically map alerts to MITRE
- How much time does my security team spend on the manual correlation of data?



#### **TCO Reduction**

- Can we integrate additional third-party security tools (like threat intelligence and sandbox capabilities) into our Endpoint, Identity, and Cloud threat triage and response workflow?
- Is integrating with other technologies simple and frictionless?
- How much data do we ingest into our current security data lake/SIEM? Does that include high-fidelity (and high-volume) EDR data? Are there specific regulatory requirements we must comply with for data visibility and retention?
- What is our data retention and storage cost?
- How many resources are dedicated to maintaining the security data platforms?

CISOs must take a close look at organizational objectives as well as their current technology capabilities when selecting the best XDR solution for their particular needs. Doing so will help ensure they receive the most value from their investment in an XDR solution. Once a CISO understands the strengths and process gaps related to their existing security stack, they can use this information to qualify the capabilities of competing security offerings. We encourage organizations to look at how an XDR solution automates and empowers security teams, breaks down data silos as well as provides comprehensive coverage from endpoints to identity and multi-cloud environments.



#### Innovative. Trusted. Recognized.

## Gartner.

A Leader in the 2022 Magic **Quadrant for Endpoint Protection Platforms** 



#### **Record Breaking ATT&CK Evaluation**

- 100% Protection 100% Detection
- Top Analytic Coverage, 3 Years Running
- 100% Real-time with Zero Delays

#### Gartner. Peer Insights...

#### 96% of Gartner Peer Insights™

**EDR Reviewers Recommend** SentinelOne Singularity

















#### **About SentinelOne**

SentinelOne (NYSE:S) 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 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