exabeam

DATASHEET

EXABEAM ADVANCED ANALYTICS

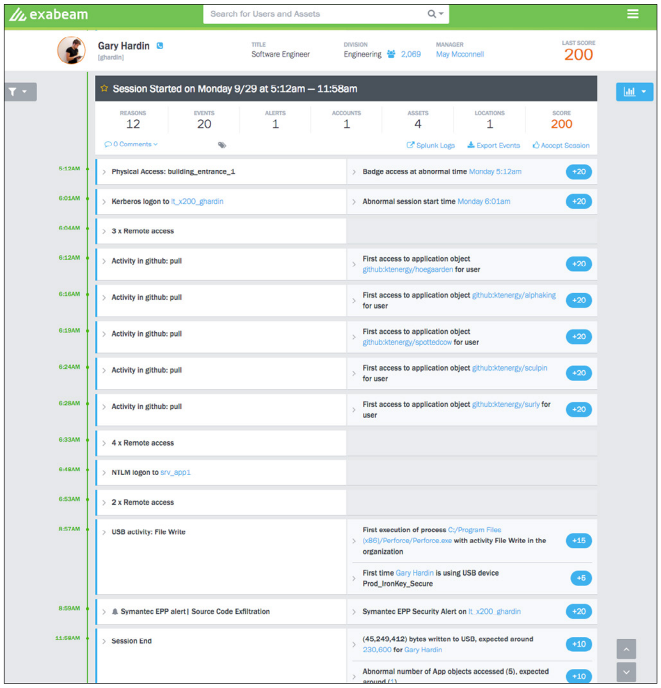
SHINE A LIGHT ON MODERN CYBER-ATTACKS

Today's credential based threats are complex, often touching many systems, using multiple log-ins, and spanning a period of several months. These insider threats involve the legitimate credentials and access privileges of real users, making them challenging for legacy security solutions to detect. In order to tackle these insidious threats, organizations need a solution built from the ground up using modern technologies such as machine learning, behavioral analysis and data science.

A SMARTER APPROACH TO DETECTION AND INVESTIGATION

Exabeam Advanced Analytics is the world's most deployed behavioral analytics platform. Advanced Analytics automatically links and analyzes user and entity activity to better inform security analysts about threats and corresponding remediation. Advanced Analytics provides a powerful analytics layer on top of existing SIEM and log management technologies, detecting new attacks, prioritizing incidents, and guiding a more effective response.

Exabeam Advanced Analytics combines a purpose-built architecture with an investigation-focused user experience designed to fit the way security professionals actually work. Advanced Analytics uses a proprietary Session Data model that automatically stitches together event timelines, including both normal and abnormal behavior, before flagging potential threats. This reduces the manual effort security analysts spend on investigations and increases their productivity.



Gary Hardin [ghardin]

TITLE	DIVISION	MANAGER	LAST SCORE
Software Engineer	Engineering 2,069	May Mcconnell	200

Session Started on Monday 9/29 at 5:12am — 11:58am

REASONS	EVENTS	ALERTS	ACCOUNTS	ASSETS	LOCATIONS	SCORE
12	20	1	1	4	1	200

5:12AM	Physical Access: building_entrance_1	Badge access at abnormal time Monday 5:12am	+20
6:01AM	Kerberos logon to lt_x200_ghardin	Abnormal session start time Monday 6:01am	+20
6:04AM	3 x Remote access		
6:12AM	Activity in github: pull	First access to application object github:ktenergy/hoegaarden for user	+20
6:16AM	Activity in github: pull	First access to application object github:ktenergy/alphaking for user	+20
6:19AM	Activity in github: pull	First access to application object github:ktenergy/spottedcow for user	+20
6:24AM	Activity in github: pull	First access to application object github:ktenergy/sculpin for user	+20
6:28AM	Activity in github: pull	First access to application object github:ktenergy/surly for user	+20
6:33AM	4 x Remote access		
6:48AM	NTLM logon to srv_app1		
6:53AM	2 x Remote access		
8:57AM	USB activity: File Write	First execution of process C:/Program Files (x86)/Perforce/Perforce.exe with activity File Write in the organization	+15
		First time Gary Hardin is using USB device Prod_IronKey_Secure	+5
8:59AM	Symantec EPP alert | Source Code Exfiltration	Symantec EPP Security Alert on lt_x200_ghardin	+20
11:58AM	Session End	(45,249,412) bytes written to USB, expected around 230,600 for Gary Hardin	+10
		Abnormal number of App objects accessed (5), expected around (1)	+10

RAPID TIME TO VALUE

Regardless of the data type or source, Exabeam makes it easy for customers to make use of all of the information available to them in order to perform a truly comprehensive assessment of the threats on their network. Advanced Analytics can ingest logs from a SIEM or directly from the data sources themselves via Syslog. Customers are able to rapidly deploy and analyze historical logs for quick time to value, or analyze new log sources in Advanced Analytics which were previously cost prohibitive to send to their SIEMs. This flexible data handling delivers a fast time to value of unmatched by other behavioral analytics solutions.

COMPOUNDING OPERATIONAL AND COST EFFICIENCIES

The benefits of the Advanced Analytics solution are compounded by Exabeam Data Lake and Incident Responder which together provide full end-to-end coverage for data storage, access, analytics, and automated response. Advanced Analytics can be deployed as a standalone solution, or as part of the larger Exabeam Security Intelligence Platform.

KEY FEATURES

Exabeam provides world class threat detection, prioritizes analyst workloads, and greatly improves SOC productivity. Its key features include:

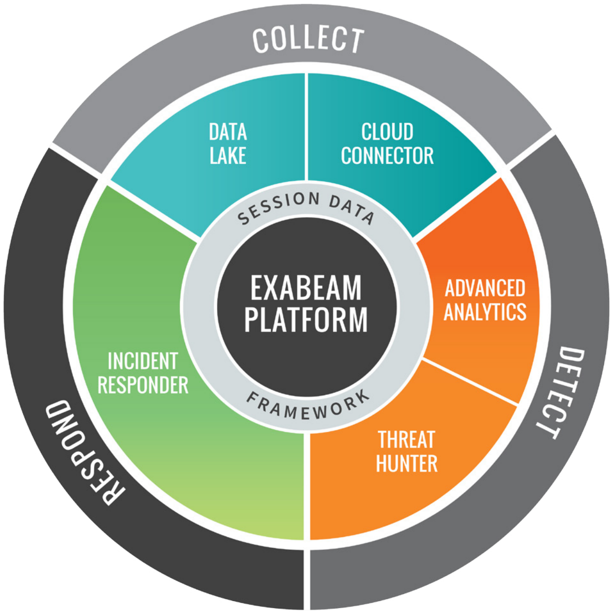
- User and Entity Behavior Analysis (UEBA) based detection for complex modern threats including credential-based attacks, insider threats, and ransomware
- Pre-constructed session timelines which automate analyst investigation, and make proactive analysis faster and easier
- Intelligent security alert prioritization to ensure analysts can easily find the alerts which require the most attention
- A unique session data model that automatically detects lateral movement including changes of credentials, IP addresses, or devices
- Interoperability with all major SIEM solutions, as well as Exabeam's Log Management and Incident Response solutions
- Ease of setup and use
- Scale-out multi-node architecture
- Supports 500+ data sources out of the box
- Ability to deploy as a pre-sized physical appliances or as a cloud-ready VM

EXABEAM SECURITY INTELLIGENCE PLATFORM

Exabeam Data Lake is a key component in the Exabeam Security Intelligence Platform. Any of the platform components can be used together or separately with third party products. The platform includes:

- **Exabeam Data Lake**
- **Exabeam Advanced Analytics**
- **Exabeam Threat Hunter**
- **Exabeam Incident Responder**
- **Exabeam Cloud Connectors**

To learn more about these products, please visit www.exabeam.com/products to download whitepapers, datasheets, etc.



OPERATING INFORMATION

- Deployable as a physical appliance (in multiple sizes) or as a cloud-ready virtual machine
- Includes out of the box collection agents and parsers for over 500 security data sources
- Agents operate on Windows or Linux platforms

For more information, please contact Exabeam at info@exabeam.com