Introducing
Exabeam

The Industry's Leading Platform for AI-Driven Security Operations

Max Klerkx | Channel Manager Nordics

Exabeam at a Glance

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

25 Cybersecurity patents, the majority are for AI

GLOBAL CUSTOMERS

620+

RECOGNITION

5x Leader of the Gartner MQ

IMPACT

>1,800 Behavioral rules & AI models for unparalleled detections

Exabeam leads in AI/ML in this Market

AI-DRIVEN SECURITY INTELLIGENCE FOR 10+ YEARS

Exabeam Analytics
AI/ML

Established Leader

- ✓ Pioneered anomaly detection via ML (UEBA)
- ✓ Threat detection and prioritization
- ✓ Near real-time across all data sources
- ✓ ML monitoring of log source health / volume
- ✓ Only viable solution to insider threats and compromised credentials

Exabeam Copilot
GenAI

New

- ✓ Conversational experience
- ✓ Powerful, natural language prompted search
- ✓ Threat explainers
- ✓ Faster threat hunting
- ✓ Easier on-boarding with less training

exabeam®

What are your top cybersecurity challenges?

1 **Industry-leading analytics**

2 **Security operations automations**

3 **Outcomes-based security solution**

4 **Integrates with your existing investments**

Detect high-risk threats from a sea of noise

Accelerate investigation and response

Map security data to strategic outcomes

Extract value from existing investments

exabeam®

What we learned from Lapsus$

Highly disruptive attacks don't always require highly sophisticated techniques
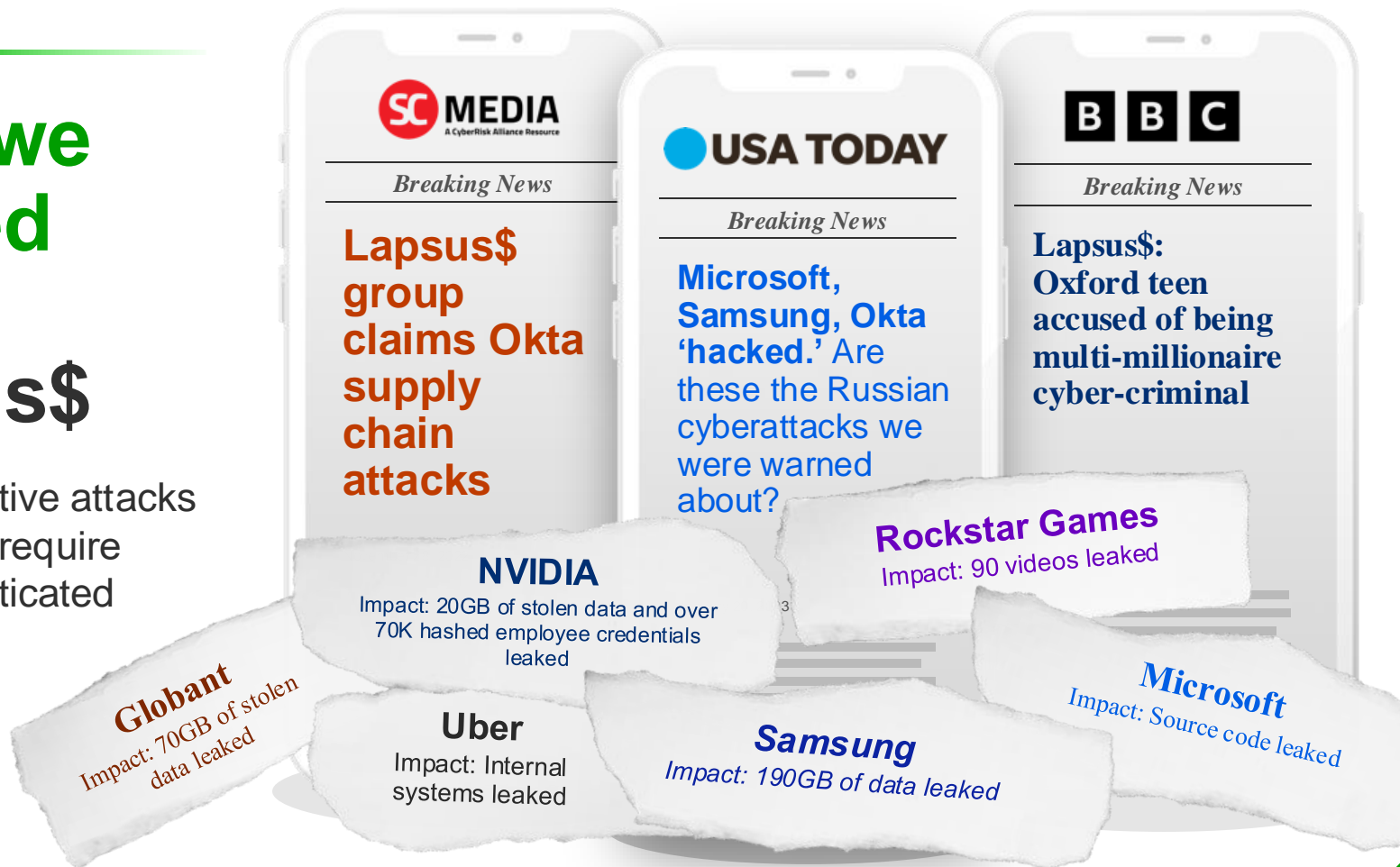
Lapsus$ group claims Okta supply chain attacks

USA TODAY

Breaking News

Microsoft, Samsung, Okta 'hacked.' Are these the Russian cyberattacks we were warned about?

BBC

Breaking News

Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal

Rockstar Games
Impact: 90 videos leaked

NVIDIA
Impact: 20GB of stolen data and over 70K hashed employee credentials leaked

Globant
Impact: 70GB of stolen data leaked

Uber
Impact: Internal systems leaked

Samsung
Impact: 190GB of data leaked

Microsoft
Impact: Source code leaked

exabeam
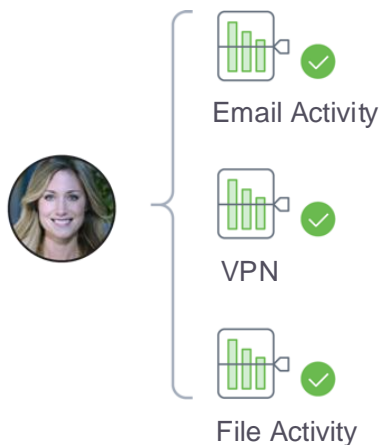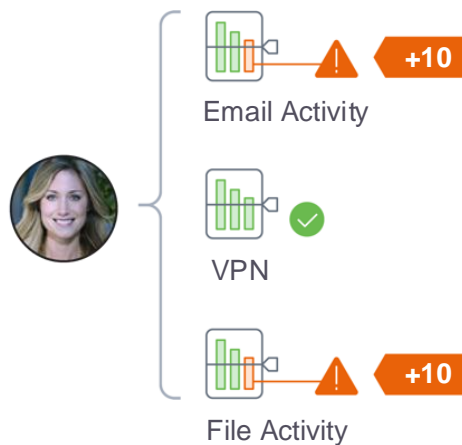
How different tools detect
a Lapsus$ attack

DLP
Detection

SIEM
Detection

EDR
Detection

Privilege
escalation via
custom
compiled tooling

EDR
Disabled

Mimikatz
executed

New admin
accounts
created

Lateral
movement to
cloud O365
environment

Email transport
rule to BCC
malicious
account on all
emails

Outbound
Emails
detected

First logon
event

RDP login
to "DC"

Next Gen
EDR
Detection

UEBA
Detection

SASE
Detection

Next Gen
DLP
Detection

exabeam®

Meeting you where you are

MODULAR PLATFORM

Augment

Using a SIEM / data lake, but need to augment or add Insider Threat capabilities with an advanced AI-Driven Security Operations Platform with continuous risk scoring and behavioral anomaly detection
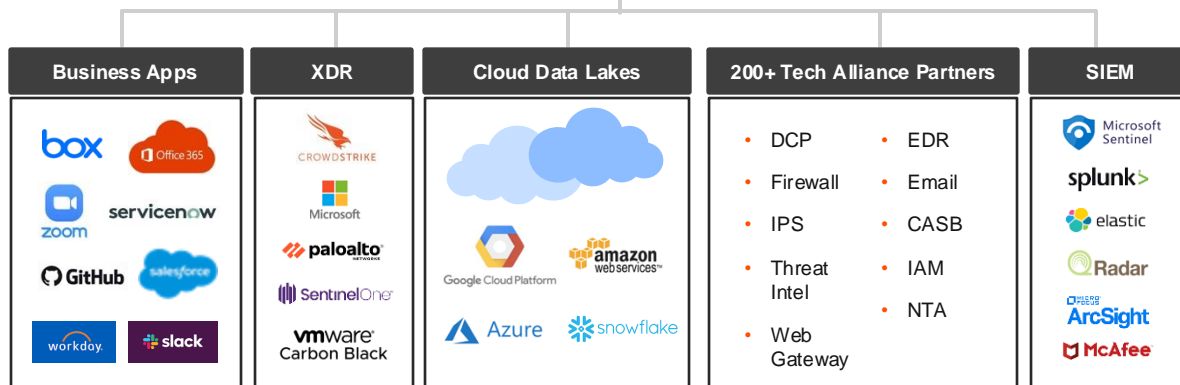
Full SIEM

Outgrown capabilities of your current SIEM or don't have a SIEM and need an AI-Driven Security Operations platform that includes SIEM, advanced analytics, and automation

exabeam®

Extend the value of your security investments

exabeam

Business Apps	XDR	Cloud Data Lakes	200+ Tech Alliance Partners	SIEM
box, Office 365, zoom, servicenow, GitHub, salesforce, workday, slack	CROWDSTRIKE, Microsoft, paloalto, SentinelOne, vmware Carbon Black	Google Cloud Platform, amazon web services, Azure, snowflake	• DCP • EDR • Firewall • Email • IPS • CASB • Threat Intel • IAM • NTA • Web Gateway	Microsoft Sentinel, splunk>, elastic, Radar, ArcSight, McAfee

Exabeam adds intelligence to any stack, any architecture

New efficiencies
Strengthen existing security stack with AI and automation for repeatable TDIR

New detections
UEBA analyzes data to deliver contextualized detections

Broader Insights
Consolidate security information to see analysis from the point of view of an alert, event, user or entity

Automated workflows
Uplevel security team's ability to learn fast and accomplish more

exabeam

Thank you
for your
time today