exabeam™

Too Late to the GenAI Party?

Transforming a Technology Enterprise at Scale

The Exabeam Executive Team

Chris O’Malley

Chief Executive Officer

David Rizzo

Chief Development Officer

Steve Wilson

Chief AI and Product Officer

Exabeam at a Glance

exabeam™

The Leading AI-Driven Security Operations Platform

CAPABILITIES

SIEM, UEBA, SOAR, Insider Threat, TDIR, Compliance

STABLE & SCALABLE

99.9% Platform Uptime

500+ TB Daily Peak Ingestion

INNOVATION

75 Cybersecurity patents, the majority are for AI

GLOBAL CUSTOMERS

3000+

RECOGNITION

14 years combined Gartner MQ leadership

MARKET IMPACT

22

Countries covering small, mid, and large enterprises

AI-Native Companies are Growing at Frightening Speed

Shopify – 6 years

Twilio – 5 years

Slack – 3 years

OpenAI – 2 years AI

Cursor – 1 year AI

Lovable – 6 months AI

Growth from $1M to $100M (fastest companies ever)

Be Amazon Not Sears

Be Netflix Not Blockbuster

How can an existing business thrive in an environment of AI-native predators?

Three Keys to Re-engineering a Business for the AI Age

No one said this would be easy

AI-Native Development

Change the Way You Build

Don’t Settle for Marginal Improvements

Tackle the Impossible Problems

AI-Native Products

Bolt-on AI Won’t Do

Agents not Chatbots

Work Back from the Objective

AI-Native Business

ChatGPT for Everyone Doesn’t Move the Needle

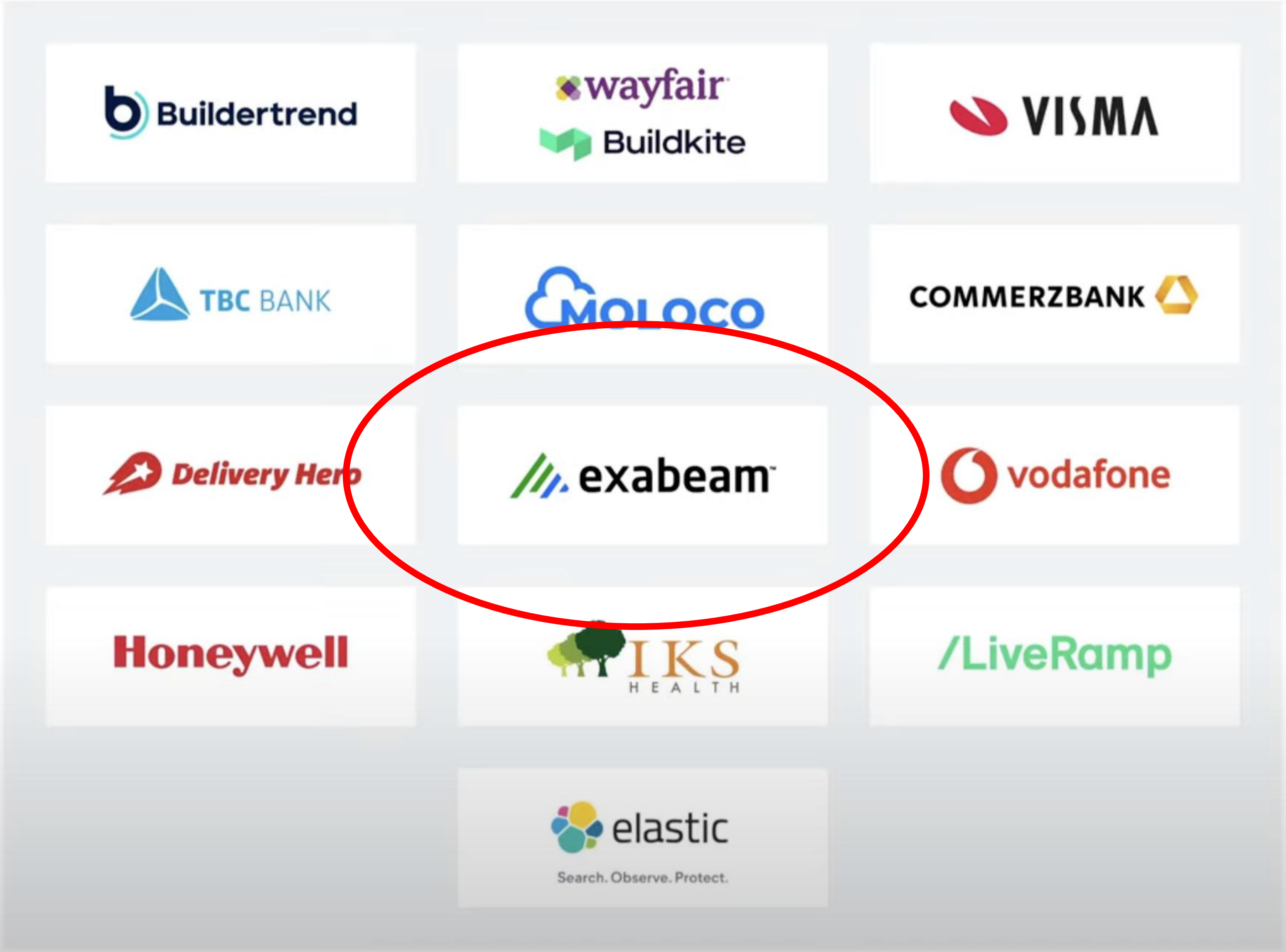
Find the hard problems and build the solution

Re-engineer business processes

AI-Native Development

Re-engine Your Engineering

2025 DORA Awards



Winner

exabeam™

Developer Productivity and Velocity

"We learned that **AI is most effective when it augments the skills of talented engineers**. By automating the tedious, repetitive tasks, AI freed up their developers to focus on strategic problem-solving and innovation."

Challenge

Need to accelerate feature velocity, reduce manual toil, and sustain elite DevOps performance while growing globally

Free up engineers from repetitive tasks, minimize deployment errors, and drive consistency in software quality

Solution

Modernize the development lifecycle through the integration of intelligent automation directly within CI/CD pipelines

Gemini powering 100% of code reviews and supporting deployment automation

Measurable Impact

- Lead Time for Changes: Decreased from 2 days to **8 hours**
- Mean Time to Recovery: Improved from 2 hours to **1 hour**
- Deployment Frequency: Maintained a high frequency of ~5 deployments per day with greater stability
- Change Failure Rate: Remained low, supported by AI-driven consistency checks and automated verification

Accelerate Development with AI Coding Tools

Accelerating Development with AI Coding Tools

Generate, refactor and explain complex code

Real-time code suggestions with IDE integration

CI/CD integration – trigger automated code & test generation

Learn from org-specific patterns and best practices

Higher code quality with fewer defects

Continuous improvement through feedback loops

Sure, you can build a new product, but can you radically improve one that’s 20 years old and drives $100M in revenue?

AI Empowers teams to safely modernize legacy code

Problems become Advantages

AI-Driven Code Refactoring
Modernizing Legacy Code

Automated Code Analysis – detect inefficiencies and technical debt

AI Refactoring Proposals – generate optimized, maintainable code

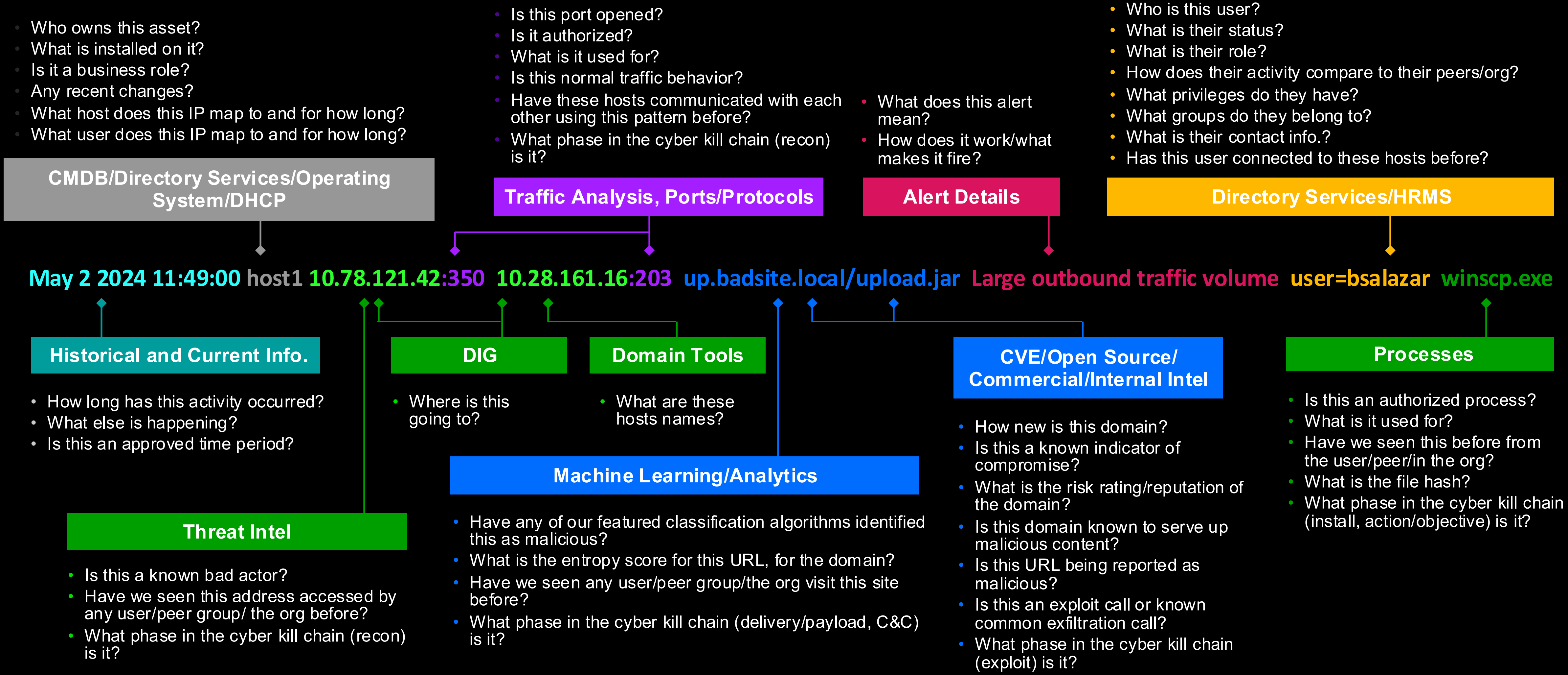
Predictive Stability Modeling – forecast impact of code changes

Continuous Performance Feedback - integrate into CI/CD pipelines

AI-Native Products

Upend Your Market

Find Your Biggest Problem – The Dark Corner You Don’t want to talk about….



- Who owns this asset?
- What is installed on it?
- Is it a business role?
- Any recent changes?
- What host does this IP map to and for how long?
- What user does this IP map to and for how long?

CMDB/Directory Services/Operating System/DHCP

- Is this port opened?
- Is it authorized?
- What is it used for?
- Is this normal traffic behavior?
- Have these hosts communicated with each other using this pattern before?
- What phase in the cyber kill chain (recon) is it?

Traffic Analysis, Ports/Protocols

- What does this alert mean?
- How does it work/what makes it fire?

Alert Details

- Who is this user?
- What is their status?
- What is their role?
- How does their activity compare to their peers/org?
- What privileges do they have?
- What groups do they belong to?
- What is their contact info.?
- Has this user connected to these hosts before?

Directory Services/HRMS

```
May 2 2024 11:49:00 host1 10.78.121.42:350  10.28.161.16:203  up.badsite.local/upload.jar  Large outbound traffic volume  user=bsalazar  winscp.exe
```

Historical and Current Info.

- How long has this activity occurred?
- What else is happening?
- Is this an approved time period?

DIG

- Where is this going to?

Domain Tools

- What are these hosts names?

Threat Intel

- Is this a known bad actor?
- Have we seen this address accessed by any user/peer group/ the org before?
- What phase in the cyber kill chain (recon) is it?

Machine Learning/Analytics

- Have any of our featured classification algorithms identified this as malicious?
- What is the entropy score for this URL, for the domain?
- Have we seen any user/peer group/the org visit this site before?
- What phase in the cyber kill chain (delivery/payload, C&C) is it?

CVE/Open Source/ Commercial/Internal Intel

- How new is this domain?
- Is this a known indicator of compromise?
- What is the risk rating/reputation of the domain?
- Is this domain known to serve up malicious content?
- Is this URL being reported as malicious?
- Is this an exploit call or known common exfiltration call?
- What phase in the cyber kill chain (exploit) is it?

Processes

- Is this an authorized process?
- What is it used for?
- Have we seen this before from the user/peer/in the org?
- What is the file hash?
- What phase in the cyber kill chain (install, action/objective) is it?

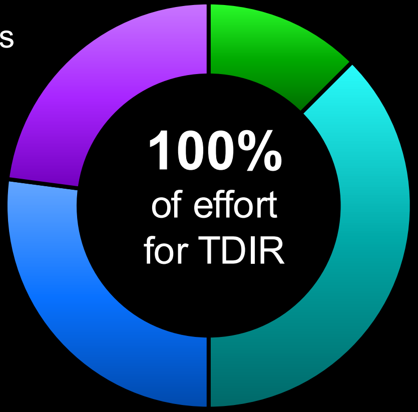
exabeam

10, 20, 30% Doesn't Move the Needle - Think Big!

Without Exabeam Nova

- ⊗ Manual Effort
- ⊗ Cumbersome collection
- ⊗ Too many false positives
- ⊗ Insufficient Triage
- ⊗ No time for thorough Investigation
- ⊗ Static playbooks

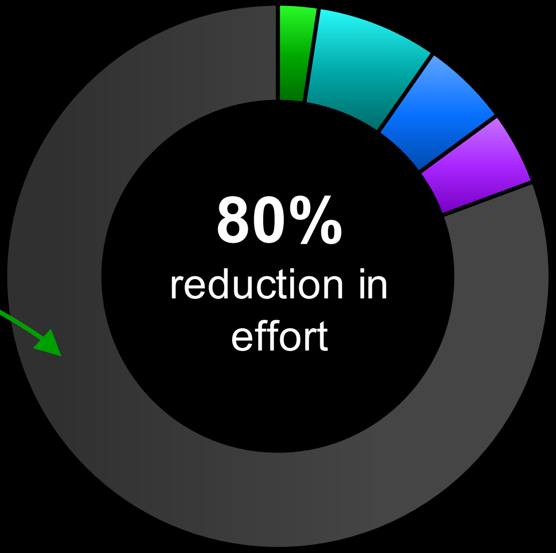
Collection → Detection (**12%** of effort) → Triage (**36%** of effort) → Investigation (**26%** of effort) → Response (**22%** of effort)



With Exabeam Nova AI

Improve Analyst Productivity By Up To 80%

- Save 3 hours per shift alert triage
  37.5% productivity increase
- Eliminate writing incident summaries
  50% of analyst effort erased
- Automated evidence collection & Investigation Summary
  26% analyst effort erased



Find an aging competitor with revenue. How long would it take you to rebuild their product with modern, AI-native approach?

AI-Native Business

Accelerate The Business

Broad-based Adoption

- Every employee can benefit from use of AI
- Random shadow AI/IT puts you at risk
- Curate your tools
  - Choose tools to solve specific problems
  - Evaluate cost and security (e.g. data management policy)
- Simple guidelines for users
  - Don’t scare them away with “prompt injection” and “hallucinations”
  - Do ensure they understand “they are responsible for content the create with AI tools”

Targeted Use-Cases

- Training people to use ChatGPT doesn’t move the needle
- Find problems where solving them delivers real ROI
- Invest in solving hard problems that impact the business
  - Writing better emails (meh?)
  - Responding to sales prospect questionnaires 100x faster (hey!)
  - Answering routine support questions (meh?)
  - Analyzing all support cases on the “new product” and find the “sharp edges” to fix first (hey!)
  - Internal NLP search of JIRA and Confluence (meh?)
  - Each department grooms and maintains critical data for the new knowledge-base (hey!)

The Help We’re Looking For

- What’s the “just enough AI” training recipe for a non-technical AI user?
  - Prompting
  - How does it work, without scaring people away?
  - Moving beyond “chatbot” use-cases
- Strategies for “internal” agent sharing inside an Enterprise

Thank You

exabeam™