A Strategic Framework for Selecting Your Cloud-Native SIEM

10 Critical Factors for Modern Security Operations

Migrating from a self-hosted security information and event management (SIEM) to a cloud-native platform is a strategic move for modern security operations, offering faster deployment, lower overhead, and continuous innovation. However, choosing the right vendor is critical to success. This white paper is an essential guide for security leaders, architects, and analysts evaluating cloud-native SIEM solutions.

The document details 10 critical factors for a thorough vendor evaluation. It covers key technical capabilities, from effortless data ingestion and integration to precise, analytics-driven threat detection and streamlined incident response. It also highlights the importance of intelligent data normalization for powerful search and clear mapping to security frameworks like MITRE ATT&CK®.

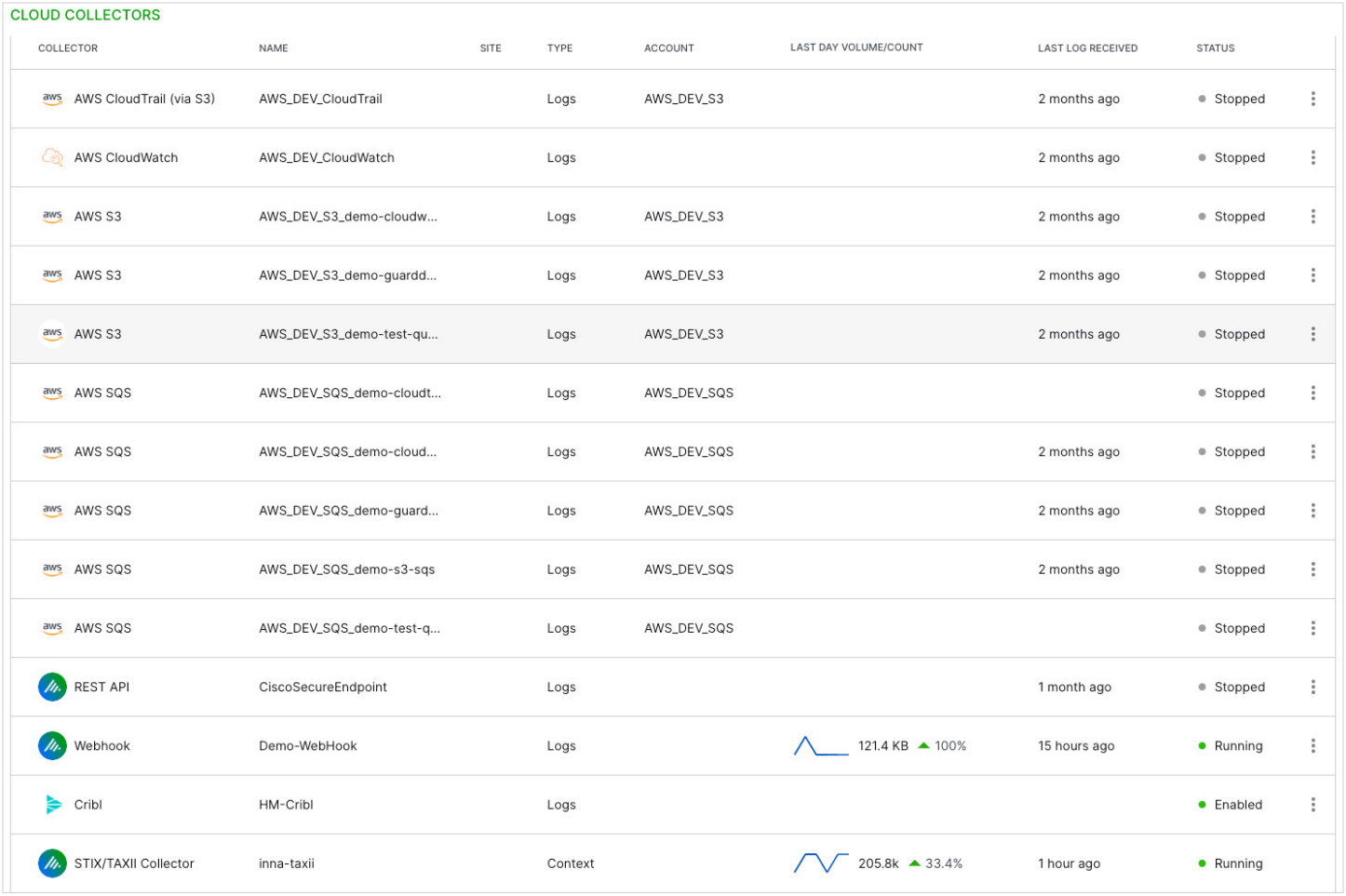
Beyond product features, the guide examines crucial vendor attributes like platform architecture, scalability, data security, and the provider's long-term vision and support structure. Complete with a detailed buyer's checklist, this paper equips readers with acomprehensive framework to confidently select a cloud-native SIEM that strengthens their security posture and drives operational efficiency.

The Advantages of a Cloud-Native SIEM Approach

While some security teams still manage self-hosted SIEM systems, many organizations now strategically shift to cloud-native SIEM platforms. A cloud-native SIEM offers significant advantages:

- Rapid deployment delivers faster time to insight.
- Security analysts and engineers focus on threat hunting and response.
- Operational complexity is minimal.
- Access to advanced security techniques fully uses cloud computing resources.
- New features and updates deploy continuously, without complex upgrade cycles.

The effectiveness of a cloud-native SIEM depends on the vendor's capabilities and cultural fit. Here are 10 critical factors to consider when evaluating cloud-native SIEM vendors.



CLOUD COLLECTORS

COLLECTOR	NAME	SITE	TYPE	ACCOUNT	LAST DAY VOLUME/COUNT	LAST LOG RECEIVED	STATUS
AWS CloudTrail (via S3)	AWS_DEV_CloudTrail		Logs	AWS_DEV_S3		2 months ago	Stopped
AWS CloudWatch	AWS_DEV_CloudWatch		Logs			2 months ago	Stopped
AWS S3	AWS_DEV_S3_demo-cloudw...		Logs	AWS_DEV_S3		2 months ago	Stopped
AWS S3	AWS_DEV_S3_demo-guardd...		Logs	AWS_DEV_S3		2 months ago	Stopped
AWS S3	AWS_DEV_S3_demo-test-qu...		Logs	AWS_DEV_S3		2 months ago	Stopped
AWS SQS	AWS_DEV_SQS_demo-cloudt...		Logs	AWS_DEV_SQS			Stopped
AWS SQS	AWS_DEV_SQS_demo-cloud...		Logs	AWS_DEV_SQS		2 months ago	Stopped
AWS SQS	AWS_DEV_SQS_demo-guard...		Logs	AWS_DEV_SQS		2 months ago	Stopped
AWS SQS	AWS_DEV_SQS_demo-s3-sqs		Logs	AWS_DEV_SQS		2 months ago	Stopped
AWS SQS	AWS_DEV_SQS_demo-test-q...		Logs	AWS_DEV_SQS			Stopped
REST API	CiscoSecureEndpoint		Logs			1 month ago	Stopped
Webhook	Demo-WebHook		Logs		121.4 KB ▲ 100%	15 hours ago	Running
Cribl	HM-Cribl		Logs				Enabled
STIX/TAXII Collector	inna-taxii		Context		205.8k ▲ 33.4%	1 hour ago	Running

Figure 1. Exabeam provides an extensive library of prebuilt connectors and parsers to ensure seamless data ingestion from your entire technology stack.

Success Factor 1: Effortless Data Ingestion and Integrations

Effective SIEM relies on comprehensive access to logs and security data from all your environments, both on-premises and cloud. Evaluate your prospective cloud-native SIEM's data ingestion capabilities for robustness and ease of use. Prioritize vendors with established partnerships and prebuilt integrations for your existing security tools. Ensure the vendor supports diverse ingestion techniques, including cloud collectors, AI agents, and API and webhook integrations. Additionally, look for user-friendly mechanisms to create custom data parsing policies when needed.

Strategic Takeaway for Leaders: Comprehensive data ingestion is the foundation for total visibility across your entire digital footprint. This directly impacts your ability to assess and manage enterprise-wide risk.

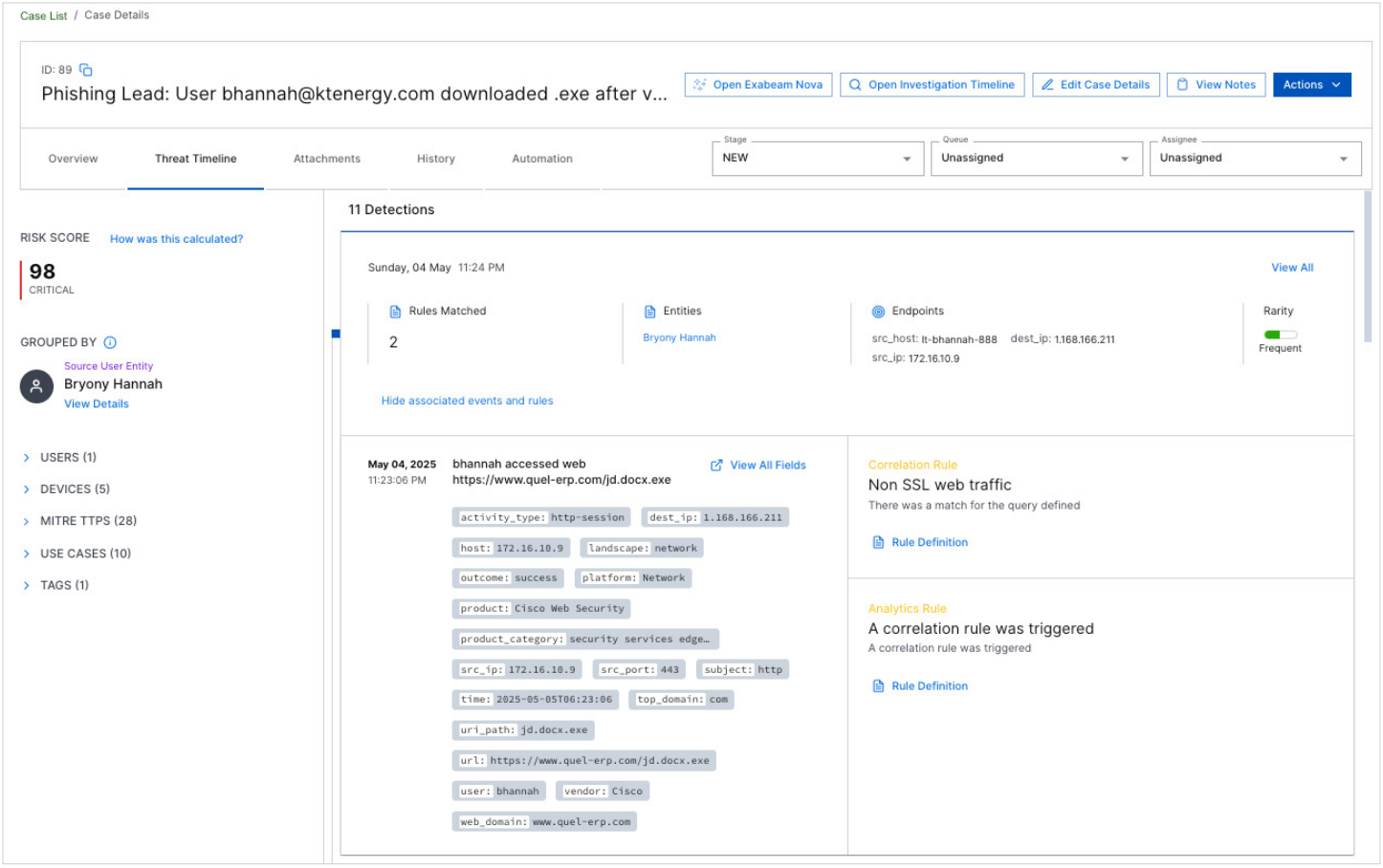


Figure 2. A user's Threat Timeline automatically reconstructs the story of an attack. This example shows a high-risk score generated after a user downloaded an .exe file as part of a potential phishing attack.

Success Factor 2: Precise Threat Detection and Adaptive Flexibility

A cloud-native SIEM's primary function is to detect security threats comprehensively, accurately, and efficiently. Challenge vendors to demonstrate the effectiveness of their threat detection techniques. Understand how they prevent visibility gaps, minimize false positive alerts, and avoid false negatives. Focus on how the solution intelligently correlates disparate data points. Sophisticated native detection methods and dynamic risk scoring should integrate with the flexibility to customize detection rules for your organization's specific needs.

Strategic Takeaway for Leaders: The quality of threat detection directly impacts business risk and team efficiency. Advanced, adaptable detection minimizes false negatives (missed threats) and reduces the false positive noise that leads to analyst burnout, allowing your team to focus on the prioritize and respond to credible threats.

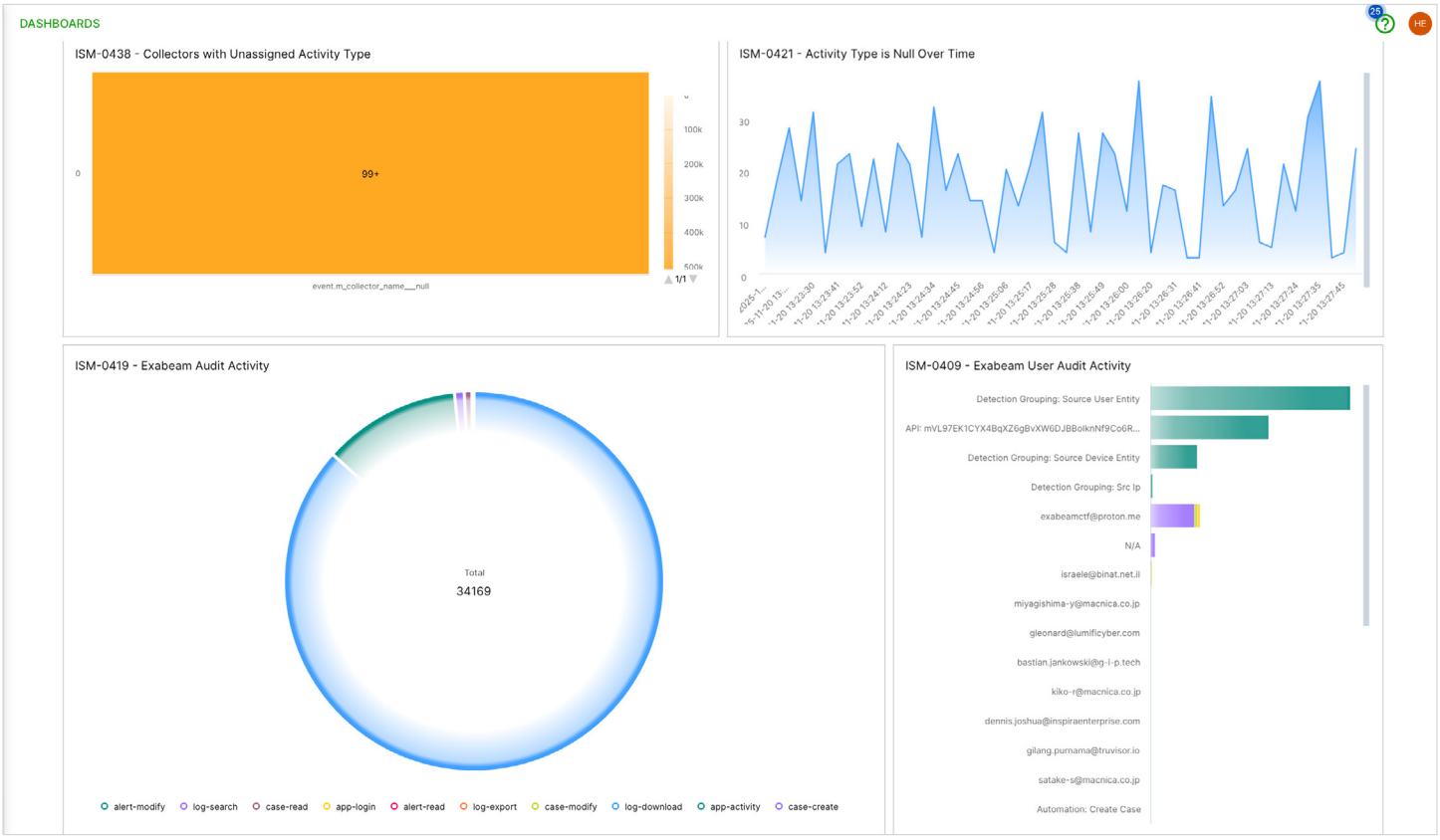


Figure 3. Customizable dashboards provide a comprehensive, top-level view of your security posture. A variety of widgets for tracking notable users, assets, and event trends helps security leaders make data-informed decisions and communicate risk.

Success Factor 3: Robust Analytics and Reporting

Beyond incident response, your cloud-native SIEM platform's data and insights drive your overall security strategy and threat hunting. This requires powerful, user-friendly analytics and reporting. An effective cloud-native SIEM includes dashboards that offer a top-level view of your security posture, along with flexible interfaces that integrate with search functionality. Evaluate the flexibility and customizability of dashboards and the data visualization techniques available for individual widgets.

Strategic Takeaway for Leaders: Advanced analytics and reporting are how you translate security data into business intelligence. This is your tool for communicating risk, demonstrating program ROI to the board, and making data-driven budget decisions.

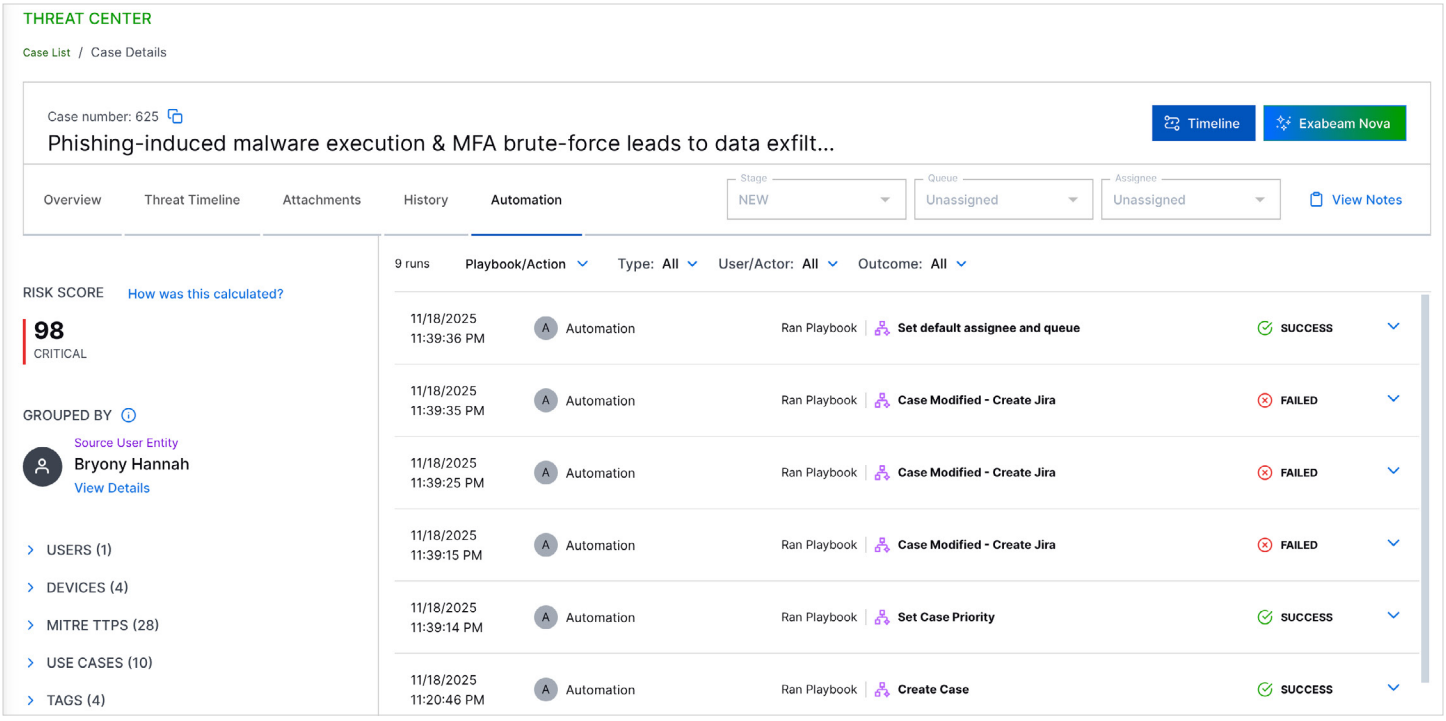


Figure 4. A unified platform for incident response streamlines investigations. This view combines case management with an interactive playbook that guides analysts through response tasks, such as isolating an endpoint or disabling a user, directly from the case.

Success Factor 4: Streamlined Incident Response Workflows

A cloud-native SIEM should combine threat detection with integrated tools for managing the response process. This creates an advanced security operations model where security analysts and incident responders swiftly respond, contain, and recover from incidents. A systematic approach with clear prioritization and communication among stakeholders is crucial. Effective and user-friendly capabilities accelerate new security personnel onboarding and prevent analyst burnout.

Strategic Takeaway for Leaders: Integrated response workflows are critical for reducing mean time to respond (MTTR) and minimizing the business impact of a breach. A streamlined process also combats analyst burnout and improves talent retention in a competitive market.

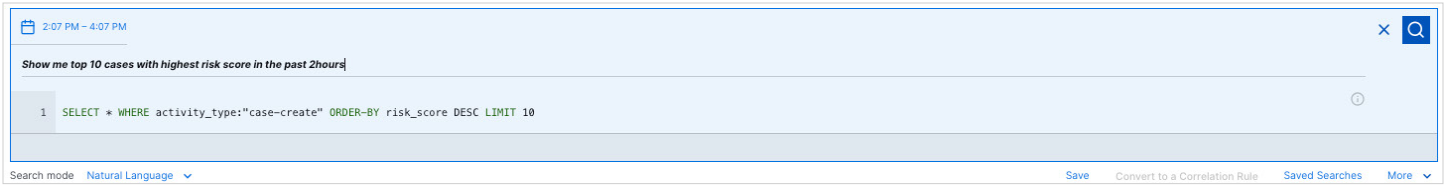


Figure 5. Natural Language Search makes it easy for analysts of all skill levels to find answers. Simply type a question, and Exabeam automatically translates it into an Exabeam Query Language (EQL) query to find the relevant data.

Success Factor 5: Intelligent Data Normalization, Enrichment, and Search

A cloud-native SIEM's effectiveness depends on extracting meaningful insights from large volumes of raw security event data. Evaluate the techniques your prospective SIEM vendor uses to normalize and enrich ingested data. Scrutinize how effectively the vendor automates bringing diverse data types into a consistent format, extracting and organizing meaningful

metadata, and enabling comprehensive search. Search capabilities should support basic and sophisticated queries, including compound operators, separators, and regular expressions. Look for analyst convenience features such as assisted search wizards, saved searches, search history, and auto-refresh.

Strategic Takeaway for Leaders: Investing in a platform that automates data normalization and simplifies search empowers your entire team, not just a few highly specialized analysts. This broadens your team's capabilities and accelerates investigation, improving overall operational efficiency.

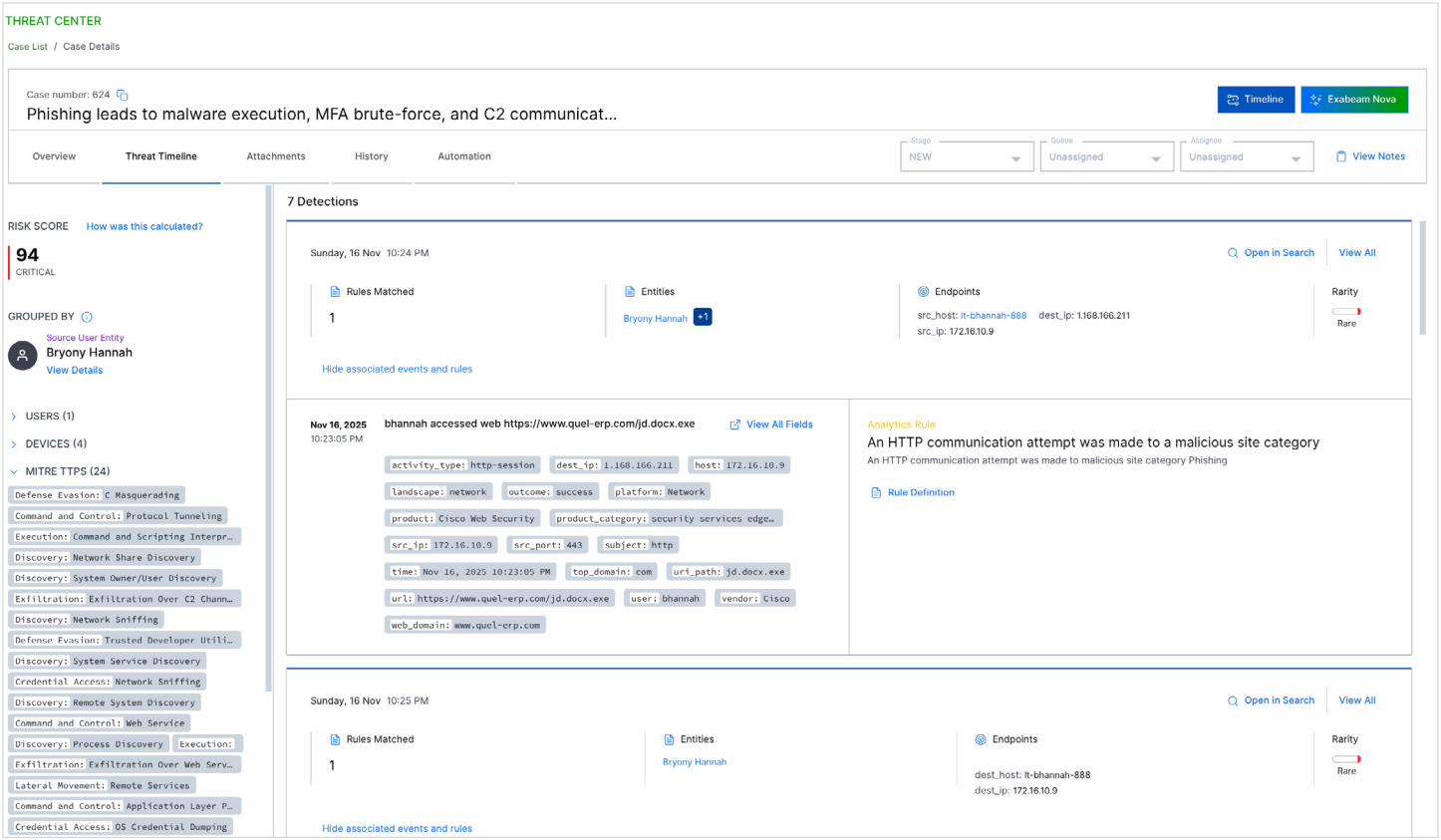


Figure 6. Automatically map detected threats to industry-standard frameworks. Exabeam enriches investigations by highlighting the specific ATT&CK tactics, techniques, and procedures (TTPs) associated with an incident, providing valuable context for analysts and security leaders.

Success Factor 6: Clear Security Framework Mappings

Mapping security operations practices to industry frameworks like ATT&CK can be complex and time-consuming. A cloud-native SIEM vendor simplifies and accelerates this process by providing native modules for specific cybersecurity frameworks and best practices. Explore the vendor's capabilities in this area and seek relevant case studies in your industry for proof points of real-world success.

Strategic Takeaway for Leaders: Native framework mapping provides a clear, defensible path to maturing your security program and demonstrating compliance. It operationalizes best practices like ATT&CK, saving significant time and resources on manual correlation and reporting.

Success Factor 7: Expert Support and Services

A cloud-based SIEM platform reduces the burden on in-house teams for deployment, customization, and operation compared to traditional on-premises software. However, effective support and services from your vendor remain crucial. Instead of relying on your SIEM vendor for administrative tasks like platform deployments, maintenance, and upgrades, you can engage their specialized expertise for higher-value activities. While self-sufficiency is a goal, a cloud-native SIEM vendor with strong support and professional services accelerates time to value and continuously maximizes your investment.

Strategic Takeaway for Leaders: View your vendor as a strategic partner, not a supplier. Expert services should focus on accelerating your time-to-value and maximizing the long-term ROI of your investment, freeing your internal resources for high-impact security work.

Success Factor 8: Vendor Vision and Future Innovation

Security leaders navigate complex decisions when selecting strategic vendors. While large vendors offer stability, they often move slower than startups. Startups introduce new ideas but can pose uncertainties regarding product maturity and long-term viability. An ideal cloud-native SIEM vendor balances these extremes: they are established with mature product capabilities and financial independence, yet nimble enough to innovate rapidly. Consider the benefits of a pure-play security vendor versus a company offering SIEM as part of a broader portfolio. Vendors with a core focus on SIEM invest deeply in product usability and feature innovation.

Strategic Takeaway for Leaders: Selecting a SIEM is a long-term commitment. A vendor's financial stability, focus, and clear innovation roadmap are leading indicators of a healthy partnership that will reduce the risk of your investment and ensure the platform evolves with your future needs.

Success Factor 9: Secure Data Storage and Compliance

Organizations considering a cloud-native SIEM often express concerns about data storage and security. A key consideration is how effectively your sensitive security data is segmented and secured within a shared cloud environment. Additionally, consider data residency requirements that dictate where specific data types must be stored. Your cloud-native SIEM should also adhere to data retention policies relevant to your industry and geography. Challenge prospective vendors to demonstrate infrastructure, policies, and flexibility that meet your organization's needs in these critical areas.

Strategic Takeaway for Leaders: How a vendor handles data storage, security, and residency is a direct reflection of their ability to support your governance, risk, and compliance (GRC) posture. This is a foundational trust and security requirement for any cloud partnership.

Success Factor 10: Platform Architecture, Resilience, and Scalability

The continuous collection and analysis of vast amounts of data presents a significant challenge in security operations. While a SIEM platform might perform well in a demo, its enterprise-scale performance and scalability can differ substantially. Critically assess your cloud-native SIEM vendor's architectural design and operational practices. Ensure they have a proven track record of scaling to meet the needs of organizations like yours. This evaluation must include factors like platform uptime and performance, especially security event data processing throughput.

Strategic Takeaway for Leaders: A resilient and scalable architecture ensures your security investment can support future business growth, not hinder it. This is a critical factor for managing total cost of ownership (TCO) and de-risking future technology needs.

Your Path to a Stronger Security Posture

Deploying a cloud-native SIEM transforms your risk posture by simplifying your security tool footprint and providing continuous access to the latest innovations. Operating a critical component of your security stack in the cloud demands significant trust in your vendor. Partnering with a vendor that cohesively integrates these elements ensures you:

- Respond efficiently and effectively to emerging security threats.
- Gain meaningful insights from your SIEM quickly.
- Address your unique requirements and regulatory needs.
- Meet critical scalability needs as your organization grows and evolves.

Buyer's Checklist for Your Cloud-Native SIEM

Ease of Data Ingestion and Integrations

What to Look For:

- Native data integrations
- Multiple data ingestion methods, including cloud collectors, Exabeam Nova agents, and API/webhook integrations
- Flexible and intuitive custom parsing

Questions to Ask:

- How many of my existing data sources does your platform support natively?
- What techniques do you use to ingest customer data?
- Walk me through the process for creating a custom parsing rule.

Precise Threat Detection and Adaptive Flexibility

What to Look For:

- Systematic approach to preventing visibility gaps
- Well-defined techniques for minimizing false positives
- User-friendly custom detection rules

Questions to Ask:

- How do you ensure critical security events are detected?
- What techniques and tuning are used to avoid false positive alerts?
- Describe your approach for creating custom detection rules.

Robust Analytics and Reporting

What to Look For:

- Information-rich dashboards
- Customizable dashboard widgets
- Direct integration between dashboards and search

Questions to Ask:

- Show me examples of dashboards that provide a top-level view of risk posture.
- What types of data visualizations does your platform support?
- How can I drill down and search if something in a dashboard interests me?

Streamlined Incident Response Workflows

What to Look For:

- Incident prioritization and tracking integrated with SIEM
- Customizable response workflows

Questions to Ask:

- Does your platform include incident prioritization and tracking?
- Demonstrate the process for tracking and reporting on incidents.

Intelligent Data Normalization, Enrichment, and Search

What to Look For:

- Capability to bring disparate data sources into a common format
- Metadata generation and enrichment
- Sophisticated search capabilities

Questions to Ask:

- What types of processing do you apply to raw log data?
- Can I perform complex searches using compound operations, separators, and regular expressions?
- Is data normalized for easy searching across various log sources?
- Is it easy to search across days, weeks, or months of logs?
- What features guide users through complex searches?

Clear Security Framework Mappings

What to Look For:

- Native frameworks for ATT&CK and other security best practices
- Success stories in your industry

Questions to Ask:

- Do your detection techniques map to industry frameworks or best practices?
- How much effort is required to configure your product to support my compliance needs?
- Which other companies in my industry are using your product?

Expert Support and Services

What to Look For:

- Well-defined onboarding services to accelerate time to value
- Ongoing support and customer success functions

Questions to Ask:

- How long does it take for a typical customer to be fully operational with your product?
- What support can I expect from your team for integrating data sources and configuring dashboards?
- How does support engagement work after the initial deployment?

Vendor Vision and Future Innovation

What to Look For:

- Financial independence
- Strong focus on cybersecurity or SIEM
- Proven track record of delivering updates and innovations

Questions to Ask:

- What percentage of your revenue comes from your SIEM offerings?
- What updates have you released for your products over the last 12 months?

Secure Data Storage and Compliance

What to Look For:

- Data retention policies that match your organization's requirements
- Ability to meet data residency requirements

Questions to Ask:

- How long do you store customer data?
- Where is customer data stored?
- Can data storage be limited to specific regions?

Platform Architecture, Resilience, and Scalability

What to Look For:

- Deployments of similar size or larger
- Mature capacity planning processes
- Strong historical uptime track record

Questions to Ask:

- How many locations and users does your biggest deployment serve?
- Does the cloud SIEM have high availability and disaster recovery capabilities?
- How do you ensure performance remains high as usage and data volumes grow?
- What is your infrastructure uptime percentage?

Achieve Modern Security Operations With Exabeam

Choosing a cloud-native SIEM using a strategic framework is the first step toward modernizing your security operations. The next is selecting a partner whose platform was purpose-built to excel across these critical factors.

The New-Scale Security Operations Platform directly answers the challenges outlined in this paper. We deliver a powerful security data foundation through broad data integration and a Common Information Model that makes searching fast and intuitive for your entire team.

Where Exabeam truly excels is in providing market-leading, analytics-driven threat detection. By using patented behavioral analytics and dynamic risk scoring, Exabeam detects complex threats—including insider threats and compromised credentials—that other tools miss, all while minimizing the noise from false positives.

This high-fidelity detection is seamlessly integrated into a unified threat detection, investigation, and response (TDIR) workflow within New-Scale SIEM. From automated timelines that reconstruct incidents to prebuilt playbooks that guide response, Exabeam empowers analysts to work more efficiently and reduce MTTR. The entire process is mapped to industry-standard frameworks like ATT&CK, helping you mature your security program and demonstrate compliance.

Built on a hyperscale, cloud-native architecture, the Exabeam platform is designed for the scale and speed your organization demands today and in the future.

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 →