



Unlock the Next Level of Threat Detection

**New-Scale Analytics delivers the foundation for a
rapidly evolving threat landscape**

Presenter Name | Title

Security Operations Challenges

Rule-based Threat Detection Alone Can't Keep Up

83%

of security professionals report alert fatigue, with teams overwhelmed by the volume of security alerts

64%

of SOC teams say manual processes slow down their response to threats

70%

of organizations struggle to scale their security operations as data volumes grow

56%

of analysts cite lack of context as the main reason for missed threats

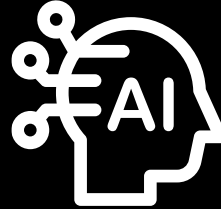
Why Exabeam?

Leading AI-Driven Security Operations



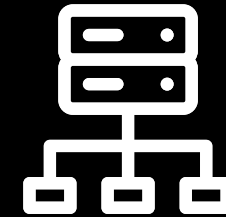
Industry-Leading Detection

Expose the threats that other tools miss. Support strategic use cases with guidance on how to improve. Meet your compliance objectives.



Faster, More Accurate TDIR

Reduce alert fatigue and accelerate your triage. GenAI-powered workflows speed analyst routines and up-level their skills.

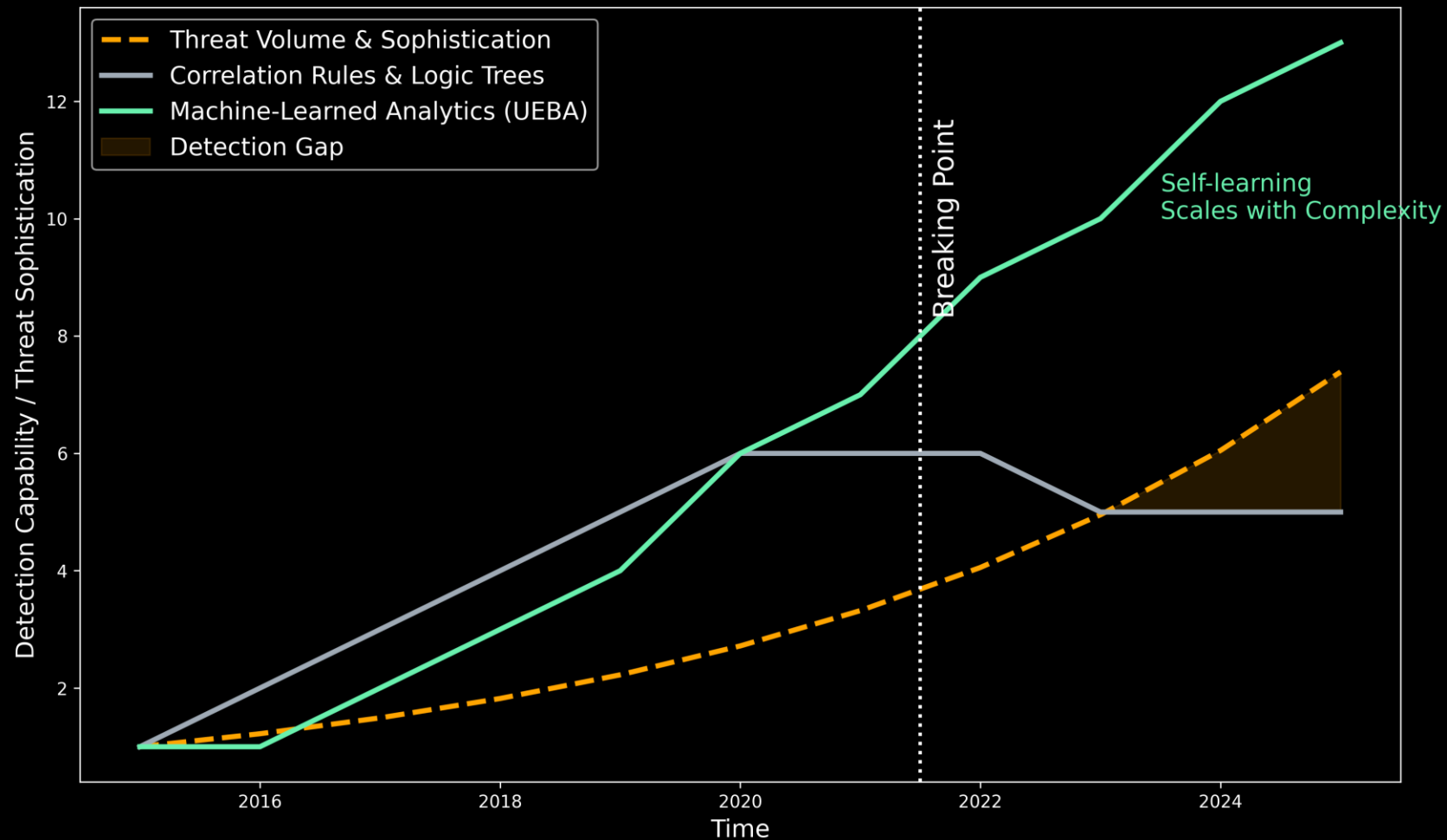


Rapid-Value, Unmatched Flexibility

Deploy a fully-featured SIEM with hundreds of integrations and the market's most flexible deployment options:
self-hosted, hybrid, or cloud-native.

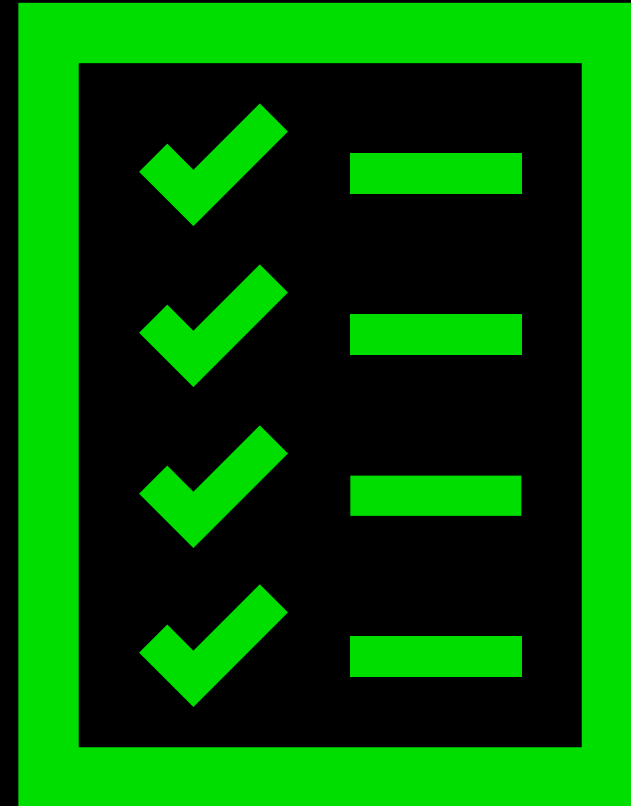
In 90% of real attacks, we see compromised credentials used, which can be very hard to detect and defend. We chose Exabeam because their technology effectively analyzes and baselines normal usage to quickly alert on a compromised user or credentials.” Sebastian Bittig SOC Leader for R-tec

The future of threat detection is machine-learned analytics



The Case for SIEM + UEBA – Closing the Detection Gap

- Detect unknown and insider threats that evade rule-based detection
- Reduce false positives and alert fatigue, focusing your team on the most credible, high-risk incidents
- Accelerate investigations and incident response with contextual, prioritized alerts
- Automate response actions based on risk scores and behavioral insights
- Protect against a wider range of threats, including account takeovers, data exfiltration, and privilege abuse

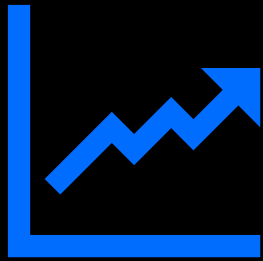


Exabeam with UEBA – Machine-learned behavioral analytics

	SIEM	New-Scale Analytics
Log Management	✓	✗
Compliance Reporting	✓	✗
Search & Query Capabilities	✓	✓
Rule-Based Correlation	✓	✓
Alert Centralization	✓	✓
Integrated AI Agent(s)	?	✓ Exabeam Nova consists of 6 coordinated AI agents
User and Entity Behavior Analytics	✗	✓ Baselines behavior across users/devices
Anomaly Detection	✗	✓ Automated machine-learning driven behavioral anomalies
Insider Threat Detection	✗	✓ Detects compromised accounts, malicious insiders
Unknown Threat Detection	✗	✓ Identifies threats without IOCs or rules
Risk Scoring (User/Device)	✗	✓ Multi-dimensional, contextual risk scoring
Automated Threat Timelines	✗	✓ Accelerates investigations
Incident Prioritization	✗	✓ Based on entity behavior and risk context

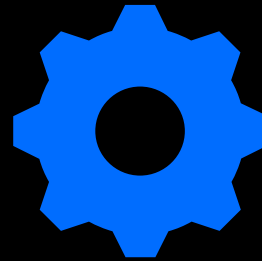
New-Scale Analytics

Built for What's Next



Scalability:

Handles today's data and tomorrow's growth



Performance:

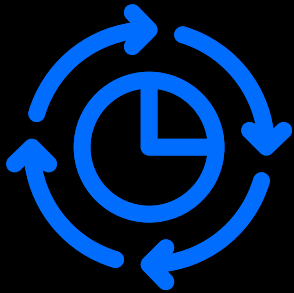
Near real-time detections



Stability:

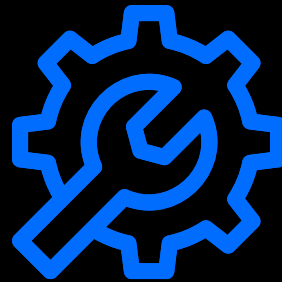
Platform reliability at scale

New-Scale Analytics Built for What's Next



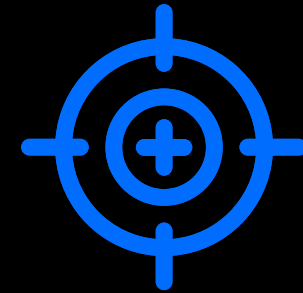
Analyst Efficiency

With Threat Center and
Exabeam Nova



Next-Gen Automation:

Cloud-native, event-driven, and
built for what's next, not stuck in
the past



Alert Reduction:

Stand out engine detection
accuracy and efficiency

Ready for tomorrow's demands.

New-Scale Platform

SKU Features Configuration

Core Components	Application	New-Scale SIEM	New-Scale Analytics	New-Scale Fusion
Collectors	Site Collectors	☐	☐	☐
	Cloud Collectors (Logs)	☐	☐	☐
	Cloud Collectors (Context)	☐	☐	☐
Security Management	Context Management	☐	☐	☐
	Log Stream (Parsing)	☐	☐	☐
	Log Stream (Enrichment)	☐	☐	☐
	Threat Detection Management (Correlation Rules)	☐	☐	☐
	Threat Detection Management (Analytics Rules)	☒	☐	☐
	Attack Surface Insights	☒	☐	☐
Platform Insights	Dashboards	☐	☐	☐
	Compliance	☐	☒	☐
	Outcomes Navigator	☐	☐	☐
	Service Health and Consumption	☐	☐	☐
Investigation	Threat Center	☐	☐	☐
	Search	☐	☐	☐
Automation	Automation Management	☐	☐	☐
	APIs	☐	☐	☐

Add-Ons	New - Scale SIEM	New - Scale Analytics	New - Scale Fusion
Long-Term Search	☒	☒	☒
Long-Term Storage	☒	☒	☒
Custom Dashboards	☒	☒	☒
Advanced Playbooks	☒	☒	☐
UEBA	☒	☐	☐
Crow dStrike Collector	☒	☒	☒
Advanced Automation	☒	☒	☒
Additional Correlation Rules	☒	☒	☒
NetMon	☒	☒	☒

☒ Add-on available

☒ Add-on not available

☐ Included as a standard feature

Additional applications optimized with New-Scale Analytics

Threat Center Unifies the New-Scale Analytics Architecture

Unified Workbench for Analysts

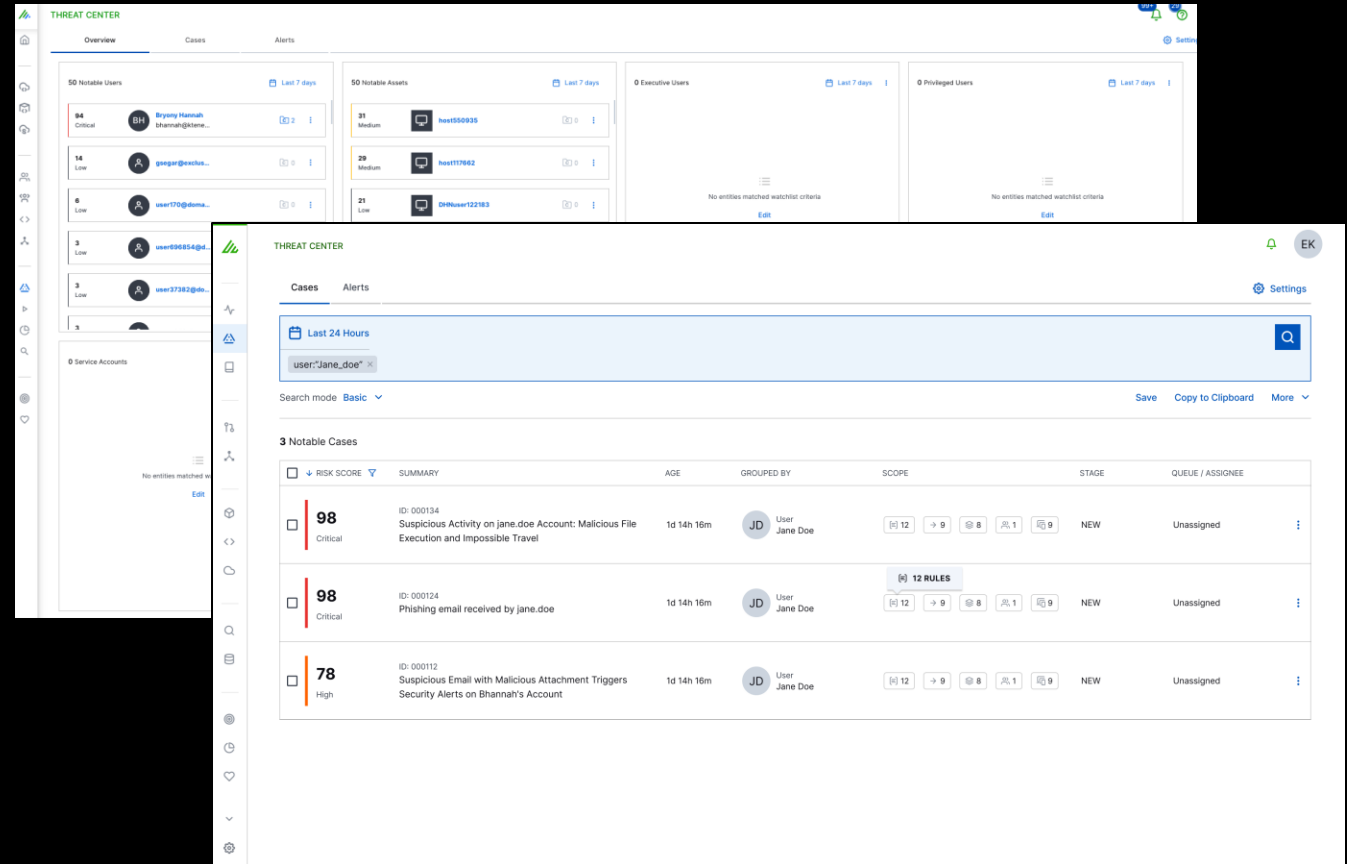
- Combines TDIR workflows into a single experience
- Improves analyst productivity

Intelligent Alert Grouping

- Recognizes that individual anomaly detections are not always useful in isolation
- Allows ML and static rules to intelligently group detections for improved threat triage

Exabeam Nova - Agentic AI Integration

- Investigation Agent - generates detailed case summaries and threat analyses to ensure a consistent response and help prioritize or deprioritize threats.
- Analyst Assistant Agent - gives analysts of all skill levels an expert assistant with access to all the case data
- Threat Scoring Agent - understands your environment and automatically surfaces the most security relevant events for analysis.



Attack Surface Insights for Faster Investigations

Adds Structure to Chaos

- Aggregates user and asset information to create easy to understand entities
- Entity can be user, device, file, endpoint, server, applications, and processes

Accelerated Investigations

- Unified entity profiles enables cross-profile behavioral analytics
- Analysts can pivot faster with linked context to other potential areas of concern

Expanded Context Sources

- Active Directory still available as a native context source
- Entra ID and Okta added as context source with more to follow (including custom context)

The screenshot displays the 'ATTACK SURFACE INSIGHTS' application interface. At the top, there are tabs for 'Users' and 'Devices'. A search bar contains the query 'full_name: "bryony hannah"'. Below the search bar, a dropdown menu lists several email addresses associated with the search: 'bhannah - juniper vpn', 'bhannah - microsoft 365', 'bhannah@exaverse', 'bhannah@exaverse.online', and 'bhannah@itrecruiter.com'. The search mode is set to 'Basic'. Below the search results, a '1 selected' button is visible, along with 'View Details' and 'Edit' links. A 'User Entity' section shows a profile for 'Bryony Hannah' with a circular icon containing the letters 'BR'. To the right of the profile, there are buttons for 'AND' and 'AND NOT'. Below the profile, a list of context sources is shown, including 'bhannah - ivanti pulse secure', 'bhannah@ktenergy.com', 'bhannah - microsoft 365', 'bhannah@exaverse', 'bhannah - juniper vpn', 'bhannah@itrecruiter.com', and 'bhannah@exaverse.online'. A '+7' icon indicates additional context sources are available.

Automated, Multi-layer Risk Scoring

Dynamic Risk Scoring

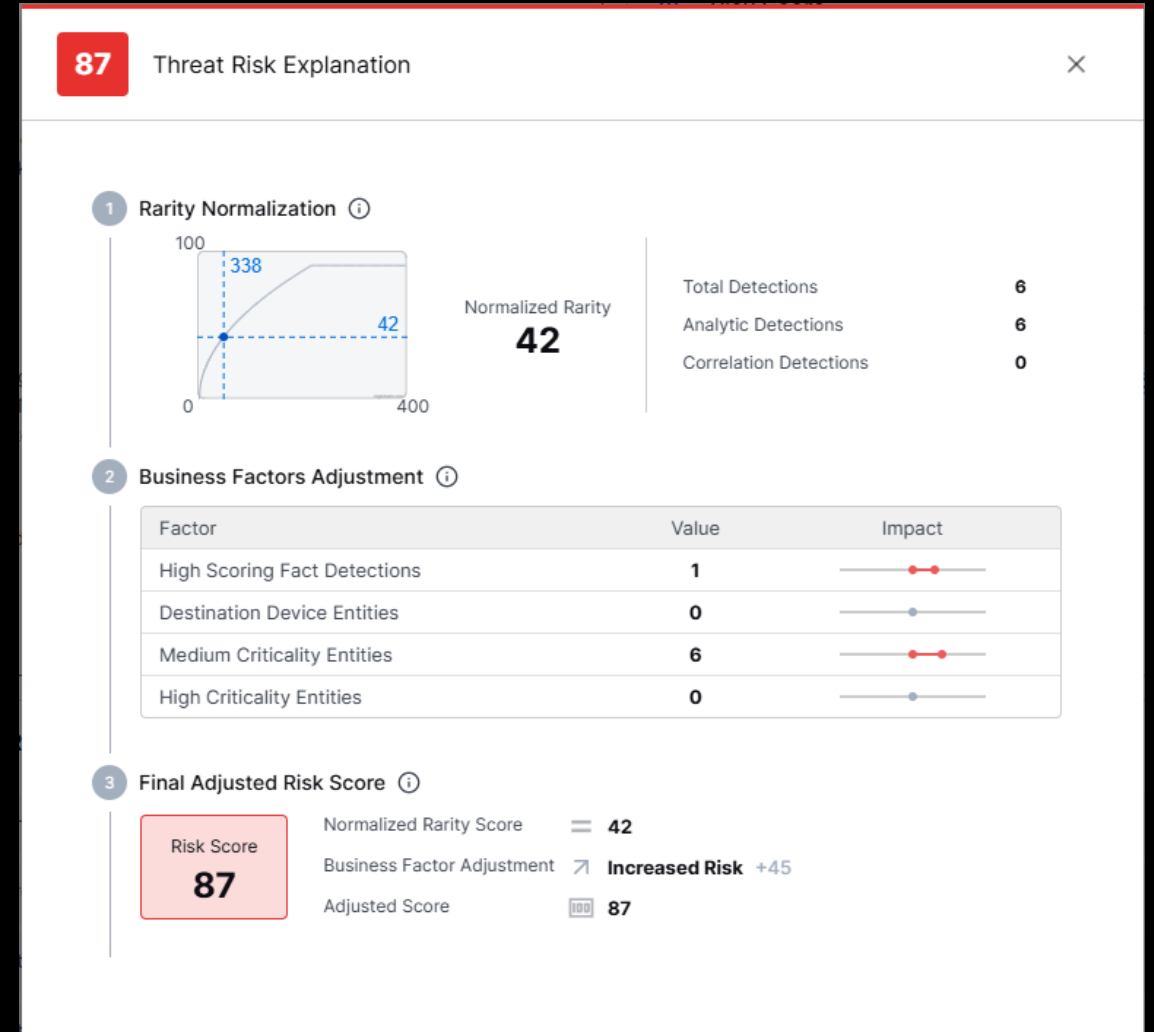
- Risk scores for detections generated using machine-learning
- Drastically reduce the amount of tuning and manual intervention – human bias!

Risk Normalization

- Combined risk scores for all detections in a case, normalized to a 0-100 score
- Bounded scores makes contextualizing the criticality of a case much easier

Business Factors Adjustment

- Only Exabeam includes factors outside of rarity scoring that impact the severity of the threat – Who, what, why, when
- Give SOC teams the ability to influence case risk scores through Attack Surface Insights



The Benefits of SOAR Without the Complexity

Automation Management Simplifies and Accelerates SOC Automation

Open API Standard Compatibility

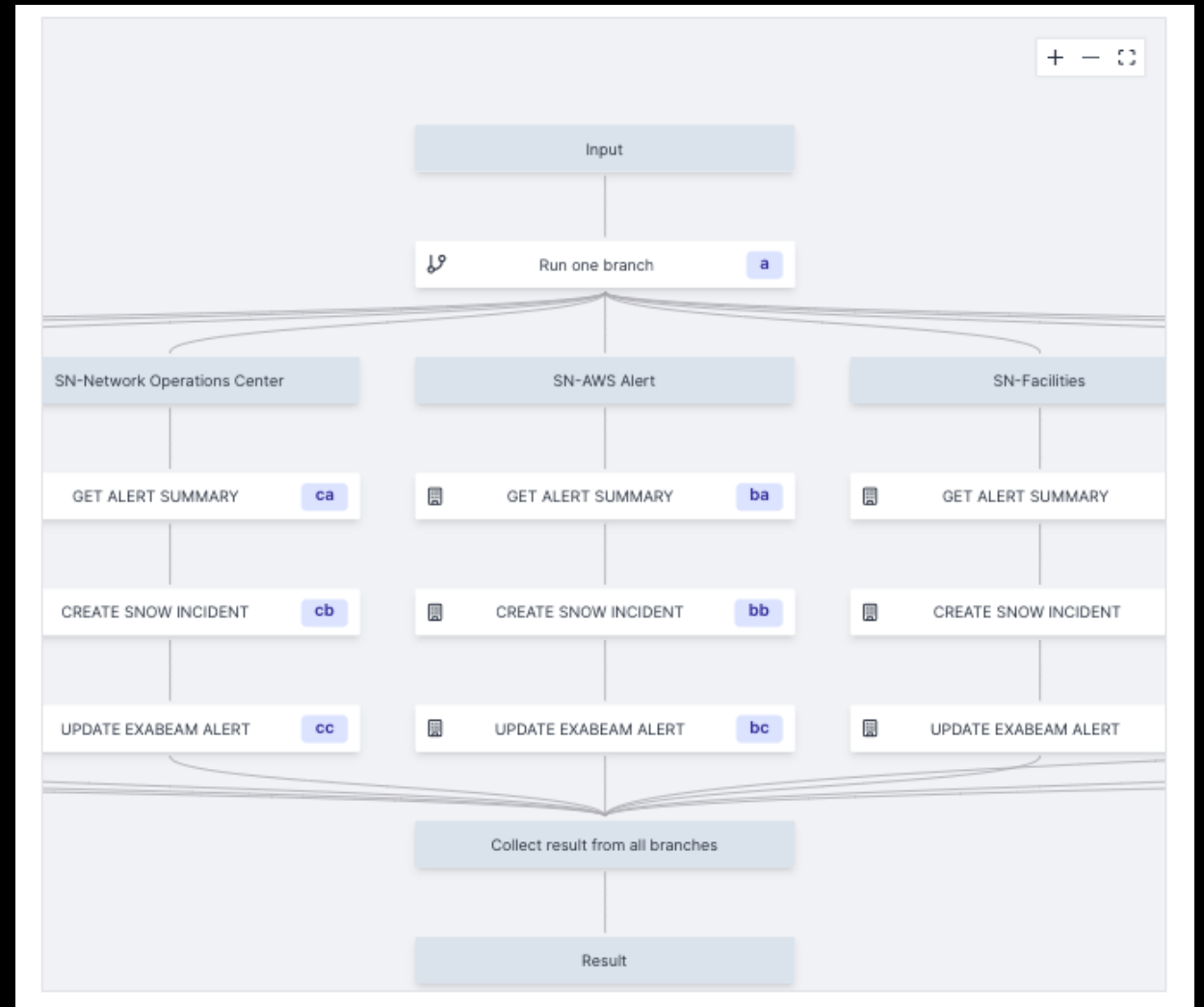
- Industry-first native integration - Access to 1000's of pre-built services across hundreds of vendors for faster, easier automation
- Leverage SOAR capability without the need for dedicated, expensive coding resources

Intuitive Playbook Builder

- Click and drag independent services into complex workflows
- Drive integration across products and systems to speed up analyst workflow

Streamlined Incident Response

- Enrich cases with better context for faster triage driving down MTTD/R
- Trigger playbooks from Threat Center, when seconds matter in incident response





Key Takeaways

- ✓ Works with ANY SIEM
- ✓ Next-gen threat detection capability
- ✓ Fully-integrated multi-agent capabilities at no additional cost
- ✓ Existing apps benefit from improved data
- ✓ Access to new apps and features

Demo



Thank You



Appendix



Elevator Pitch – CISOs

Strategic-Focused Pitch

- Reducing organizational risk
- Maximizing ROI on security investments
- Demonstrating measurable improvements
- Aligning security with business outcomes
- Ensuring defensible, audit-ready posture

New-Scale Analytics helps reduce risk by delivering **more accurate threat detection** and dramatically **fewer false positives**, so your team spends time on real issues—not the noise. Our platform adapts to your environment using **data-driven risk scoring**, eliminating the need for complex manual tuning or constant rule updates.

Most importantly, it translates that activity into **clear, measurable outcomes** through our Outcomes Navigator, mapping your coverage to the use cases that matter most. Our **transparent, explainable AI models** ensure every risk score and detection is **traceable and defensible**—building trust in automation and supporting audit-ready reporting.

The result: a security investment that delivers **greater impact, strategic clarity, and board-ready visibility.**

Elevator Pitch – SOC Managers

Operational-Focused Pitch

- Reducing alert fatigue and false positives
- Improving SOC efficiency and consistency
- Minimizing manual tuning
- Clear visibility into coverage and effectiveness
- Supporting, scaling and automating analyst workflows

New-Scale Analytics equips your SOC to work faster and smarter by reducing alert noise through **time-based profiling** and **adaptive, behaviour-driven risk scoring**, no manual rule tuning required. Our platform surfaces **richer, more complex detections** from fewer alerts, giving analysts the clarity they need to act decisively.

With support for **automating key investigative and operational tasks**, teams can scale their efforts without burning out. And with **Outcomes Navigator**, you gain clear insight into how your coverage maps to top use cases and the **MITRE ATT&CK framework**, helping you prioritize where to strengthen next.

Elevator Pitch – Security Analysts

Execution-Focused Pitch

- Getting accurate, actionable alerts
- Minimizing time wasted on false positives
- Having clear, contextual information for investigations
- Tools that are intuitive and reduce repetitive tasks
- Focusing on real threats — not chasing noise

New-Scale Analytics helps you cut through the noise with **high-fidelity alerts** driven by **time-based profiling**, so you're not drowning in false positives. Its **adaptive learning** continuously adjusts risk based on actual user behavior, so you're focused on what's real, not what's misconfigured.

With **greater detection complexity**, multiple threat indicators are surfaced in one view, and **advanced contextual AI** provides the background you need to act fast - no guesswork, no digging. It's the kind of tool that gets out of your way and helps you get to the answer quicker.

Digging Deeper – New-Scale Analytics Advantages

Count-Based Profiling Advanced Analytics

Detection based on building histogram models of all datapoints for an event then alerting based on “abnormal” behaviour

- Storing Histograms is **hard**
 - Primary cause of platform stability concerns seen by support
- Configuring the rules is **hard**
 - Every custom detection needs to be completely defined in a complex JSON object
- Maintaining rule fidelity is **hard**
 - Detecting on “abnormal” leads to losing the wood for the trees, relying heavily on tuning

Time-Based Profiling New-Scale Analytics

Detections based on time. Was this the first time we’ve seen an event? Has it exceeded the anomaly threshold since it was last seen?

- **Easier** to store
 - No histograms to carry around makes the platform more performant
- **Easier** to configure
 - Individual features are simplistic and easy to create, combining to make complex detections
- **Easier** to detect
 - “First” historically more useful than “abnormal”, better fidelity