10 SIEM Questions Outcomes Navigator Helps You Answer

Want to know if your SIEM is detecting what matters?

Use this checklist to map coverage, identify gaps, and take action with Outcomes Navigator.

Not all data is equally valuable—and not all detections are equal. Outcomes Navigator helps you map log sources to MITRE ATT&CK® techniques and core detection use cases, giving you clear answers on what's covered, what's missing, and how to improve.

Use this checklist to explore 10 essential questions every smart security operations center (SOC) leader should ask when evaluating a SIEM—and how Outcomes Navigator helps you detect true threats with greater clarity and control.

1. **Solution Delivery and Data Storage**
   - ☐ Confirm the platform supports flexible, cloud-native deployment and data residency options.
   - ☐ Ensure your organization retains full control of its data.
   - ☐ Use Outcomes Navigator to map log sources directly to detection rules, use cases, and the ATT&CK framework, so you know your data supports outcomes, not just storage.

2. **Data Protection**
   - ☐ Require end-to-end encryption in transit and at rest (TLS, SSL, encrypted API).
   - ☐ Confirm SOC 2 Type II certification.
   - ☐ Use Outcomes Navigator to validate that protected data is contributing to real detection, not just retention.

3. **Scalability**
   - ☐ Choose a platform that scales without introducing complexity or cost overhead.
   - ☐ Look for prebuilt parsers and integrations to streamline ingestion.
   - ☐ Use Outcomes Navigator to identify which log sources support detections and which don't, so you can scale strategically and reduce waste.

4. **Data Collection and Transportation**
   - ☐ Assess whether the platform supports site, cloud, and context collectors.
   - ☐ Ensure it can securely ingest from modern hybrid environments
   - ☐ Use Outcomes Navigator to evaluate log source quality, parsing completeness, and contribution to use case coverage, helping you close critical gaps.

5. Network Impact

- ☐ Ensure collectors minimize impact through compression, batching, and buffering.
- ☐ Use Outcomes Navigator to determine whether high-volume logs are adding value or inflating costs, so you can prioritize effectively.

6. Upgrades and Quality Control

- ☐ Look for CI/CD delivery with beta programs, code testing, and pen testing.

7. Supported Security Technologies

- ☐ Look for a platform that brings together core security operations capabilities like log management, behavioral analytics, case management, automation, and response in one integrated experience
- ☐ Make sure analysts can access correlated data, timelines, and context from a single location to reduce manual effort and accelerate investigations.
- ☐ Evaluate whether the platform includes AI or intelligent guidance to assist with triage, investigation, or prioritization.
- ☐ Use Outcomes Navigator to map detections to use cases and ATT&CK techniques, identify gaps, and get prioritized recommendations to strengthen your overall detection posture.

8. Pricing Model

- ☐ Select a consumption-based model that aligns cost with value.
- ☐ Use Outcomes Navigator to focus spend on high-value data sources and optimize parsing, so you get the most from your license.

9. Solution Uptime

- ☐ Require 99.5%+ SLA and 24/7 operational support.
- ☐ Use Outcomes Navigator to get continuous insight into active detection posture, ensuring uptime translates to outcomes, not just data flow.

10. Data Ownership

- ☐ Confirm you retain full data access after your contract ends.
- ☐ Look for a 30-day grace period and Professional Services for offboarding or migration.
- ☐ Use Outcomes Navigator's coverage reports to inform future strategy and retain institutional knowledge, regardless of vendor changes.

Asking the right questions today helps ensure your security operations are focused, measurable, and ready to adapt.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at www.exabeam.com →