

An Architect's Checklist

Building a Data Platform to Power the Modern SOC

Defending against modern threats starts with data. A lot of it. Spotting, understanding, and disrupting cyber adversaries requires deep awareness of everything happening across your organization, from the desktop to the cloud. Collecting, storing, and working with telemetry at scale unlocks crucial workflows for defenders, including:



More Sophisticated Autonomous Detections: With real-time access to deep and extensive datasets, your systems can employ advanced algorithms and machine learning to autonomously detect complex threats that might otherwise remain hidden. This means stopping more threats faster than ever, often before they can cause significant damage.



Faster and More Effective Threat Investigations: When every second counts, quick access to big data enables your analysts to swiftly trace the paths of cyber threats. Connecting more dots and building a complete picture faster leads to more efficient investigations and a quicker resolution of security incidents.



Threat Hunting: Armed with the ability to sift through massive amounts of data swiftly, your team can proactively hunt for early signs of hidden threats that might otherwise fall through the cracks. This proactive stance allows you to stay ahead of attackers, identifying and mitigating risks before they can gain a foothold.

Where to start? Here are some questions to think through as you develop your own SOC data platform.

Do you have the right data?

The first step to building an effective security data platform is ensuring that you have the right data to help reveal and understand threats, no matter where they originate.

Get Started with baseline visibility into the most critical actions and behaviors across your organization.

Endpoint	The frontline of your cyber defense, capturing endpoint data from sources such as EDR provides insights into device-level activities, crucial for identifying anomalies and potential breaches.
Network	Network security logs provide a panoramic view of the battlefield, helping to spot unusual patterns and potential threats.
Authentication	Authentication logs from your enterprise directory, identity systems, and VPNs offer valuable clues about who accesses what, when, and from where, a key aspect in uncovering unauthorized access and tracing malicious activity to a user or account.
Threat Intelligence Feeds	Staying ahead means knowing the enemy; integrating threat intelligence feeds keeps you updated on emerging threats and TTPs (Tactics, Techniques, and Procedures), so you know what to be looking for.

Go Deeper by introducing telemetry from applications and services that attackers target most.

Command line logs	A goldmine for forensics, these logs reveal the exact commands executed, shedding light on any hands-on-keyboard activity.
Access logs	Access logs track user activities and access patterns within your systems.
Cloud infrastructure	Cloud-based cyber attacks continue to be on the rise. Monitoring cloud environments ensures visibility across your expanded attack surface.
API and Application logs	These are the pulse points of your applications, offering insights into how applications are used and potentially abused.

Add Context with these high-volume data sources that capture who, what, and when.

DNS	The internet's phonebook, DNS logs, can reveal a lot about the websites and domains your network interacts with, a common vector for cyber threats.
DHCP	Tracking IP address allocations via DHCP logs are essential in tracing network attacks that originate from employee laptops, as well as helping detect rogue devices.
Netflow	Keeping track of the rivers of data flow through your network is crucial for understanding traffic patterns and spotting data exfiltration attempts.

Can you use it effectively?

Having the world's deepest data lake won't help you if your team can't access the information they need in time to act. Here are some questions to ask to ensure your SOC data platform is well-tuned for optimal defense.

Retention Are you retaining data for long enough?	Investigating a stealthy, entrenched threat or doing retrospective threat hunting means having 6-12 months of historical data, at minimum.
Storage costs Are you shedding data to save money?	Organizations must balance between data retention and cost. Too often, expensive storage solutions drive security teams to drop high-volume, low-fidelity logs, leaving visibility gaps that compromise security.
Bandwidth Are you throttling data when under duress?	In the face of high traffic or DoS attacks, some systems force the need to throttle data collection at the moment when it's most important.
Accessibility Can your users access the data without special training?	Security analysts don't generally come with PhDs in data science. It's important that your team can access and interpret data without weeks of training in complex query languages.
Performance Can analysts extract data in a reasonable amount of time?	Time is of the essence in cyber defense. A query that takes minutes (or hours!) to run gives the advantage of time back to your adversary. Your data platform should enable swift data extraction and real-time insights.
Access Control Can you prevent unauthorized access?	Security data can include sensitive information. Roles-based access control ensures that analysts only see the information they need, which is particularly important in multi-tenant environments.
Extensibility Can new sources be added easily?	Consider the effort required to onboarding new sources of security data into your platform, including structured and unstructured data.

Building or choosing the right data platform for your SOC is not just a technical challenge; it's also a strategic imperative. With the complexities and the ever-changing threat landscape, a comprehensive, well-integrated data platform allows you to focus on what matters most - safeguarding your organization.

SentinelOne's Singularity Data Lake empowers businesses to centralize and transform data for cost-effective, high-performance security and log analytics—bringing SIEM, Extended Detection Response (XDR), and Log Analytics solutions together as one.

Singularity Data Lake

[LEARN MORE](#)

Innovative. Trusted. Recognized.

FROST & SULLIVAN

Growth Index Leader of the Frost™ Radar:
Extended Detection and Response, 2023

MITRE ENGENUITY

Record-breaking ATT&CK Evaluation Results

- 100% Protection. 100% Detection.
- Top Analytic Coverage, 4 Years Running
- 100% Real-time with Zero Delays

Gartner Peer Insights

95% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity



TEVORA
PCI DSS Attestation
HIPAA Attestation



SE Labs
BEST Innovator
WINNER 2021



About SentinelOne

SentinelOne is a global leader in AI-powered security. SentinelOne's Singularity™ Platform detects, prevents, and responds to cyber attacks at machine speed, empowering organizations to secure endpoints, cloud, and identities with speed, accuracy, and simplicity.

sentinelone.com

sales@sentinelone.com

+ 1 855 868 3733