exabeam

СУЧАСНА ІНТЕЛЕКТУАЛЬНА СИСТЕМА БЕЗПЕКИ

Jan2018

Доповідач Сьомакін Микола

Про компанію Exabeam

Exabeam заснована в 2013 році компаніями Norwest Venture Partners, Aspect Ventures, Icon Ventures та інвестором Шломо Крамером.

Aspect VENTURES

ICON VENTURES

NORWEST VENTURE PARTNERS

Штаб-квартира компанії Exabeam розташована в Сан - Матео, штат Каліфорнія. Заснована професіоналами, що раніше працювали в Imperva, ArcSight та Sumo Logic.

IMPERVA

ArcSight

sumologic

exabeam

200+ розгортань у клієнтів, включаючи:

Проблеми управління безпекою

Чому SIEM не достатньо ефективний проти сучасних загроз

ПРОБЛЕМА ДАНИХ

- Генерування великої кількості даних
- Занадто дорого, щоб збирати і зберігати
- Неможливо підтримати звітність або аналіз

ПРОБЛЕМА ОБРОБКИ

- Не помічає атаки та бокові зміщення(lateral movemen)
- Шум від неефективних правил та сигнатур
- Не може самостійно об'єднувати події

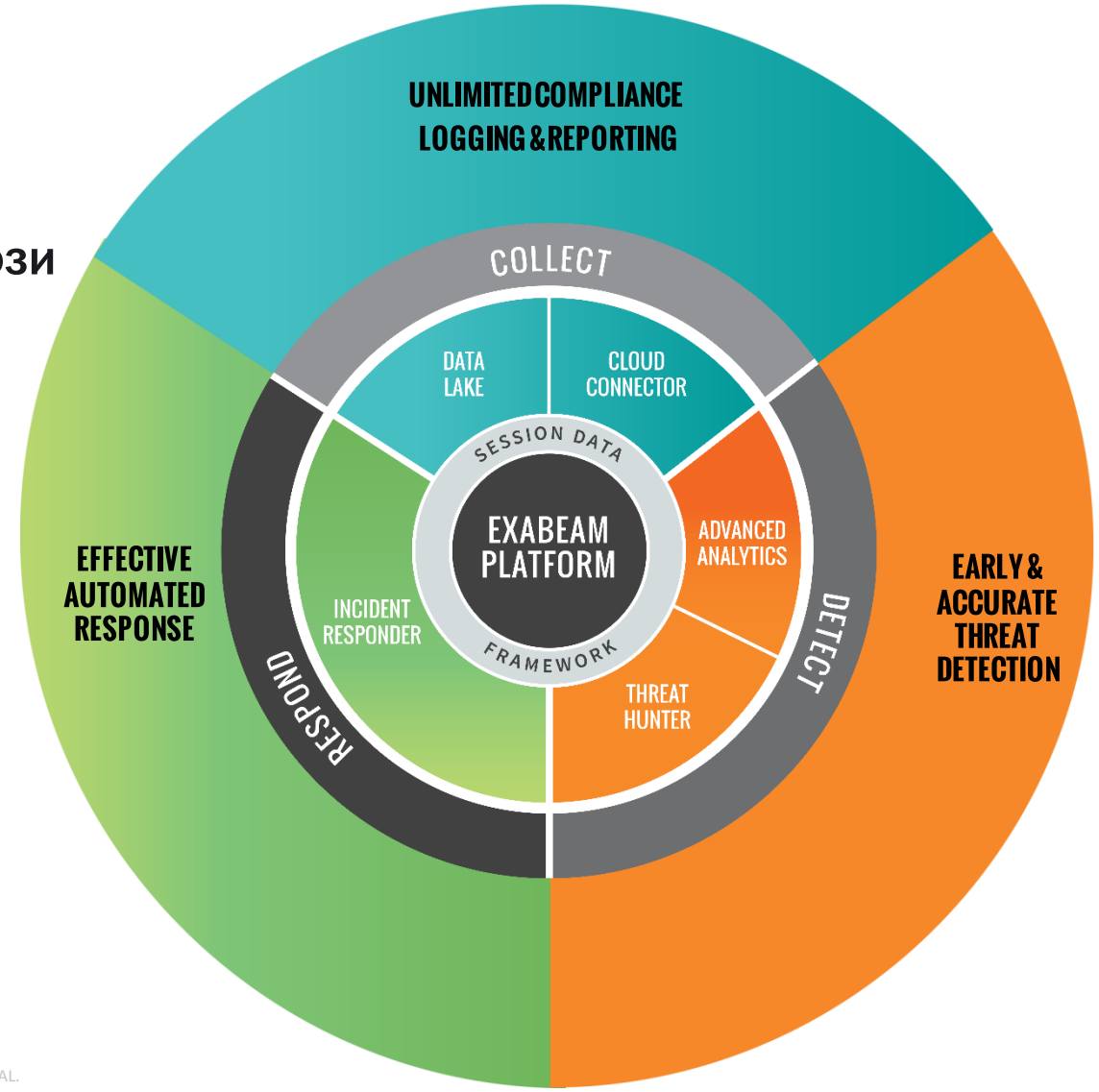
ПРОБЛЕМА ЕКСПЕРТИЗИ

- Надмірна кількість оповіщень
- Недостача кваліфікованого персоналу
- Невідповідна реакція

exabeam

Exabeam Security Intelligence Platform

Автоматизована платформа для **виявлення**, **аналізу** та **реакції** на сучасні загрози



exabeam

Головні сценарії клієнтів

COMPROMISED INSIDER

STOLEN CREDENTIALS
MALWARE/RANSOMWARE
PHISHING

92%

Зовнішні атаки, спрямовані на крадіжки облікових даних користувача

(Verizon 2016 Data Breach Report)

MALICIOUS INSIDER

INSIDER THREAT
DATA LOSS PREVENTION
DATA EXFILTRATION

60%

Атаки, пов'язані з навмисним зловживанням привілеями інсайдерами

(Verizon 2016 Data Breach Report)

INCIDENT RESPONSE

BREACH INVESTIGATION
FORENSICS
SECURITY AUTOMATION

50 днів

Днів (в середньому) на Стримування та Розслідування

(BakerHostetler 2016 Data Security IR Report)

exabeam

COMPROMISED INSIDER

STOLEN CREDENTIALS MALWARE/RANSOMWARE PHISHING

ANOMALOUS ACCESS MONITORING

ACCOUNT CREATION/MANAGEMENT MONITORING

PRIVILEGED USER/EXECUTIVE ACCOUNT MONITORING

EMAIL/WEB ANALYTICS

SERVICE ACCOUNT MONITORING

MALICIOUS INSIDER

INSIDER THREAT DATA LOSS PREVENTION DATA EXFILTRATION

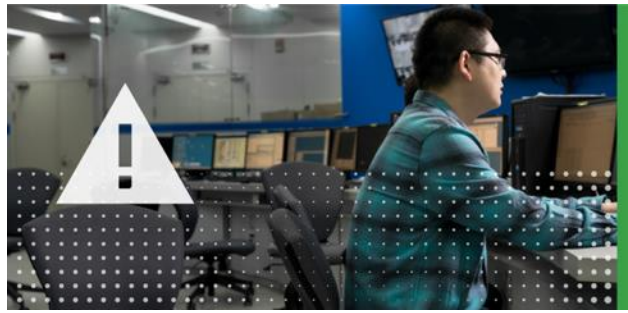
HIGH RISK EMPLOYEE MONITORING

REVOKED ACCESS MONITORING

DATA EXFILTRATION/DATA LOSS PREVENTION

EMAIL/FILE SHARING MONITORING

ENDPOINT ANALYTICS



INCIDENT RESPONSE

BREACH INVESTIGATION FORENSICS SECURITY AUTOMATION

INVESTIGATION AUTOMATION

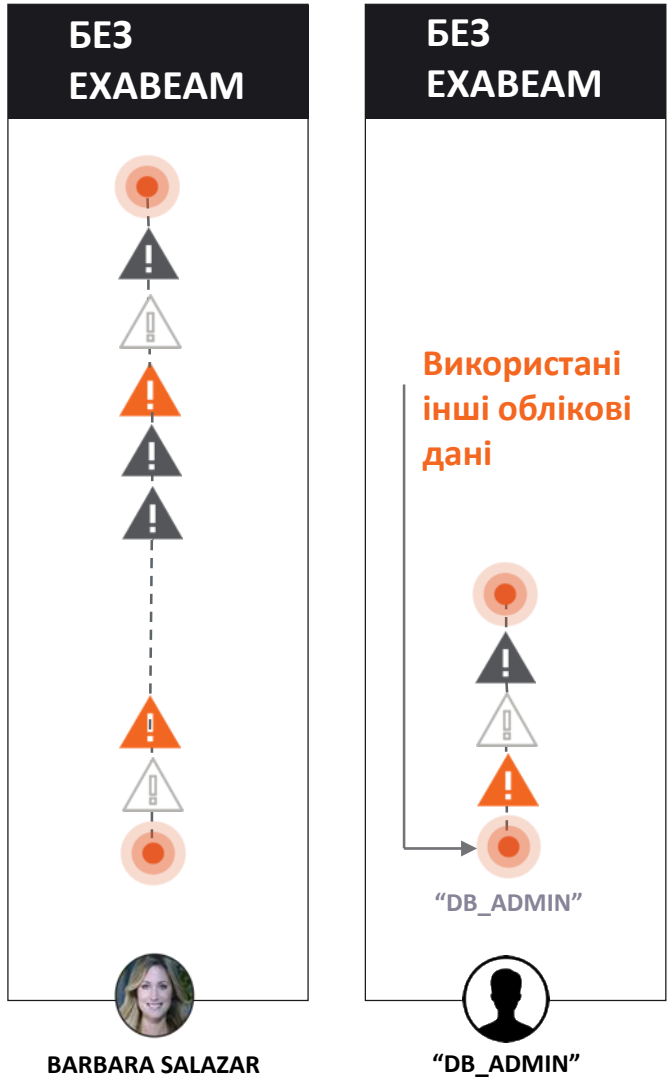
INCIDENT TIMELINES

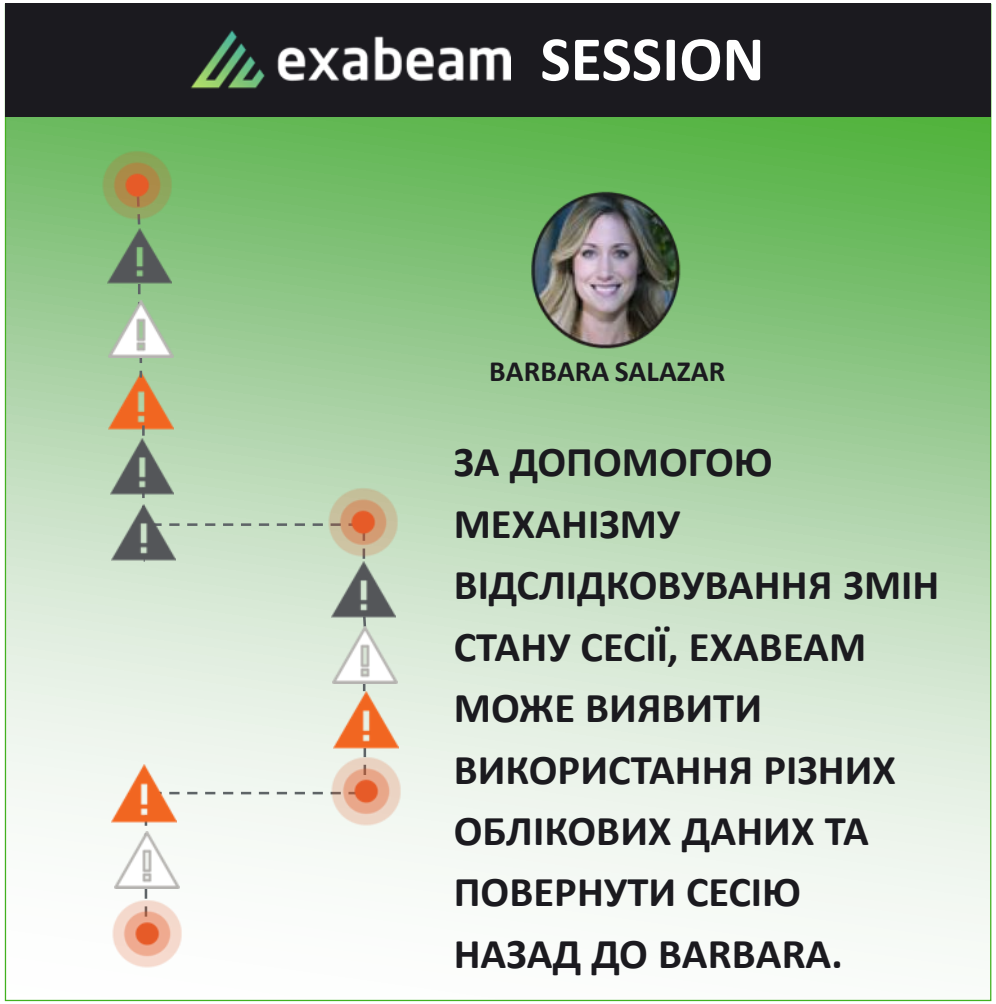
PLAYBOOK EXECUTION

THREAT HUNTING

Унікальний механізм: Stateful сесії

ЦЮ АКТИВНІСТЬ DB ВАРТО БУЛО Б ПОЄДНАТИ З АКТИВНІСТЬЮ BARBARA ЯКА ВИКОРИСТОВУЄ ІНШІ ОБЛІКОВІ ДАНІ, І ЦЕ ВИГЛЯДАЄ ЯК НЕЗАЛЕЖНІ СЕСІЇ.





Чому Exabeam

COMPLETE ATTACK CHAIN

Exabeam – єдиний вендор, який може показати повну історію —звичайну та підозрілу активність разом.

SIMPLICITY FOR FAST VALUE

Exabeam – дуже легкий в користуванні та надає оцінку діям користувачів відразу.

FLIP THE VALUE EQUATION

Exabeam дозволяє аналізувати необмежену кількість даних за передбачуваною ціною.

EASE HIRING GAPS

Exabeam дозволяє послідовно та ефективно реагувати на інциденти.

FASTEST GROWING VENDOR IN THE SIEM MARKET

exabeam

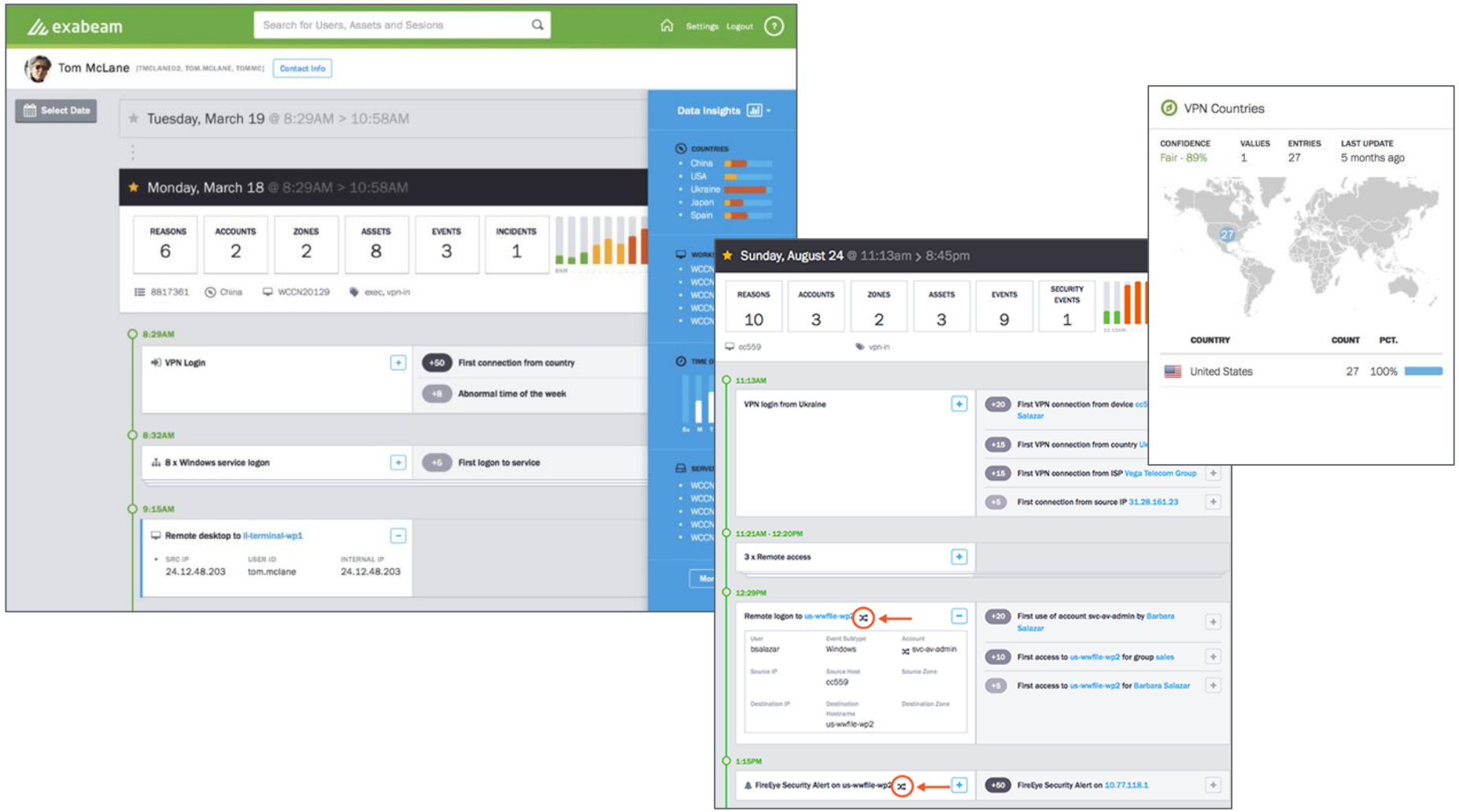
2017 Gartner Magic Quadrant for SIEM

**Gartner* Magic Quadrant for Security Information and Event *Management, Kelly Kavanagh and Toby Bussa, 12/4/17*

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Exabeam.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Демонстрація



exabeam

ДЯКУЮ ЗА УВАГУ

Питання