Coverage Analyzer

Identify coverage gaps that slow detection and response

Security teams deal with a constant influx of new attack techniques, expanding environments, and a growing mix of tools. Even well-resourced teams often struggle to answer a basic question: How effective is your detection coverage today?

As you add new data sources, deploy new capabilities, or grow your environment, it becomes harder to see where meaningful gaps exist. Tool inventories and log sources vary by team, and static assessments rarely give you enough detail to act. Without precise insight, planning becomes guesswork and real issues remain hidden.

Coverage Analyzer: A Current View of Your Detection Effectiveness

Coverage Analyzer gives you a current, data-driven understanding of your detection coverage. Delivered through an expert-led workshop, it analyzes your environment's data sources, tools, and operational processes. You walk away with a detailed view of your strengths, gaps, and the steps that will help your team improve.

It draws from a deep intelligence library that includes:

- Support for nearly 300 vendors and 600 products
- Close to 6,000 parser configurations to interpret diverse logs
- Full Exabeam detection content, including behavioral analytics and threat models aligned to real attack activity

How Coverage Analyzer Works

Your workshop begins with a straightforward discussion about your environment:

- **Data sources:** Identity, endpoint, network, cloud, and application logs
- **Security product inventory:** Vendors, features, and detection areas
- **SOC deployment information:** How your team manages detection, investigation, and response

Coverage Analyzer evaluates this information and produces a detailed report that highlights detection coverage, areas of risk, and recommended actions. You get practical guidance you can put to work right away.

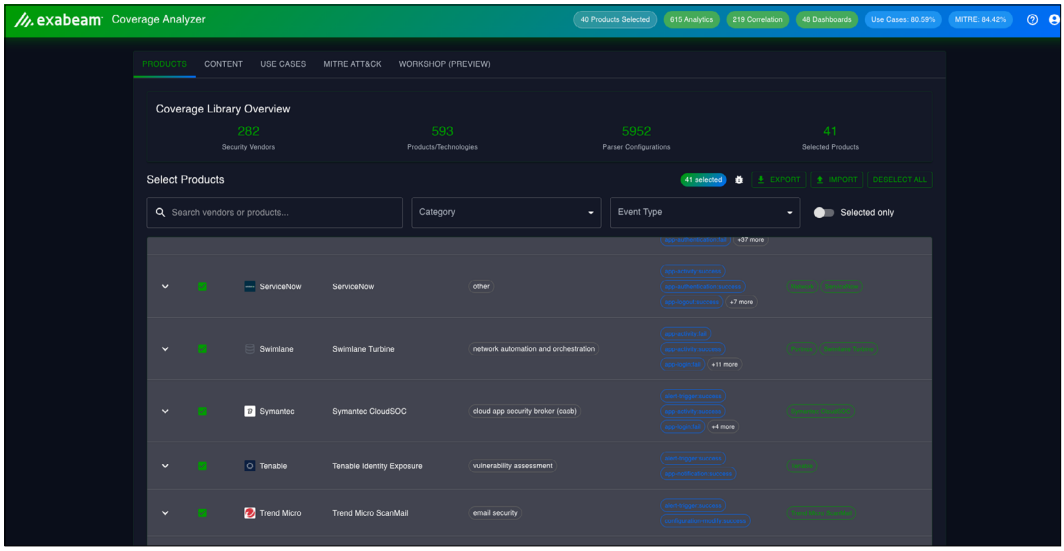

Figure 1.

The coverage library includes hundreds of vendors and products that you can easily select to match your current environment.

What You Gain

Coverage Analyzer gives you practical, outcomes-driven insights that help you make informed decisions about your program.

Pinpoint Coverage Gaps

Find the specific weaknesses that limit your ability to detect high-impact threats. Replace assumptions with measurable results you can act on.

Evaluate Detection Strength

See how well your environment detects 24 common use cases, including insider threats, compromised accounts, and lateral movement.

MITRE ATT&CK® Technique Mapping

Understand how your current tools and data sources align to hundreds of ATT&CK techniques and where you need stronger visibility.

Improve Investment Decisions

Identify overlap, missing visibility, and areas where configuration updates or new data sources will have the greatest impact.

Strengthen Strategic Planning

Use objective data to prioritize roadmap items, shape operational goals, and communicate changes to executive teams.

Simplify Reporting

Share quantitative findings that help stakeholders understand risk and the impact of planned improvements.

Plan for Future Data Needs

Test “what-if” scenarios so you can see how adding, removing, or adjusting data sources influences detection coverage.

How Teams Use Coverage Analyzer

You can apply the results to a wide range of operational and strategic initiatives.

- **Security posture assessments:** Validate how well your detections perform today.
- **Budget justification:** Show the measurable impact of new investments or configuration changes.
- **M&A due diligence:** Understand the detection maturity of an acquisition target early in integration.
- **Compliance readiness:** Demonstrate proactive work to reduce risk.
- **Program maturation:** Identify priority areas that strengthen detection and response.
- **Vendor consolidation:** Evaluate the actual value and coverage each tool provides.

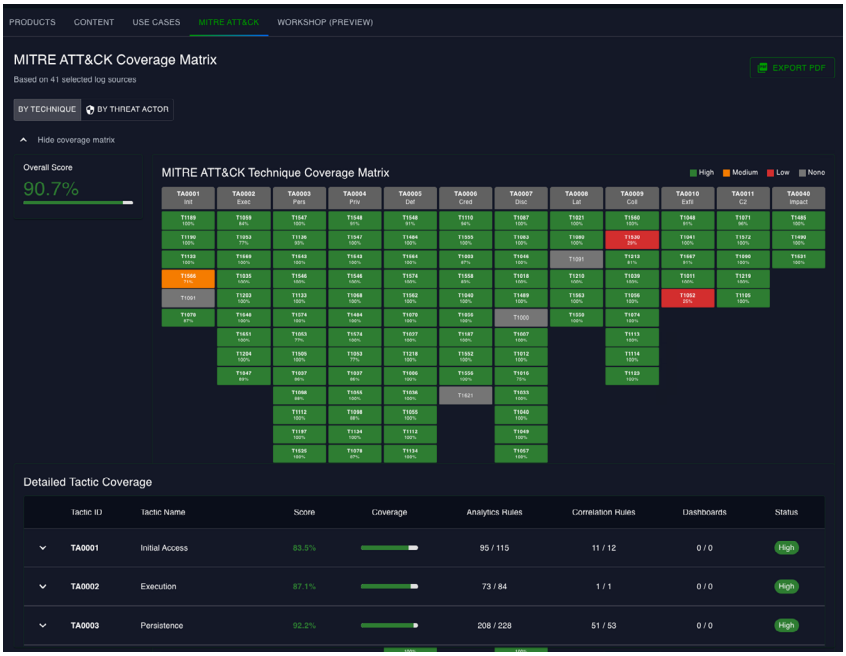

Figure 2.

The MITRE ATT&CK coverage matrix helps you understand technique- and threat actor-level coverage, including your overall score and detailed tactic results.

Why Exabeam

Exabeam helps teams detect, investigate, and respond to threats with behavioral analytics, dynamic risk scoring, automation, and open platform flexibility. Coverage Analyzer reflects this approach. It brings together:

- Deep experience understanding user and entity behavior
- A broad intelligence library aligned to ATT&CK
- An open, vendor-agnostic methodology that evaluates your environment as it is today
- Expert-guided workshops that turn complex data into practical steps

You gain a strategic partner focused on helping your team operate at a higher level.

Next Steps

If you're ready to get a precise, data-driven view of your detection coverage, schedule a complimentary Coverage Analyzer workshop. Your Exabeam account team can help you get started.

About Exabeam

Exabeam is the leader in behavior intelligence for the agentic enterprise. As organizations deploy digital workers and confront machine-speed adversaries, Exabeam delivers flexible, industry-proven solutions for insider threat coverage of humans and agents and faster, more accurate threat detection, investigation, and response (TDIR).

exabeam™

Learn more at
www.exabeam.com →