v4.00

Exabeam TDIR Training for Security Analysts

EDU-2170

Photo by Andrew Neel on Unsplash

v4.00

exabeam

How Exabeam Empowers Security Teams

EDU-2170 : Module 1

Student Notes

Thank you for attending this class! We look forward to teaching you more about Exabeam technologies.

The purpose of this course is to help analysts use daily the Exabeam SOC Platform to detect, investigate, and respond to threats, with rapid time to value, out-of-the-box integration, and pre-tuned detection mechanisms. Let’s get started!

What are your daily security challenges?

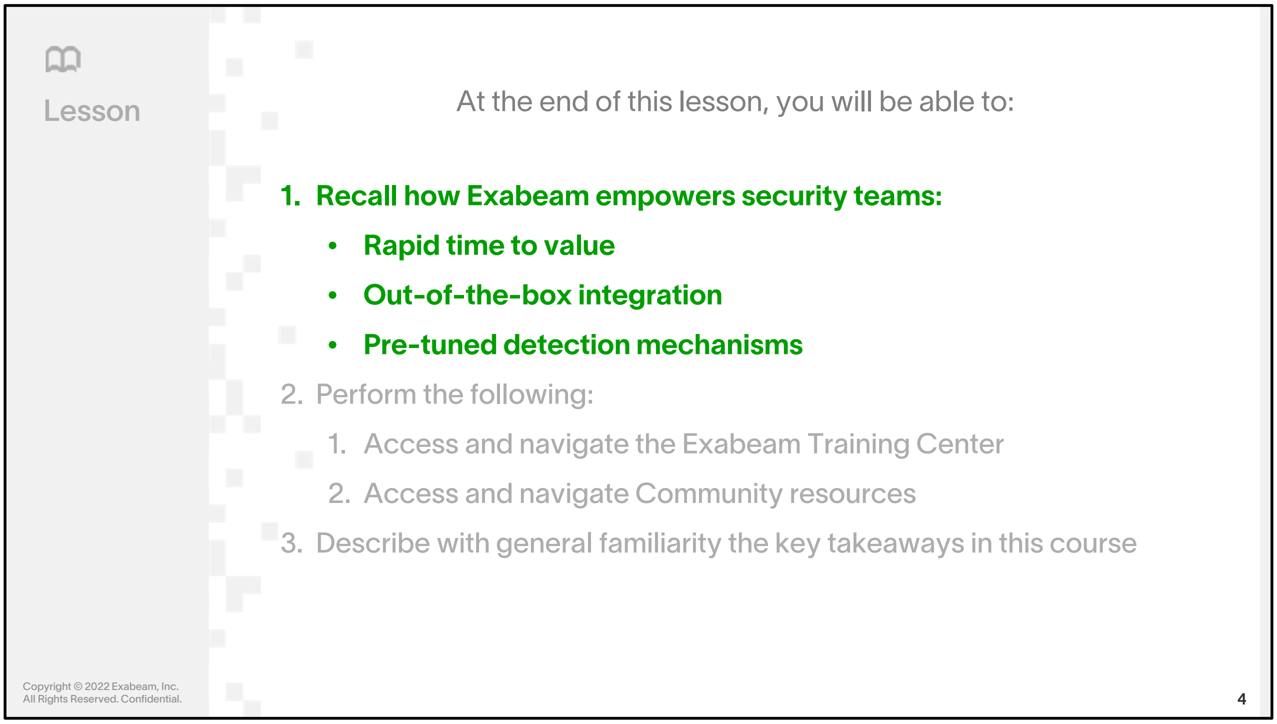
Student Notes

Security begins with a careful examination of the organization's “crown jewels” and an awareness of the threats against those assets, as well as any processes, services, functions, or protections that support those critical IT assets. One way Exabeam enriches log data is by distinguishing the critical assets your organization has identified, then assessing additional risk for those systems when abnormal behaviors are associated with them.

Think about where your team spends its most time with security incidents. What are those challenges? How would you go about fixing them?

References

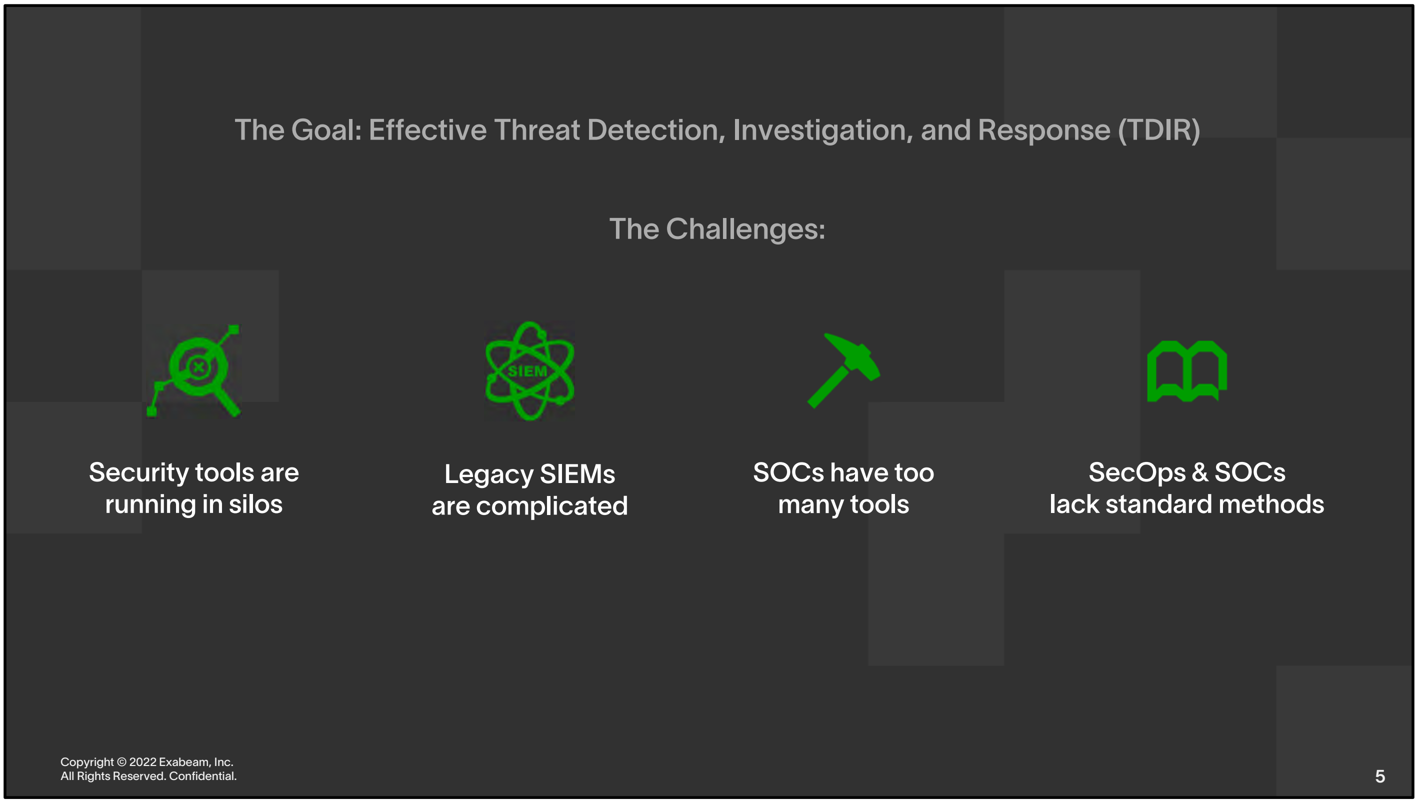
https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis



Lesson

At the end of this lesson, you will be able to:

1. **Recall how Exabeam empowers security teams:**
   - **Rapid time to value**
   - **Out-of-the-box integration**
   - **Pre-tuned detection mechanisms**
2. Perform the following:
   1. Access and navigate the Exabeam Training Center
   2. Access and navigate Community resources
3. Describe with general familiarity the key takeaways in this course



The Goal: Effective Threat Detection, Investigation, and Response (TDIR)

The Challenges:

Security tools are running in silos

Legacy SIEMs are complicated

SOCs have too many tools

SecOps & SOCs lack standard methods

Student Notes

In understanding how Exabeam will fit into your security architecture, it's important to know that establishing effective Threat Detection, Investigation, and Response is still a major problem for many SOCs.

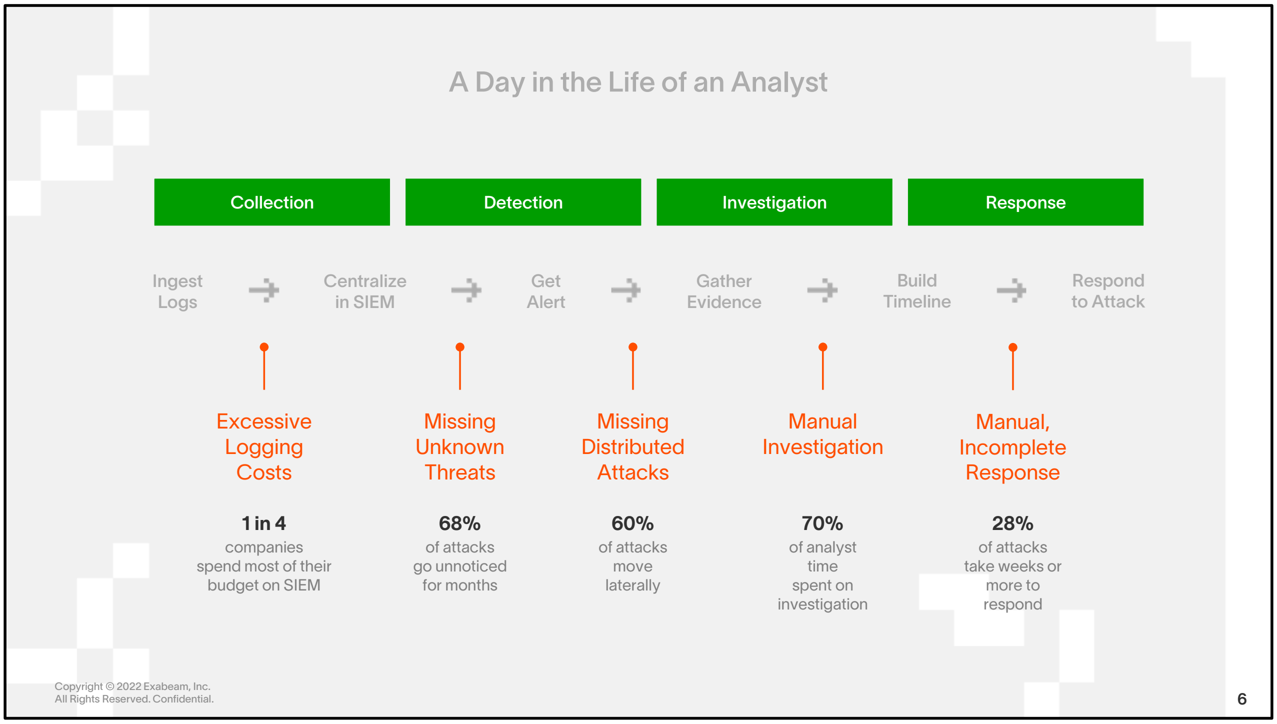
While there can be many reasons for this, several recurring themes are:

- Security tools running in solos
- Legacy SIEMs being over complicated
- SOCs using too many tools
- And the lack of standard methods for SecOps and SOCs to follow

See this series of blog posts to learn more about effective and modern SOC procedures:
https://www.exabeam.com/?s=Demystifying+the+SOC&search-type=blog&user_query=&category=&tag=

To the final point, it's critical that organizations develop and maintain a formal Incident Response capability, and that any response aligns with that IR process. For details on developing and maintaining an Incident Response plan, policy, and procedure, see the NIST documentation in the reference section below.

References
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf



A Day in the Life of an Analyst

Collection | Detection | Investigation | Response

Ingest Logs → Centralize in SIEM → Get Alert → Gather Evidence → Build Timeline → Respond to Attack

Excessive Logging Costs
1 in 4 companies spend most of their budget on SIEM

Missing Unknown Threats
68% of attacks go unnoticed for months

Missing Distributed Attacks
60% of attacks move laterally

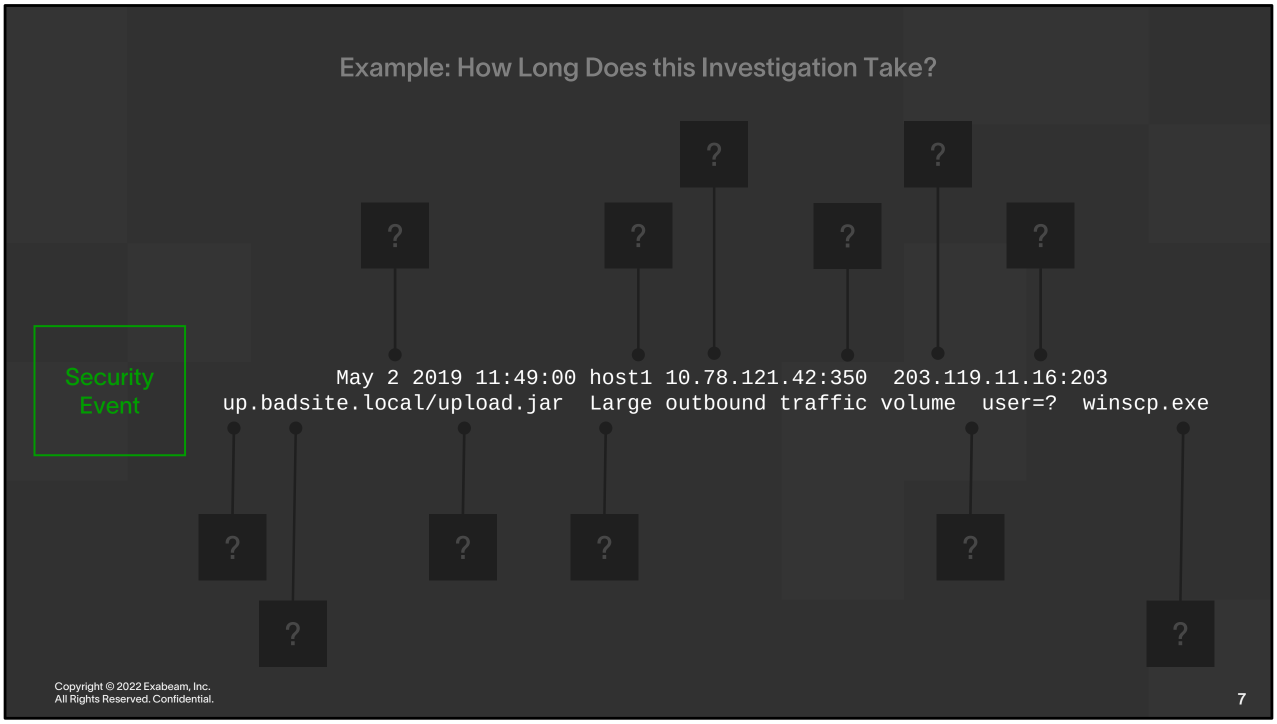
Manual Investigation
70% of analyst time spent on investigation

Manual, Incomplete Response
28% of attacks take weeks or more to respond

Student Notes

For More Information:

1- Dark Reading – How Enterprises Spend their IT Security Dollars, June 2017 - https://dsimg.ubm-us.net/envelope/390213/526993/TCM_DR_1705079_Dark%20Reading%20Security%20Spending%20Report.pdf
2 – Dark Reading, what the incident responders saw – 2018 - https://www.darkreading.com/endpoint/privacy/what-the-incident-responders-saw/d/d-id/1332349
3 – CISO public cyber security company, 2018 - https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf
4 - 2018 Verizon Data Breach Investigation Report - https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf



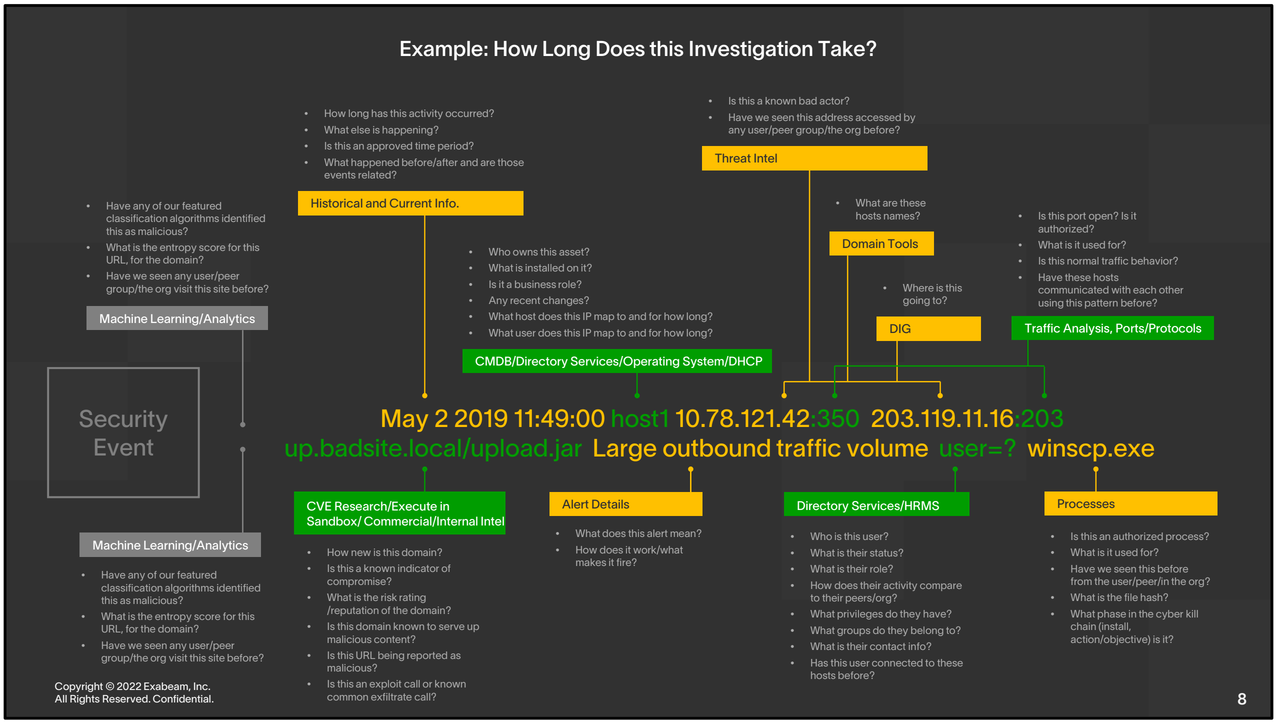
Example: How Long Does this Investigation Take?

Security Event

```
          May 2 2019 11:49:00 host1 10.78.121.42:350  203.119.11.16:203
up.badsite.local/upload.jar  Large outbound traffic volume  user=?  winscp.exe
```

Student Notes

What questions do you find your self asking with a security event you find in a log?



Example: How Long Does this Investigation Take?

Security Event

May 2 2019 11:49:00 host1 10.78.121.42:350 203.119.11.16:203 up.badsite.local/upload.jar Large outbound traffic volume user=? winscp.exe

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?

Historical and Current Info.

- How long has this activity occurred?
- What else is happening?
- Is this an approved time period?
- What happened before/after and are those events related?

CMDB/Directory Services/Operating System/DHCP

- 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?

Threat Intel

- Is this a known bad actor?
- Have we seen this address accessed by any user/peer group/the org before?

Domain Tools

- What are these hosts names?

DIG

- Where is this going to?

Traffic Analysis, Ports/Protocols

- Is this port open? Is it authorized?
- What is it used for?
- Is this normal traffic behavior?
- Have these hosts communicated with each other using this pattern before?

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?

CVE Research/Execute in Sandbox/ 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 exfiltrate call?

Alert Details

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

Directory Services/HRMS

- 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?

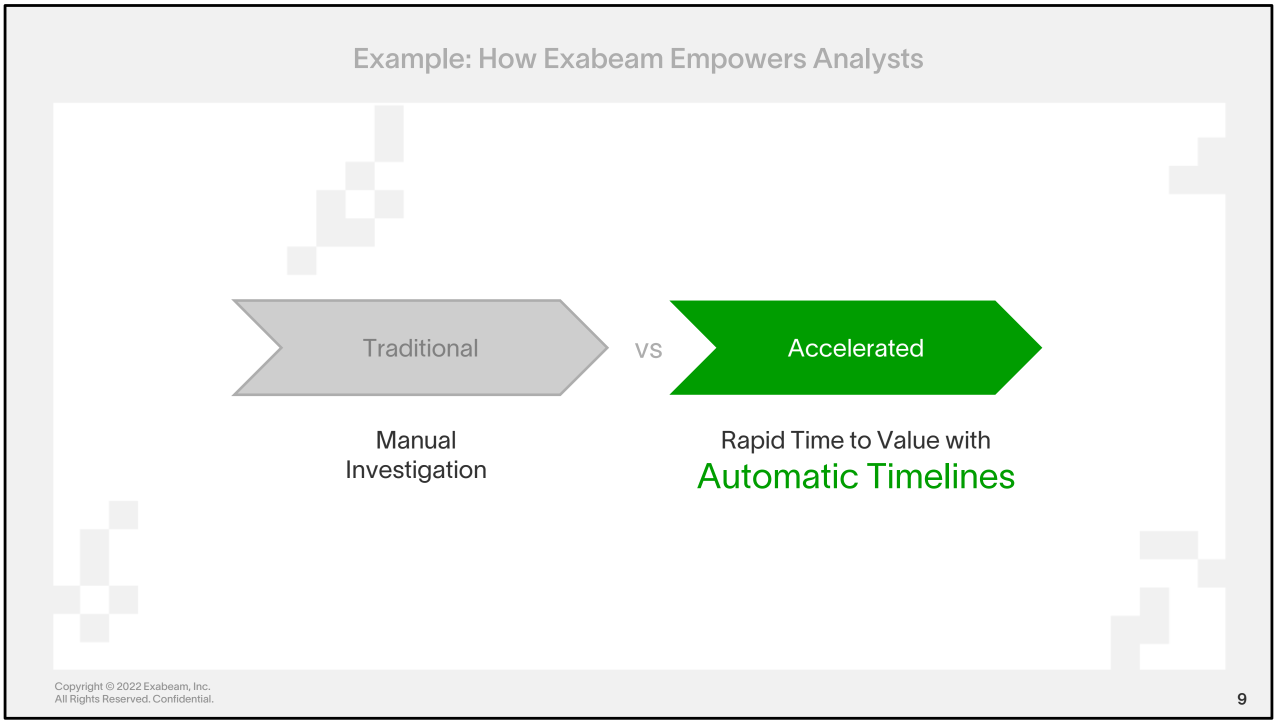
Processes

- 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?

Student Notes

How long does it take you to follow all the leads and create a timeline of what may be occurring? What tools are you using?

For more information, please see these informative blog articles:
https://www.exabeam.com/siem/recreating-an-incident-timeline-manual-vs-automated-part-1/
https://www.exabeam.com/siem/recreating-an-incident-timeline-manual-vs-automated-part-2/



Example: How Exabeam Empowers Analysts

Traditional vs Accelerated

Manual Investigation

Rapid Time to Value with **Automatic Timelines**

Student Notes

Traditional investigation is labor-intensive and manual. This is due to the volume of questions, pivots, and tools required to develop and analyze timelines to detect and then respond to threats. This is valuable time lost.

Exabeam adds power, speed, and insight to help analysts accelerate their processes.

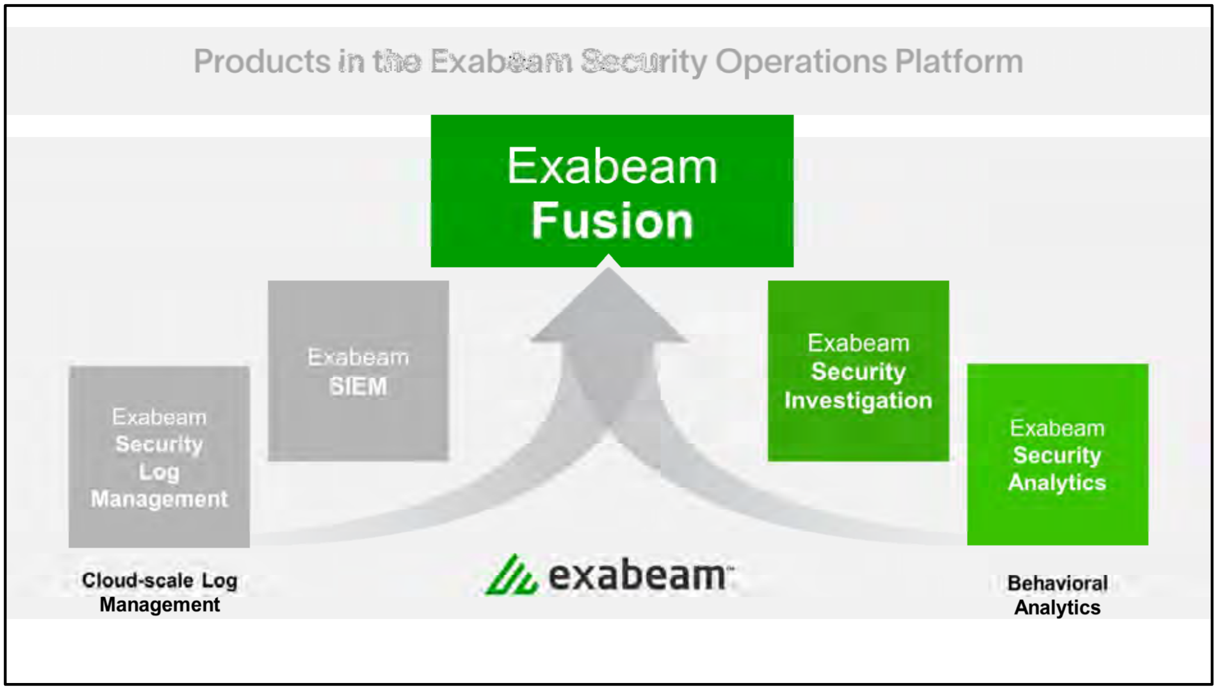
Here is a summary of the difference between a traditional and a modern accelerated threat detection, investigation, and response (TDIR) workflow:

TRADITIONAL

- Disconnected data requires manual investigation
- Manual investigations takes hours/days
- Too many tools add friction and delays

ACCELERATION

- Machine learning accelerates detection
- Automatic incident timelines accelerate analysis
- Context accelerates decisions


Products in the Exabeam Security Operations Platform
Exabeam Fusion
Exabeam SIEM
Exabeam Security Log Management
Exabeam Security Investigation
Exabeam Security Analytics
Cloud-scale Log Management
exabeam
Behavioral Analytics

Exabeam Security Analytics

Automated threat detection powered by user and entity behavior analytics with correlation and threat intelligence

Run on Top of Existing Architecture

Run Exabeam Security Analytics on top of your existing SIEM/data lakes or with Exabeam SIEM

+

Powerful Behavioral Analytics

Understand normal behavior of users and devices to detect and prioritize anomalies based on risk

Exabeam Security Investigation

Threat detection, investigation, and response powered by user and entity behavioral analytics, correlation rules, and threat intelligence, supported by alerting, incident management, automated triage, and response workflows

Run on Top of Existing Architecture

Run Exabeam Security Investigation with your existing SIEM/data lakes or with Exabeam SIEM

+

Powerful Behavioral Analytics

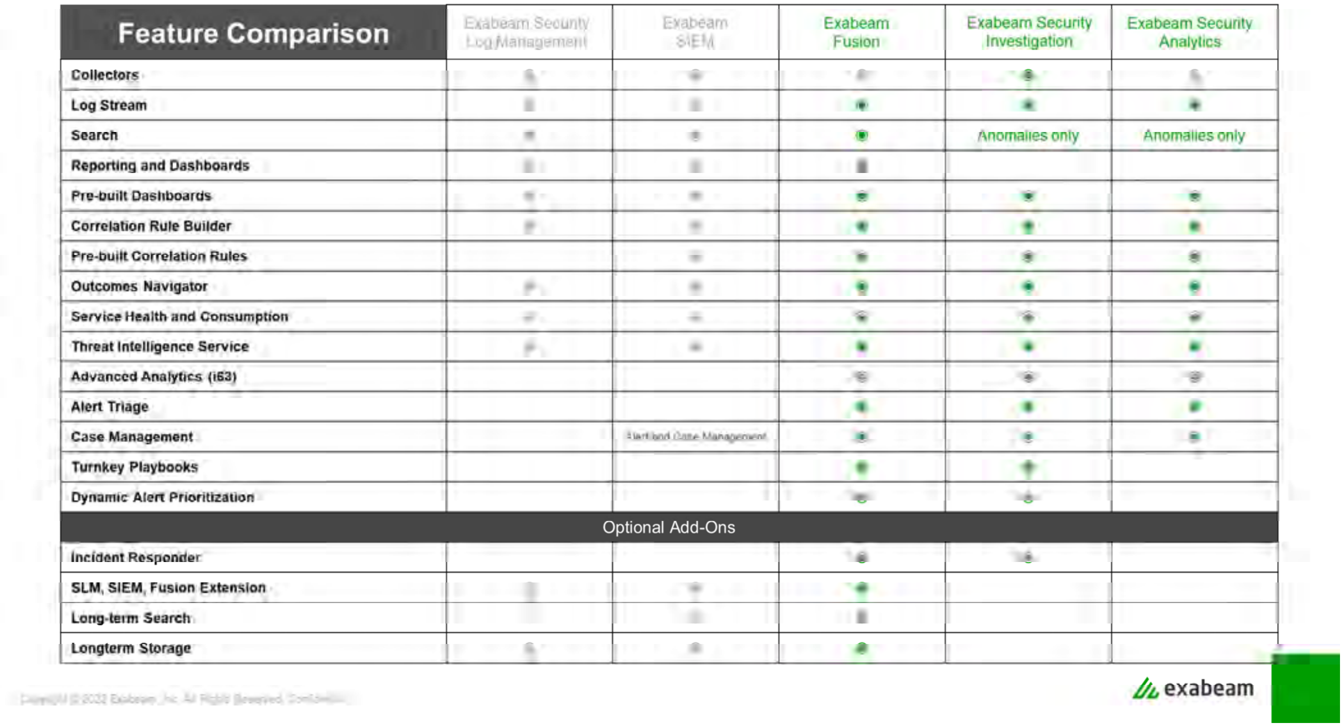
Understand normal behavior of users and devices to detect and prioritize anomalies based on risk

+

Automated Investigation Experience

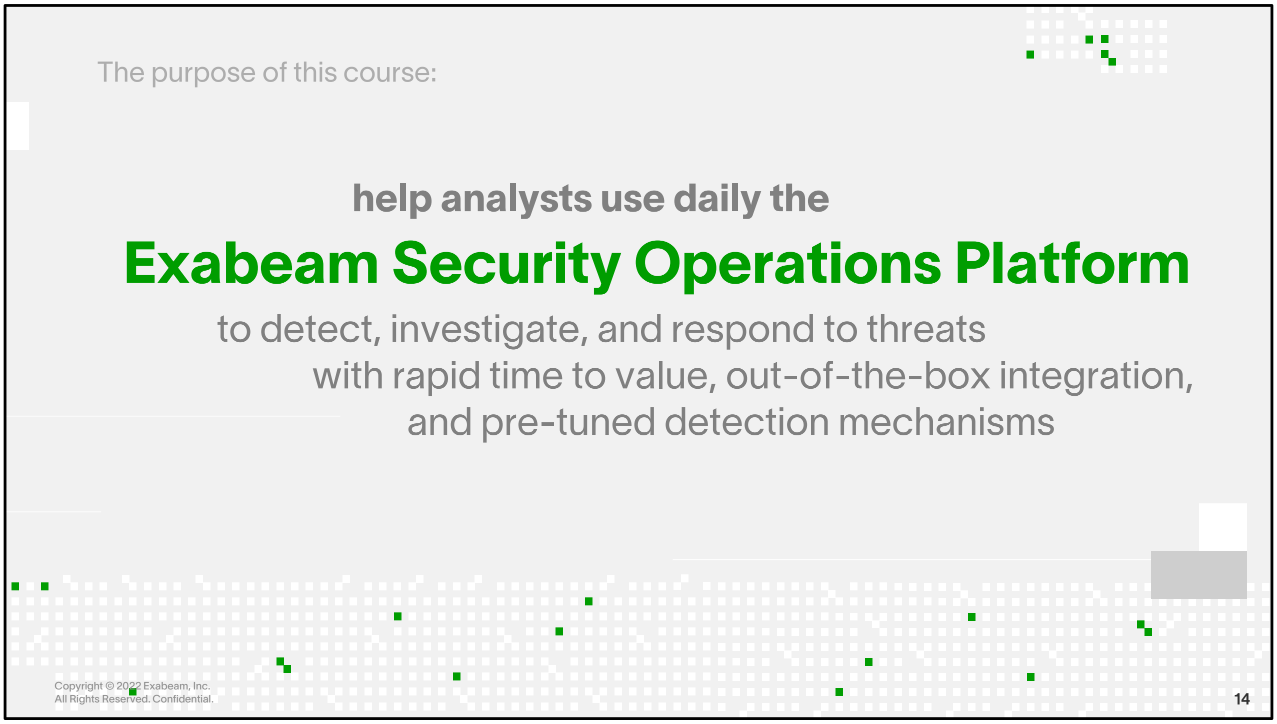
An automated experience across the threat detection, investigation, and response (TDIR) workflow to reduce manual routines

exabeam



Feature Comparison	Exabeam Security Log Management	Exabeam SIEM	Exabeam Fusion	Exabeam Security Investigation	Exabeam Security Analytics
Collectors	●	●	●	●	●
Log Stream	●	●	●	●	●
Search	●	●	●	Anomalies only	Anomalies only
Reporting and Dashboards	●	●	●		
Pre-built Dashboards	●	●	●	●	●
Correlation Rule Builder	●	●	●	●	●
Pre-built Correlation Rules		●	●	●	●
Outcomes Navigator	●	●	●	●	●
Service Health and Consumption	●	●	●	●	●
Threat Intelligence Service	●	●	●	●	●
Advanced Analytics (i63)			●	●	●
Alert Triage			●	●	●
Case Management		Alert and Case Management	●	●	●
Turnkey Playbooks			●	●	
Dynamic Alert Prioritization			●	●	
Optional Add-Ons					
Incident Responder			●	●	
SLM, SIEM, Fusion Extension	●	●	●		
Long-term Search	●	●	●		
Longterm Storage	●	●	●		

If they want incident responder, dynamic alert prioritization, automatically position security investigation
SI gets all of Security Analytics + Incident response automation and the pricing isn't too different, with the gap being only about 7%



The purpose of this course:

help analysts use daily the

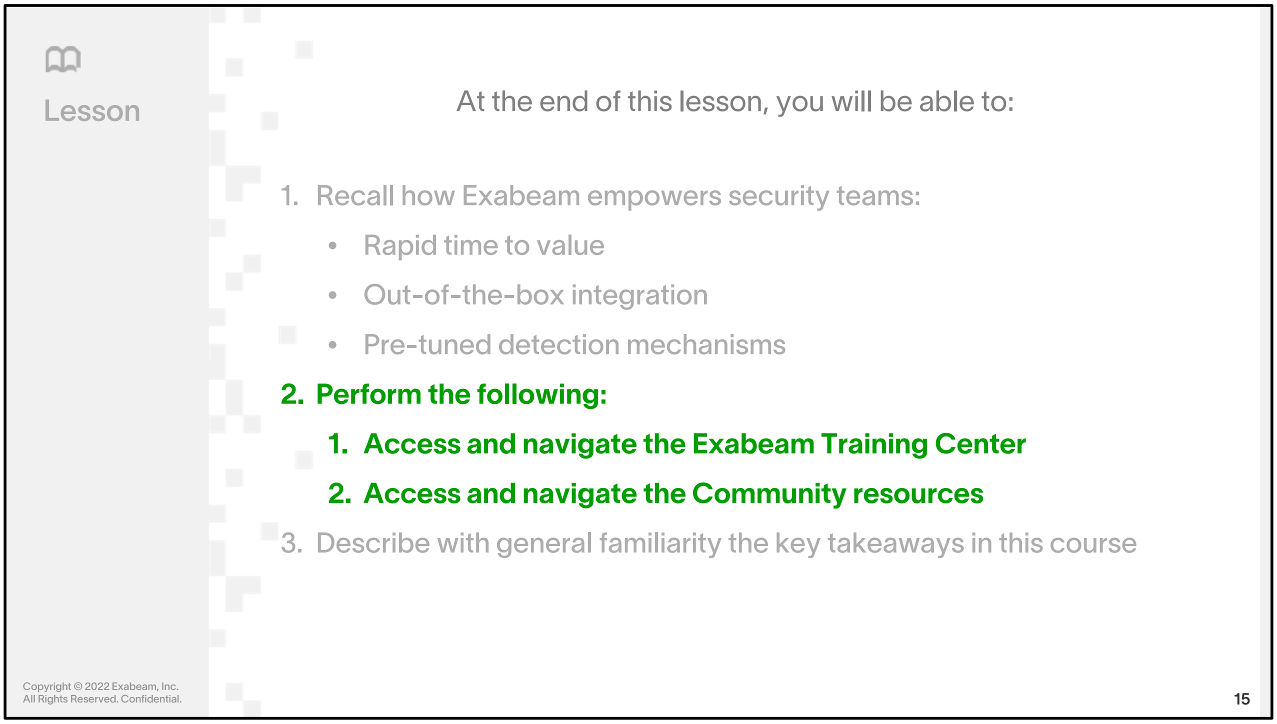
Exabeam Security Operations Platform

to detect, investigate, and respond to threats
with rapid time to value, out-of-the-box integration,
and pre-tuned detection mechanisms

Student Notes

At the end of this course, you should be able to do the following:

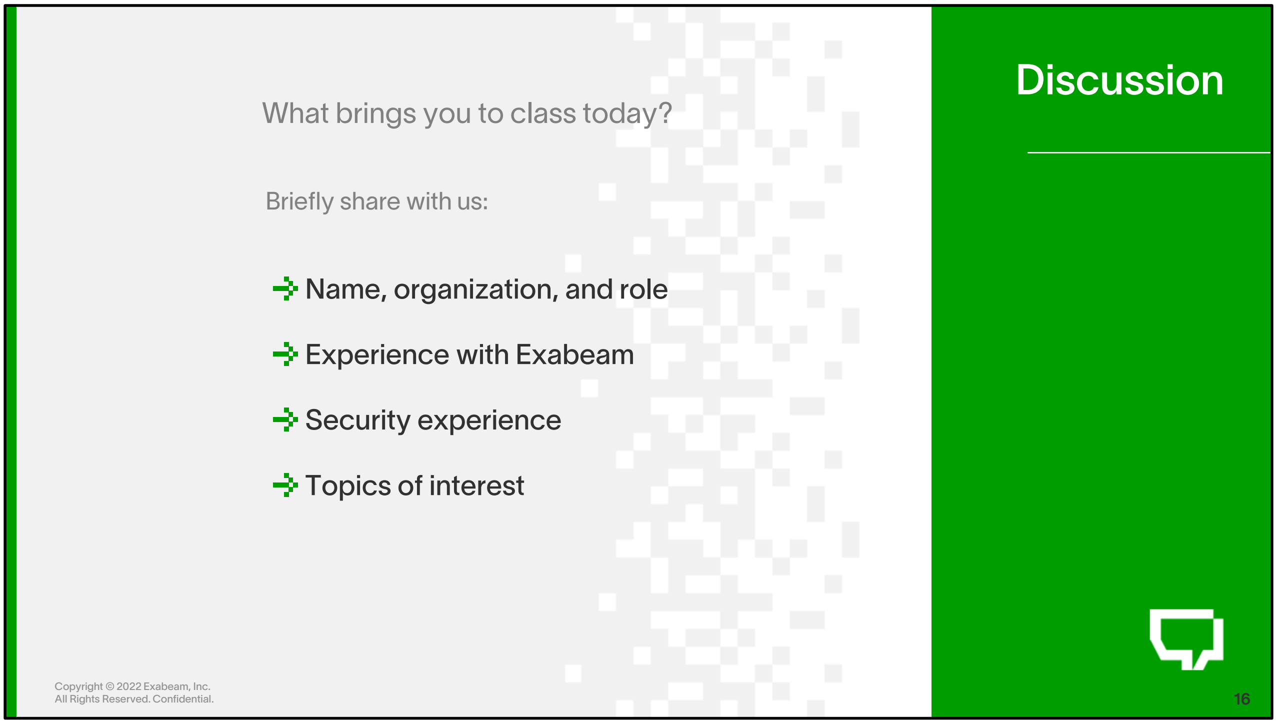
1. Recall how Exabeam empowers security teams
    a. Rapid time to value
    b. Out-of-the-box integration
    c. Pre-tuned detection mechanisms
2. Recall the capabilities of Exabeam and how they work to help gain greater visibility and security; this includes alert triage, user and entity behavior analytics (UEBA), threat hunting, risk scoring, and Smart Timelines™.
3. Perform investigations following analyst workflows using applications from the Exabeam Security Operations Platform:
    a. Reactive Investigations
        i. Incident Driven and Notables List
        ii. Alert Triage
    b. Proactive Monitoring and Hunting
        i. Watchlists
        ii. Search (basic search, TH search, TTP-based searches, model search)
4. Perform incident tracking and response, complete incident check lists, create and monitor watchlists, and apply the MITRE ATT&CK framework for higher velocity investigations, including TTP based searches.
5. Recall how to achieve security outcomes using Exabeam Threat Detection Investigation and Response (TDIR) Use Case packages:
    a. Compromised Insiders
    b. Malicious Insiders
    c. External Threats
6. Describe the role of data sources within the Exabeam SecOps Platform for both context and Use Case packages.
7. Describe the core functionality of the Exabeam Data Lake application.
8. Run Data Lake queries and generate reports, dashboards, and visualizations for monitoring and visibility.
9. Access educational resources in Exabeam's Training Center and Exabeam Community for additional learning and professional development



Lesson

At the end of this lesson, you will be able to:

1. Recall how Exabeam empowers security teams:
   - Rapid time to value
   - Out-of-the-box integration
   - Pre-tuned detection mechanisms
2. **Perform the following:**
   1. **Access and navigate the Exabeam Training Center**
   2. **Access and navigate the Community resources**
3. Describe with general familiarity the key takeaways in this course

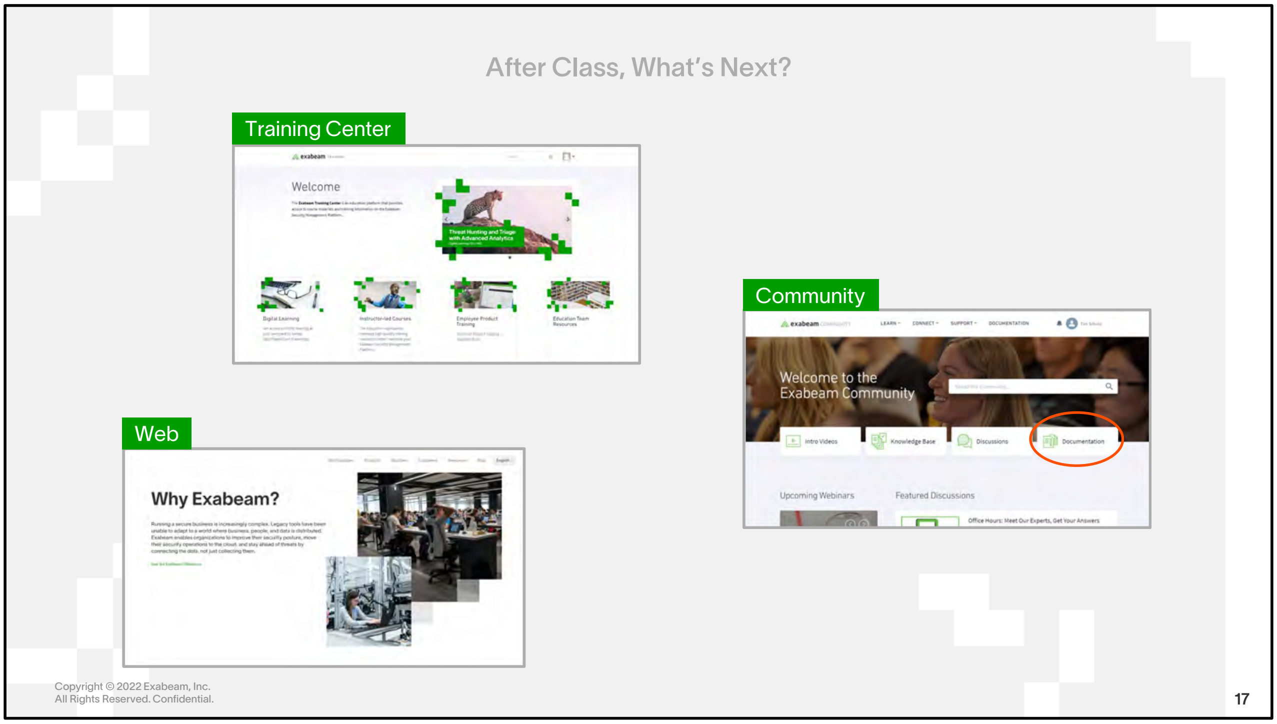


Discussion

What brings you to class today?

Briefly share with us:

- Name, organization, and role
- Experience with Exabeam
- Security experience
- Topics of interest



After Class, What's Next?

Training Center

Welcome

Threat Hunting and Triage with Advanced Analytics

Digital Learning

Instructor-led Courses

Employee Product Training

Education Team Resources

Community

Welcome to the Exabeam Community

Intro Videos

Knowledge Base

Discussions

Documentation

Upcoming Webinars

Featured Discussions

Office Hours: Meet Our Experts, Get Your Answers

Web

Why Exabeam?

Student Notes

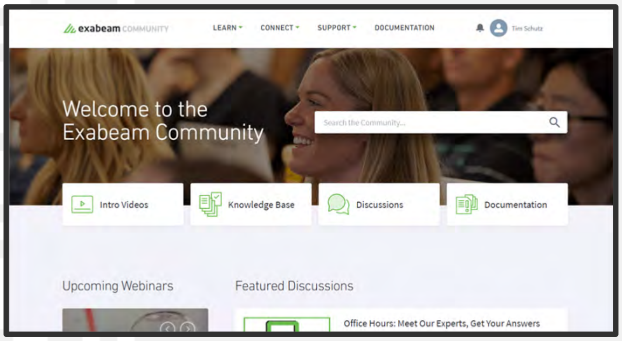
The Exabeam website includes high level information useful to orient yourself to the current product offerings – https://www.exabeam.com

The Community Pages provide in depth information, and the documentation portion can be reached directly through https://docs.exabeam.com

The Training Center provides access to engage with various types of learning resources including eLearning – https://www.customer.exabeamtraining.com

Demo

A Look at the Training Center and Community

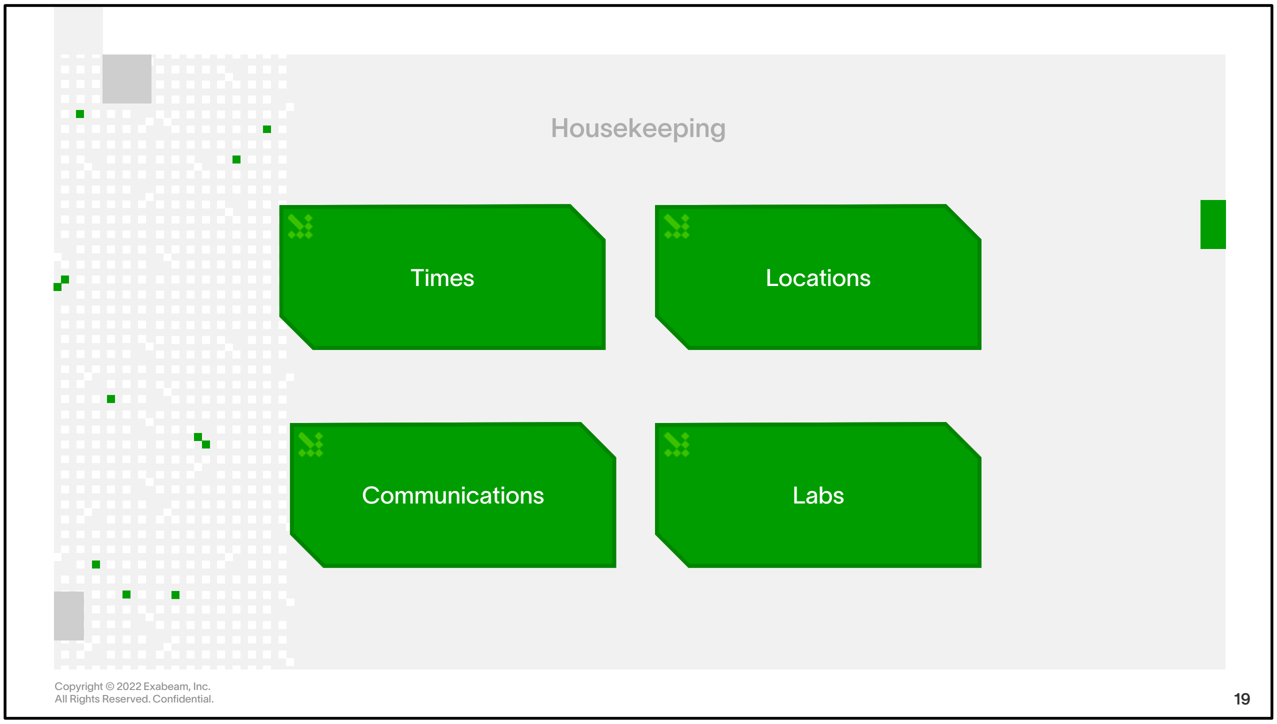


Welcome to the
Exabeam Community

Upcoming Webinars

Featured Discussions

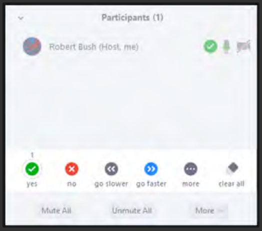
Office Hours: Meet Our Experts, Get Your Answers



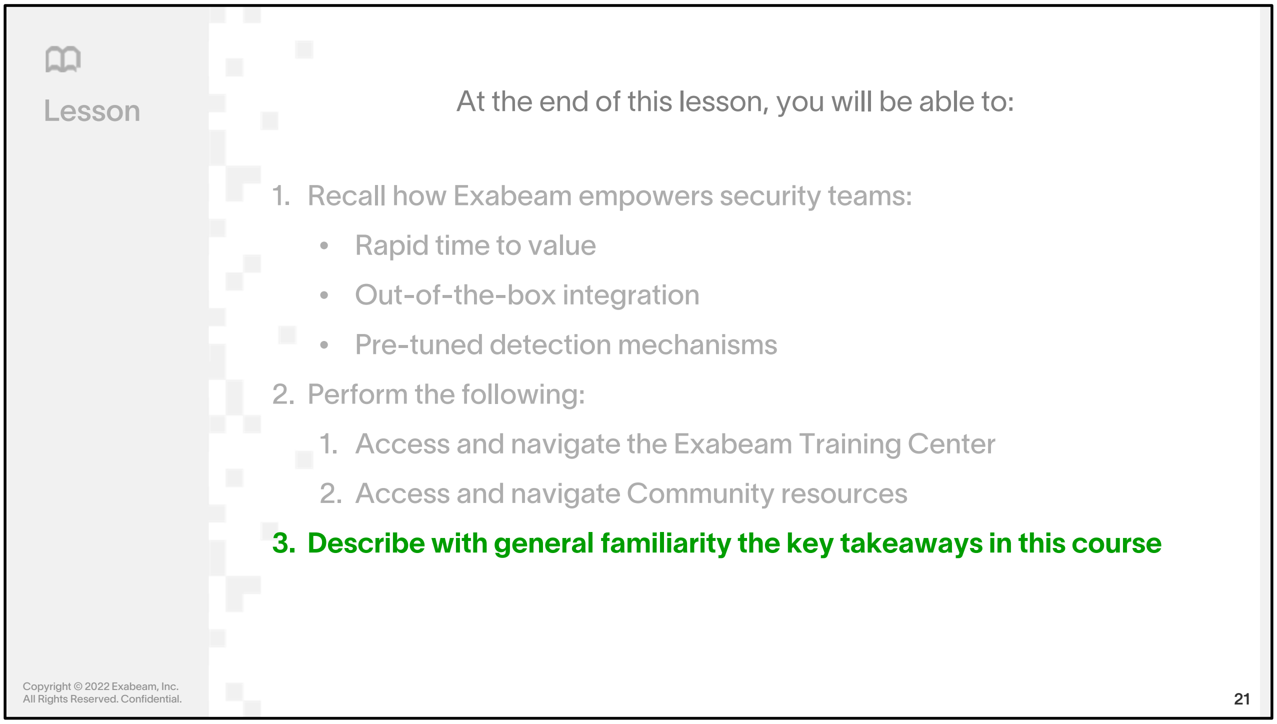
Housekeeping

- Times
- Locations
- Communications
- Labs

Virtual Training Considerations



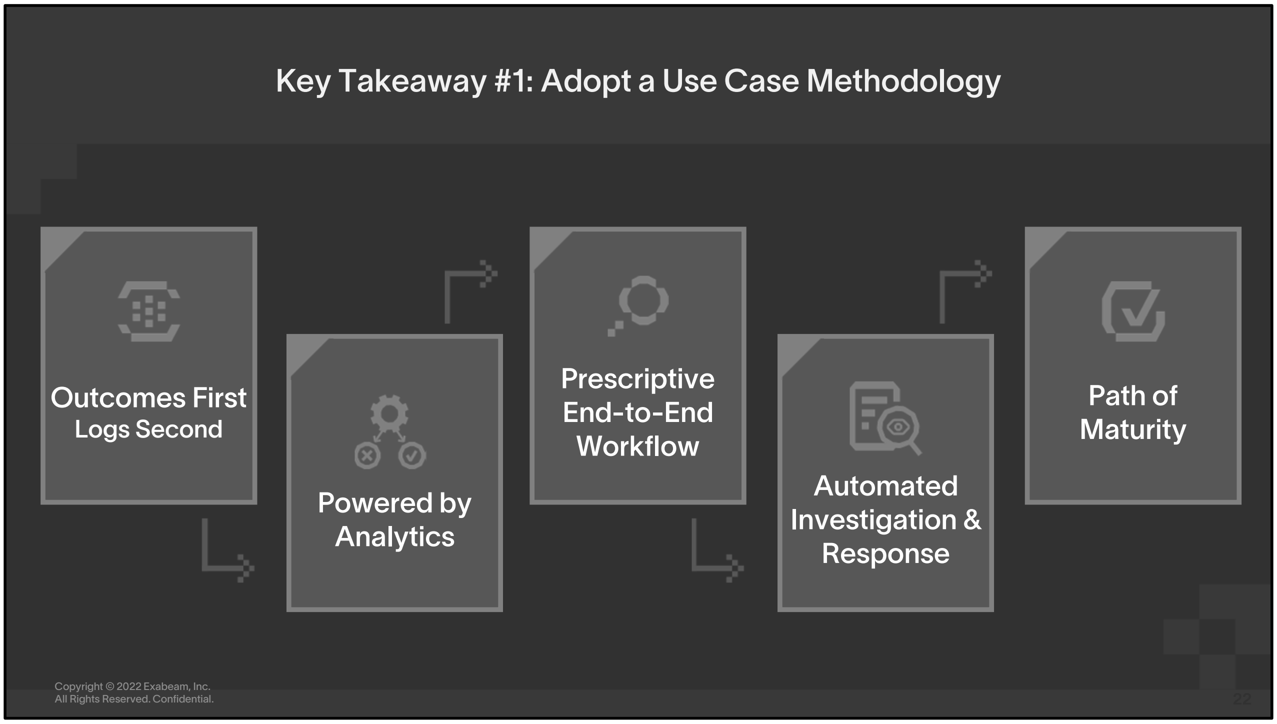
- Use Chat
- If you need a break, please say so!
- Zoom feedback functions are vital for breaks and labs



Lesson

At the end of this lesson, you will be able to:

1. Recall how Exabeam empowers security teams:
   - Rapid time to value
   - Out-of-the-box integration
   - Pre-tuned detection mechanisms
2. Perform the following:
   1. Access and navigate the Exabeam Training Center
   2. Access and navigate Community resources
3. **Describe with general familiarity the key takeaways in this course**



Key Takeaway #1: Adopt a Use Case Methodology

Outcomes First
Logs Second

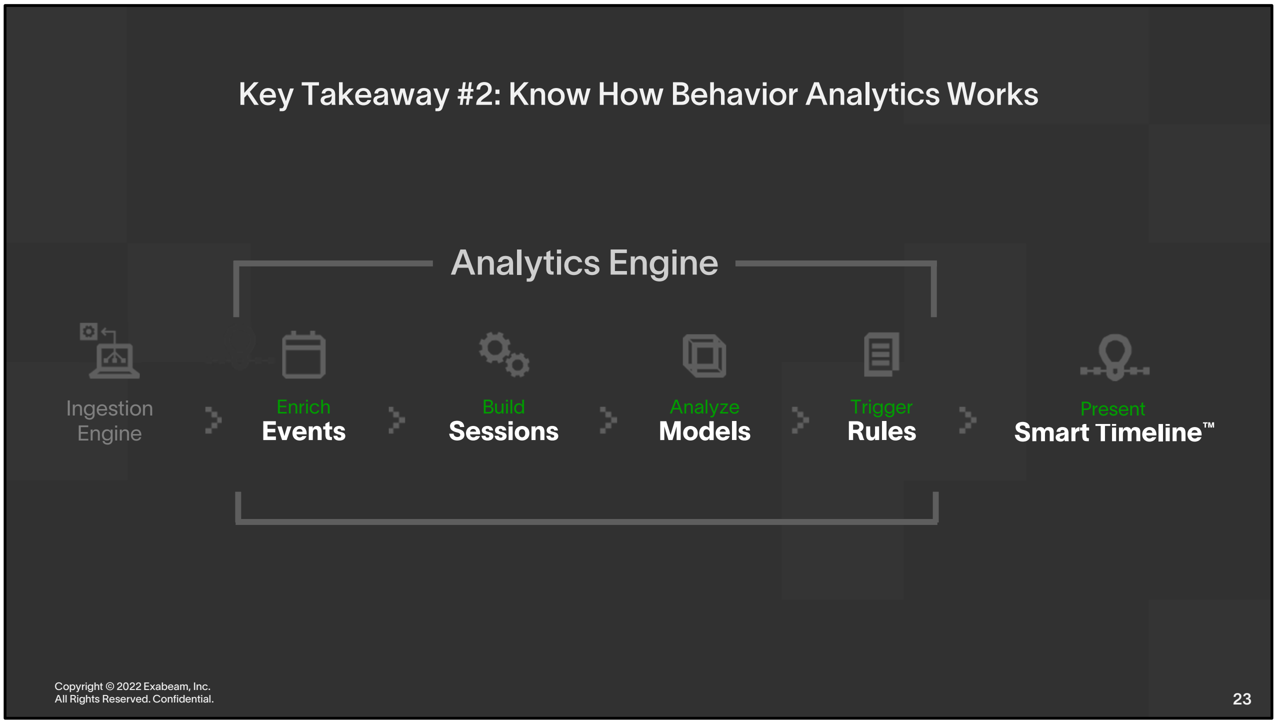
Powered by Analytics

Prescriptive End-to-End Workflow

Automated Investigation & Response

Path of Maturity

1) Outcomes First, Logs Second
2) Powered by Analytics
3) Prescriptive End-to-End Workflow
4) Automated Investigation & Response
5) Path of Maturity (continuous improvement)



Key Takeaway #2: Know How Behavior Analytics Works

Analytics Engine

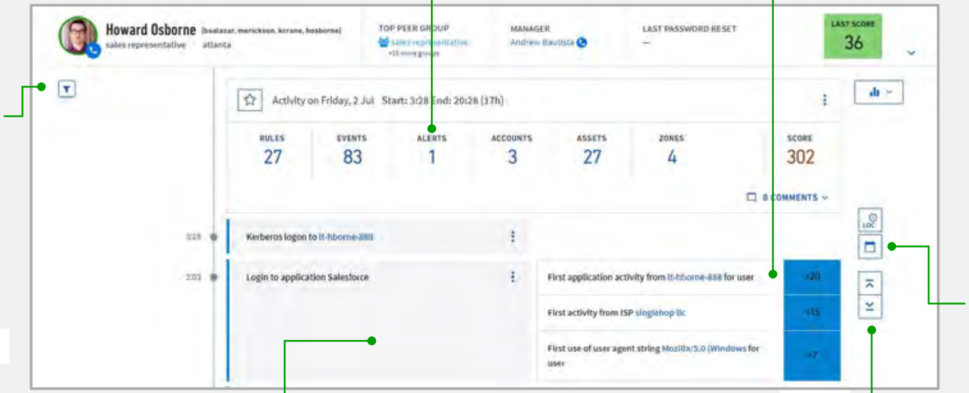
Ingestion Engine > Enrich **Events** > Build **Sessions** > Analyze **Models** > Trigger **Rules** > Present **Smart Timeline™**

Student Notes

Analytics Engine Tasks:

- Enrich the events with contextual data.
- Build sessions out of user and entity activity.
- Models analyze the events for machine-learning.
- Evaluate this activity using rules to trigger against anomalous, abnormal events and assign risk scores.
- Build Smart Timelines, showing normal and abnormal activity chronologically.

Key Takeaway#2: Know How Behavior Analytics Works



Howard Osborne (bsalazar, merickson, kcrane, hosborne)
sales representative | atlanta

TOP PEER GROUP
sales representative
+15 more groups

MANAGER
Andrew Bautista

LAST PASSWORD RESET
—

LAST SCORE
36

Activity on Friday, 2 Jul Start: 3:28 End: 20:28 (17h)

RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES	SCORE
27	83	1	3	27	4	302

0 COMMENTS

3:28 Kerberos logon to lt-hborne-888

3:03 Login to application Salesforce

First application activity from lt-hborne-888 for user	+20
First activity from ISP singlehop llc	+15
First use of user agent string Mozilla/5.0 (Windows for user	+7

Session Header with Findable Statistics

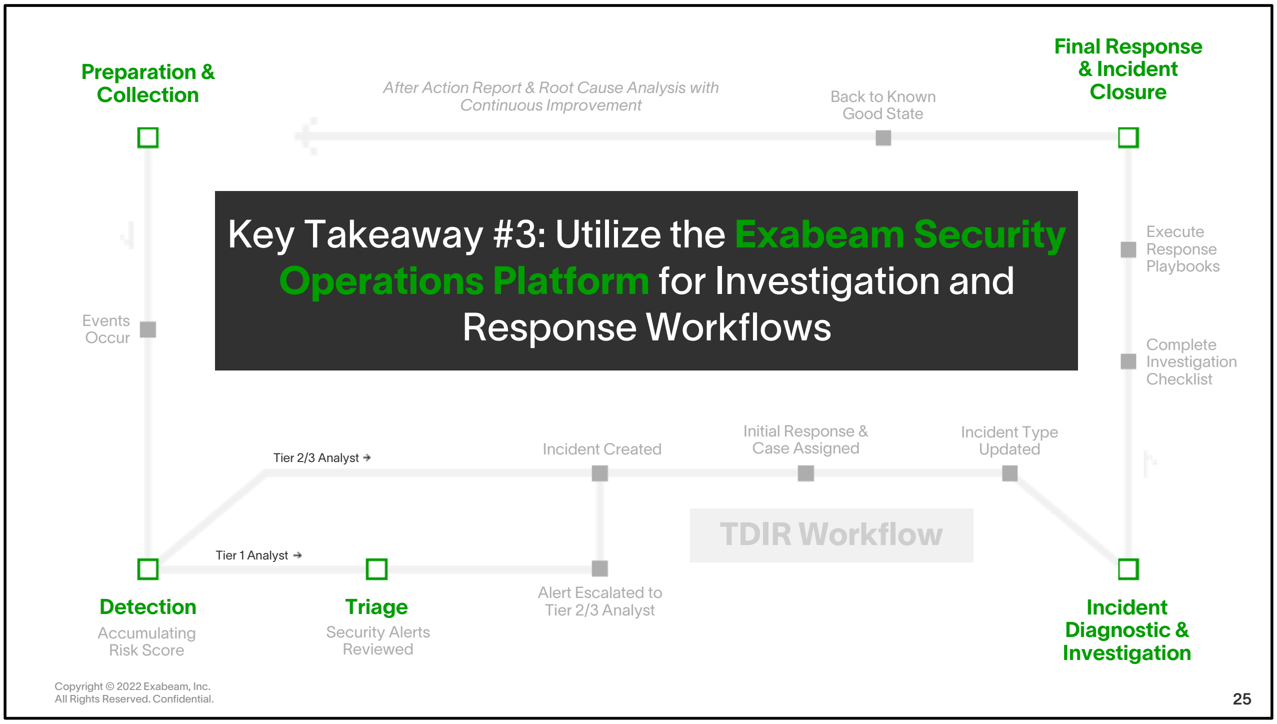
Filter Timeline

Rules Have Details

Date Picker

Events Have Details

Session Back/Forward



Key Takeaway #3: Utilize the **Exabeam Security Operations Platform** for Investigation and Response Workflows

Preparation & Collection

After Action Report & Root Cause Analysis with Continuous Improvement

Back to Known Good State

Final Response & Incident Closure

Events Occur

Execute Response Playbooks

Complete Investigation Checklist

Tier 2/3 Analyst →

Incident Created

Initial Response & Case Assigned

Incident Type Updated

TDIR Workflow

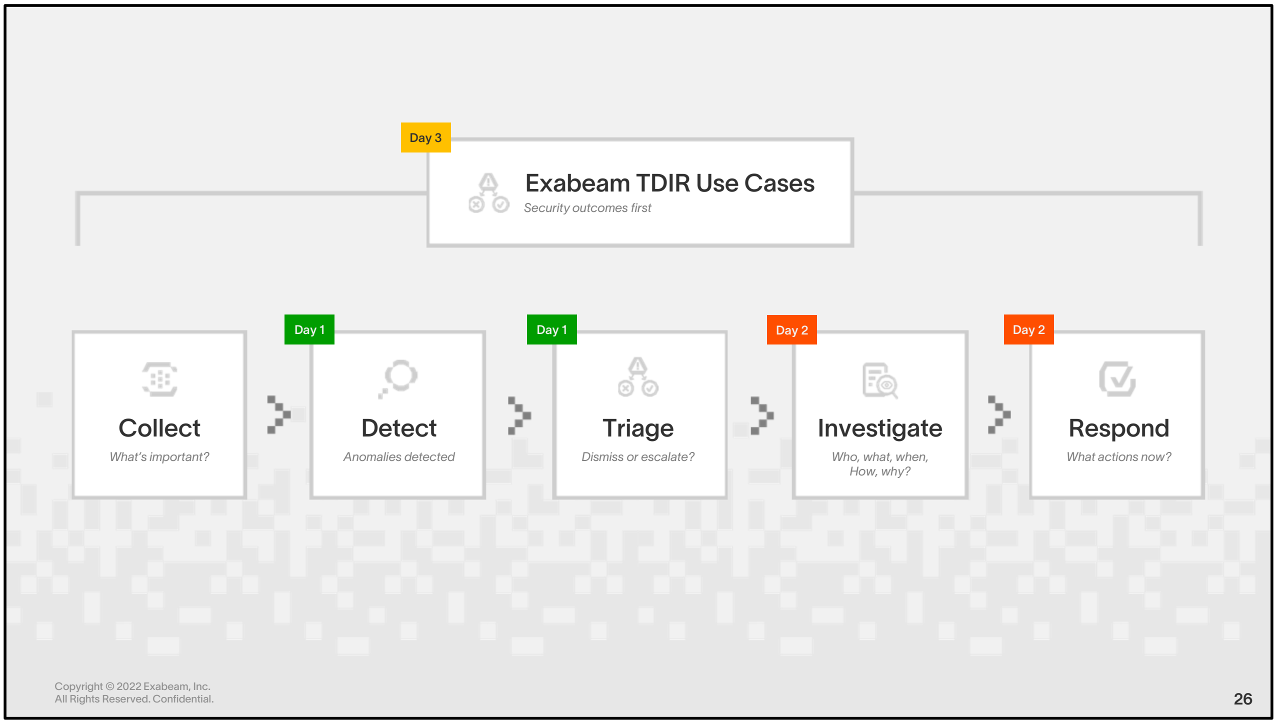
Tier 1 Analyst →

Alert Escalated to Tier 2/3 Analyst

Detection
Accumulating Risk Score

Triage
Security Alerts Reviewed

Incident Diagnostic & Investigation



Day 3

Exabeam TDIR Use Cases

Security outcomes first

Collect

What's important?

Day 1

Detect

Anomalies detected

Day 1

Triage

Dismiss or escalate?

Day 2

Investigate

Who, what, when, How, why?

Day 2

Respond

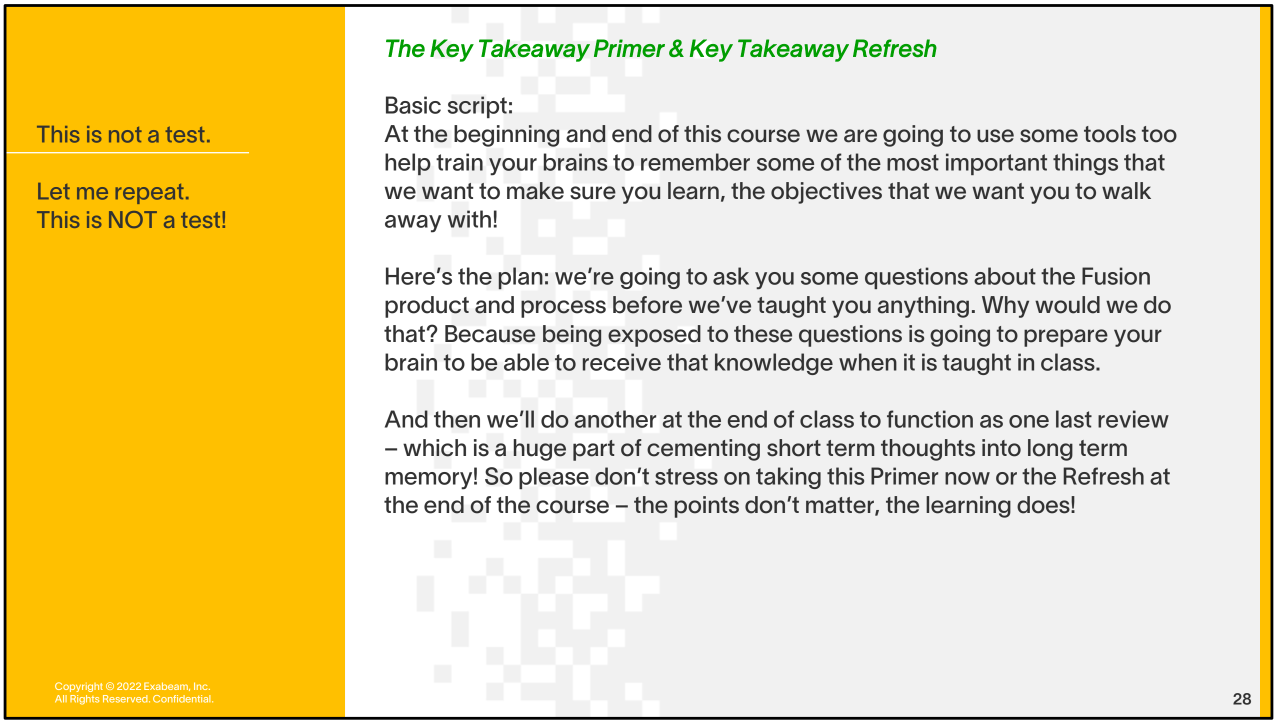
What actions now?

Student Notes

This slide shows how the course content aligns with a typical analytical workflow. This is an estimation, and the actual pace may vary.

Activity

Time for the Key Takeaway Primer!



This is not a test.

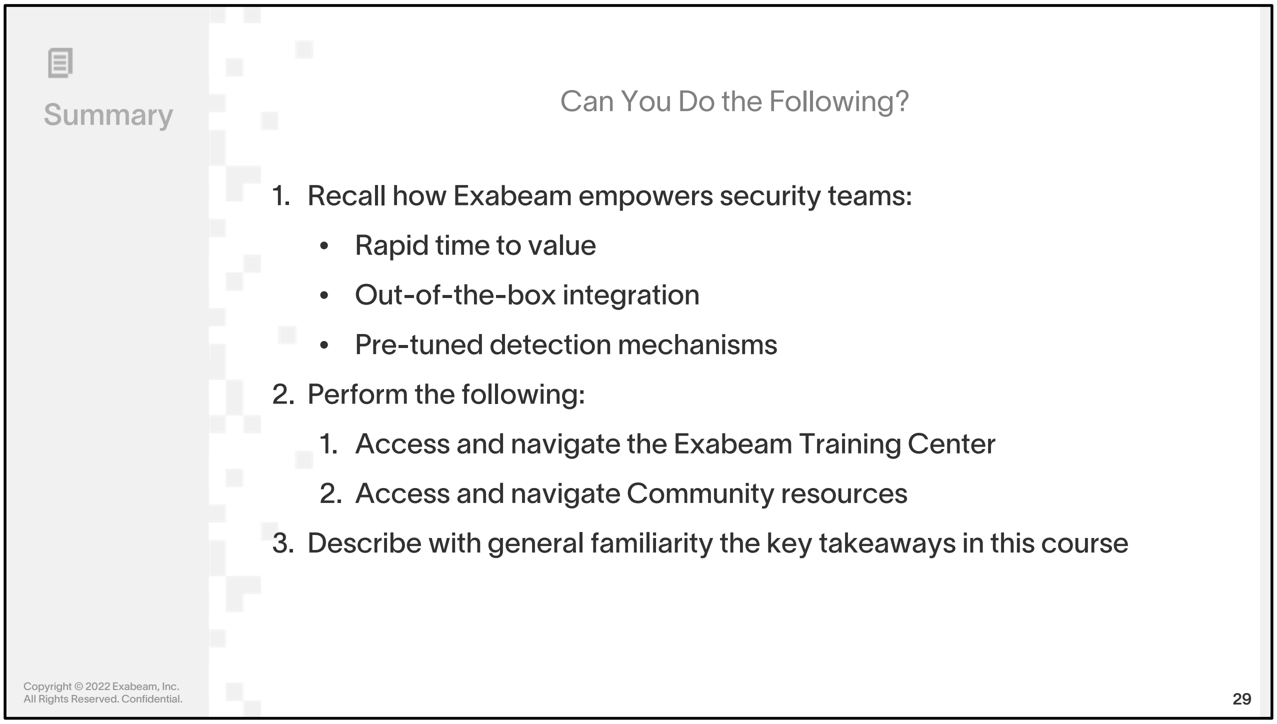
Let me repeat.
This is NOT a test!

The Key Takeaway Primer & Key Takeaway Refresh

Basic script:
At the beginning and end of this course we are going to use some tools too help train your brains to remember some of the most important things that we want to make sure you learn, the objectives that we want you to walk away with!

Here’s the plan: we’re going to ask you some questions about the Fusion product and process before we’ve taught you anything. Why would we do that? Because being exposed to these questions is going to prepare your brain to be able to receive that knowledge when it is taught in class.

And then we’ll do another at the end of class to function as one last review – which is a huge part of cementing short term thoughts into long term memory! So please don’t stress on taking this Primer now or the Refresh at the end of the course – the points don’t matter, the learning does!

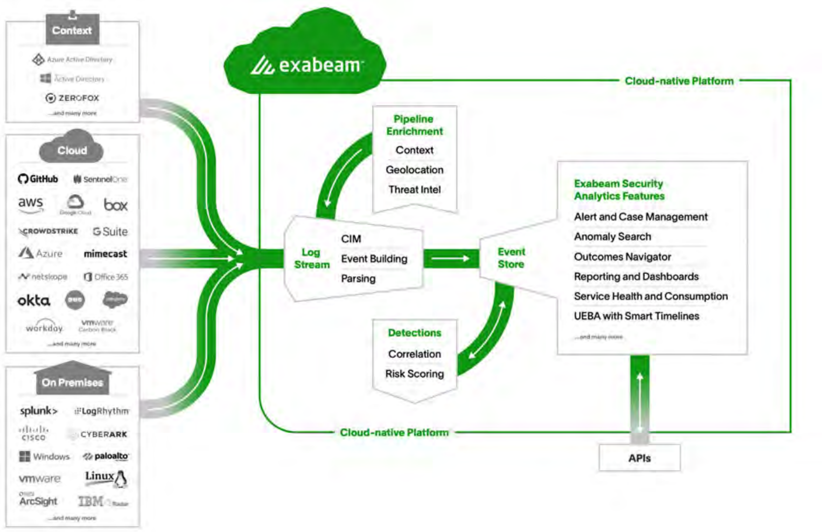


Summary

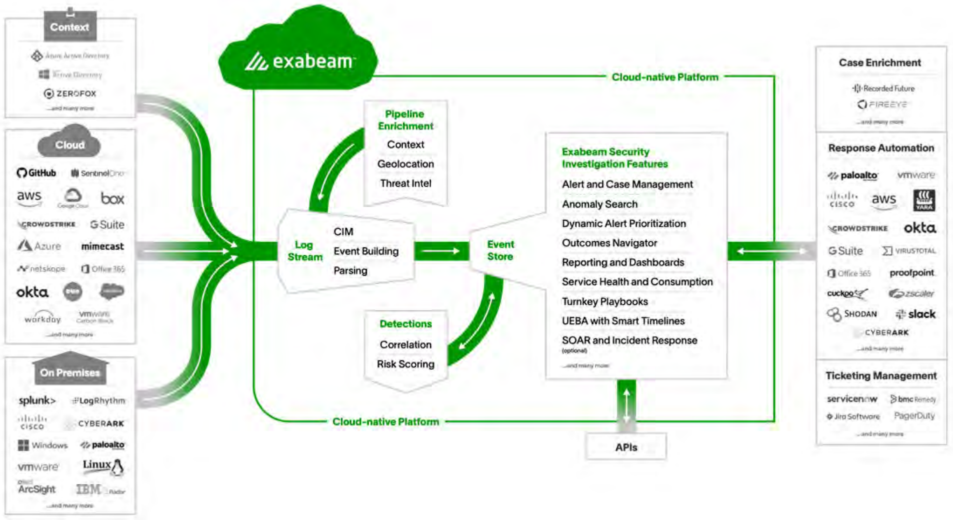
Can You Do the Following?

1. Recall how Exabeam empowers security teams:
   - Rapid time to value
   - Out-of-the-box integration
   - Pre-tuned detection mechanisms
2. Perform the following:
   1. Access and navigate the Exabeam Training Center
   2. Access and navigate Community resources
3. Describe with general familiarity the key takeaways in this course

How **Exabeam Security Analytics** Works



How **Exabeam Security Investigation** Works



Exabeam Security Investigation Features

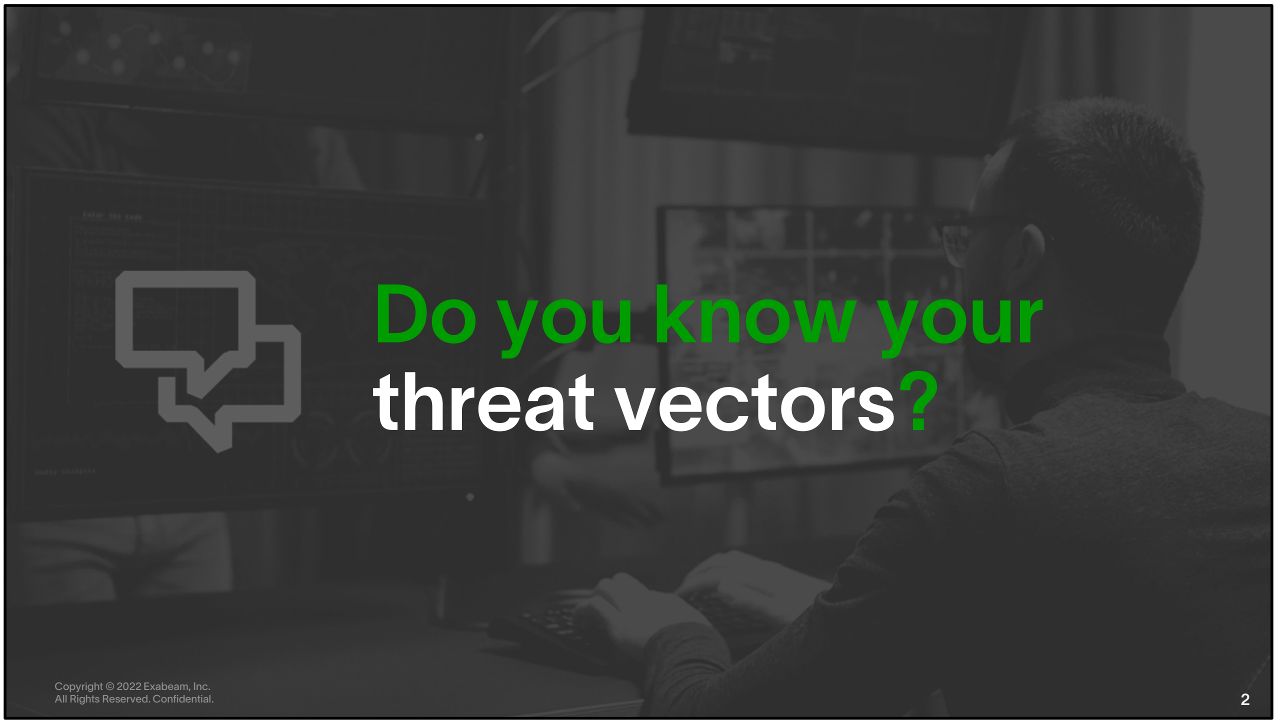
- Alert and Case Management
- Anomaly Search
- Dynamic Alert Prioritization
- Outcomes Navigator
- Reporting and Dashboards
- Service Health and Consumption
- Turnkey Playbooks
- UEBA with Smart Timelines
- SOAR and Incident Response (optional)

...and many more

v4.00

Threat Detection with Exabeam Behavior Analytics

EDU-2170 : Module 2



Do you know your threat vectors?

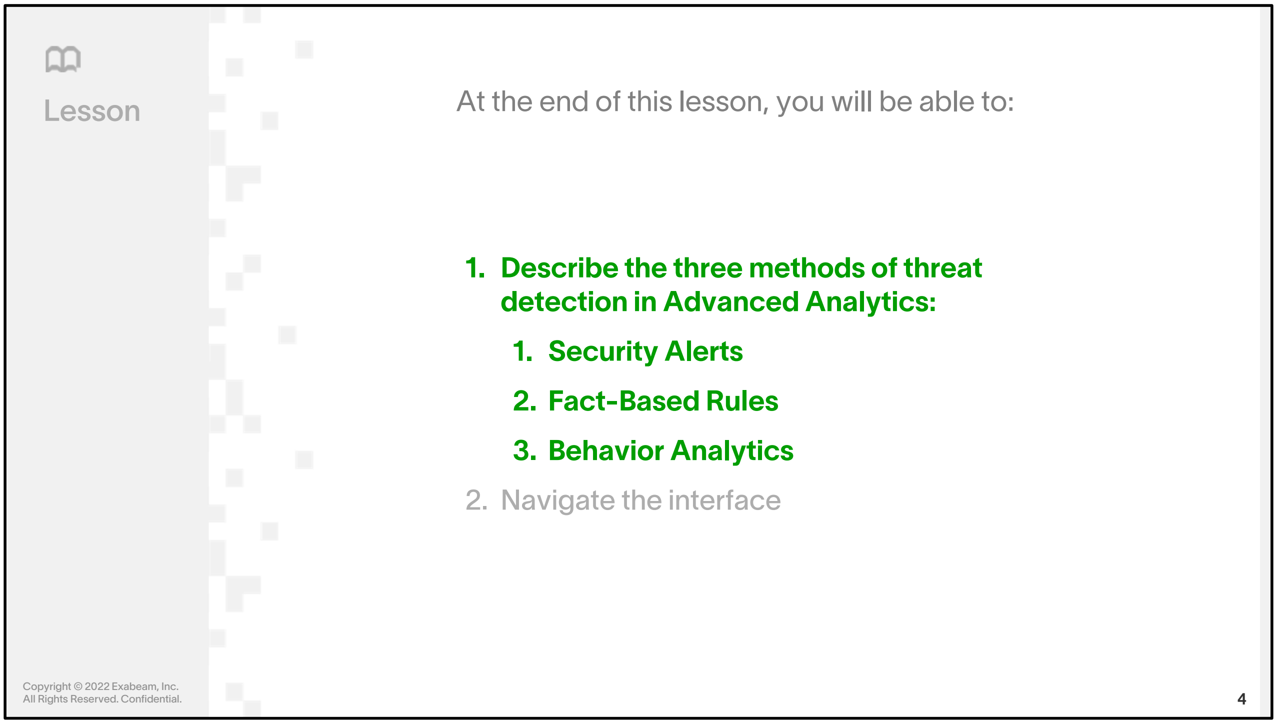
Do you know your most critical assets?

Student Notes

Security often begins with a careful examination and identification of the organizations “crown jewels”. What are the most critical assets – and users! – that you need to safeguard from threats?

Reference:

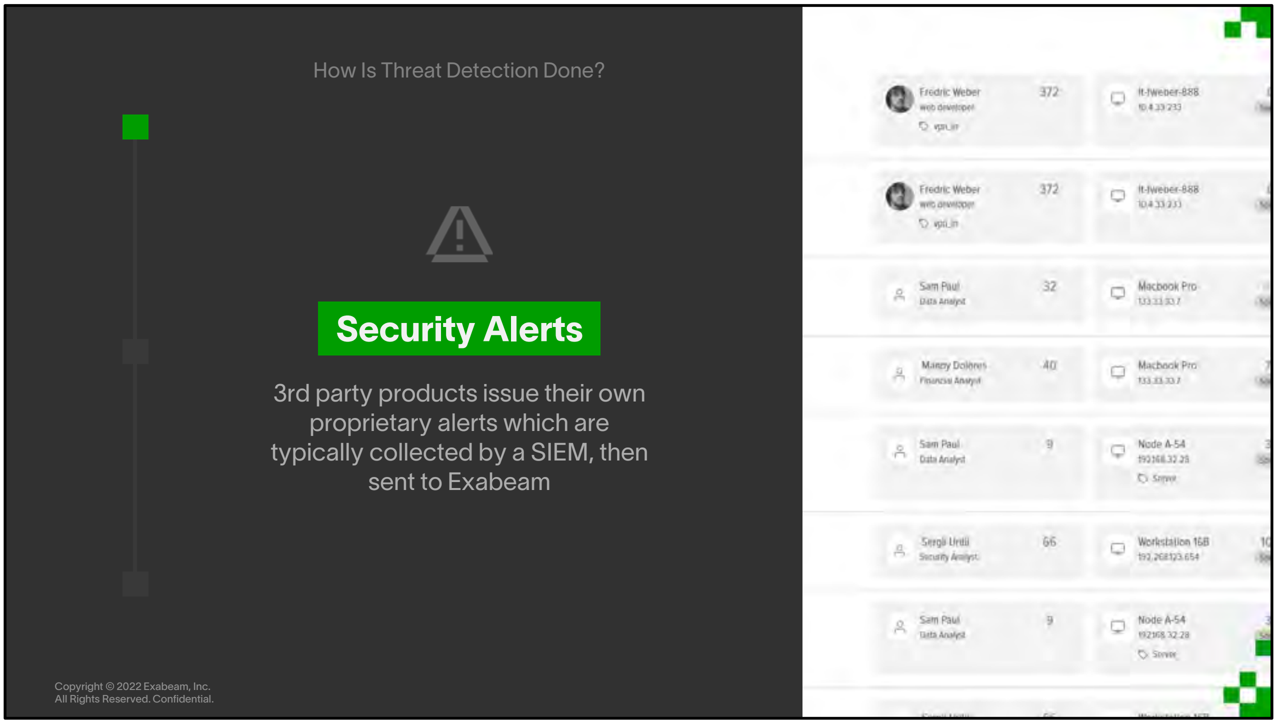
https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis



Lesson

At the end of this lesson, you will be able to:

1. **Describe the three methods of threat detection in Advanced Analytics:**
    1. **Security Alerts**
    2. **Fact-Based Rules**
    3. **Behavior Analytics**
2. Navigate the interface



How Is Threat Detection Done?

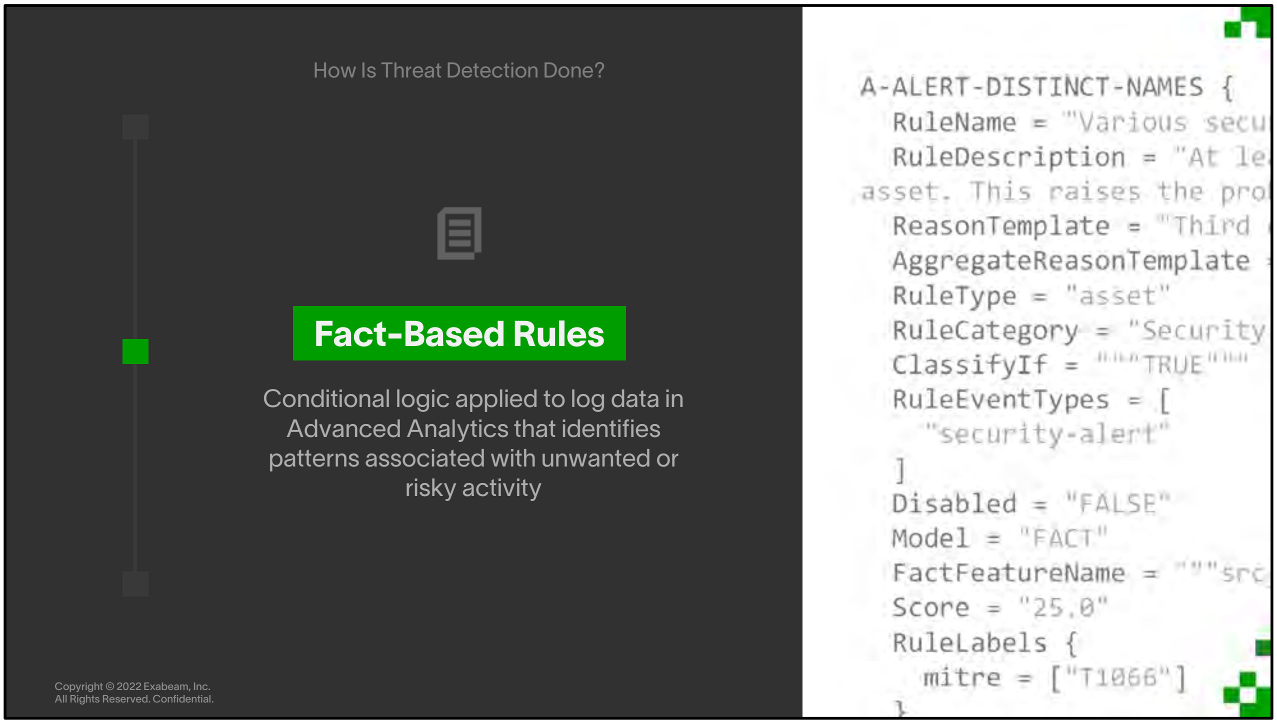
Security Alerts

3rd party products issue their own proprietary alerts which are typically collected by a SIEM, then sent to Exabeam

Student Notes

Security Alerts have many ways of being noticed – directly through consoles and notifications or indirectly through a SIEM or a tool like Exabeam Alert Triage.

Reference:
https://www.exabeam.com/ueba/advanced-analytics-and-mitre-detect-and-stop-threats/



How Is Threat Detection Done?

Fact-Based Rules

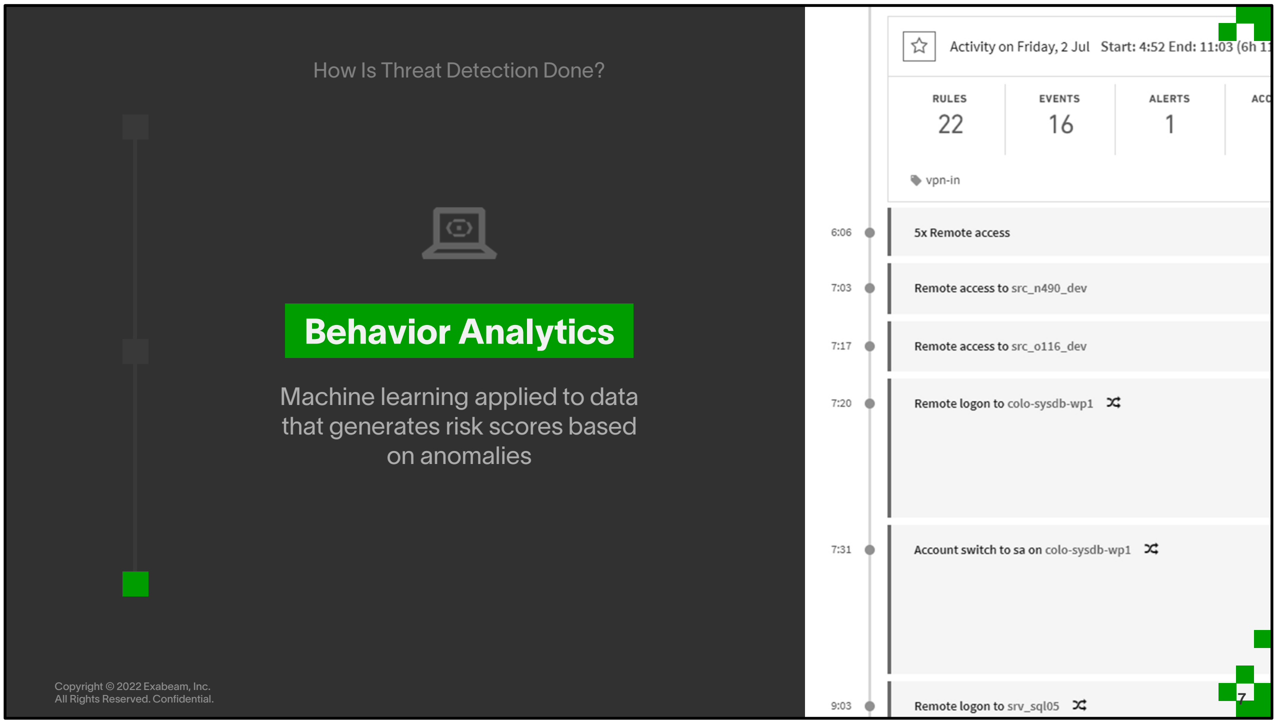
Conditional logic applied to log data in Advanced Analytics that identifies patterns associated with unwanted or risky activity

```
A-ALERT-DISTINCT-NAMES {
  RuleName = "Various secu
  RuleDescription = "At le
asset. This raises the pro
  ReasonTemplate = "Third
  AggregateReasonTemplate
  RuleType = "asset"
  RuleCategory = "Security
  ClassifyIf = """TRUE"""
  RuleEventTypes = [
    "security-alert"
  ]
  Disabled = "FALSE"
  Model = "FACT"
  FactFeatureName = """src
  Score = "25.0"
  RuleLabels {
    mitre = ["T1066"]
  }
```

Student Notes

Fact-based rules are often referred to as correlation rules in a traditional SIEM. Fact-based rules are applied to unwanted activities, risky activities, or even undesired activities, but not necessarily limited to malicious events or behavior.

Reference:
https://www.exabeam.com/ueba/advanced-analytics-and-mitre-detect-and-stop-threats/



How Is Threat Detection Done?

Behavior Analytics

Machine learning applied to data that generates risk scores based on anomalies

Activity on Friday, 2 Jul Start: 4:52 End: 11:03 (6h 11

RULES	EVENTS	ALERTS	ACC
22	16	1	

vpn-in

6:06 5x Remote access

7:03 Remote access to src_n490_dev

7:17 Remote access to src_o116_dev

7:20 Remote logon to colo-sysdb-wp1

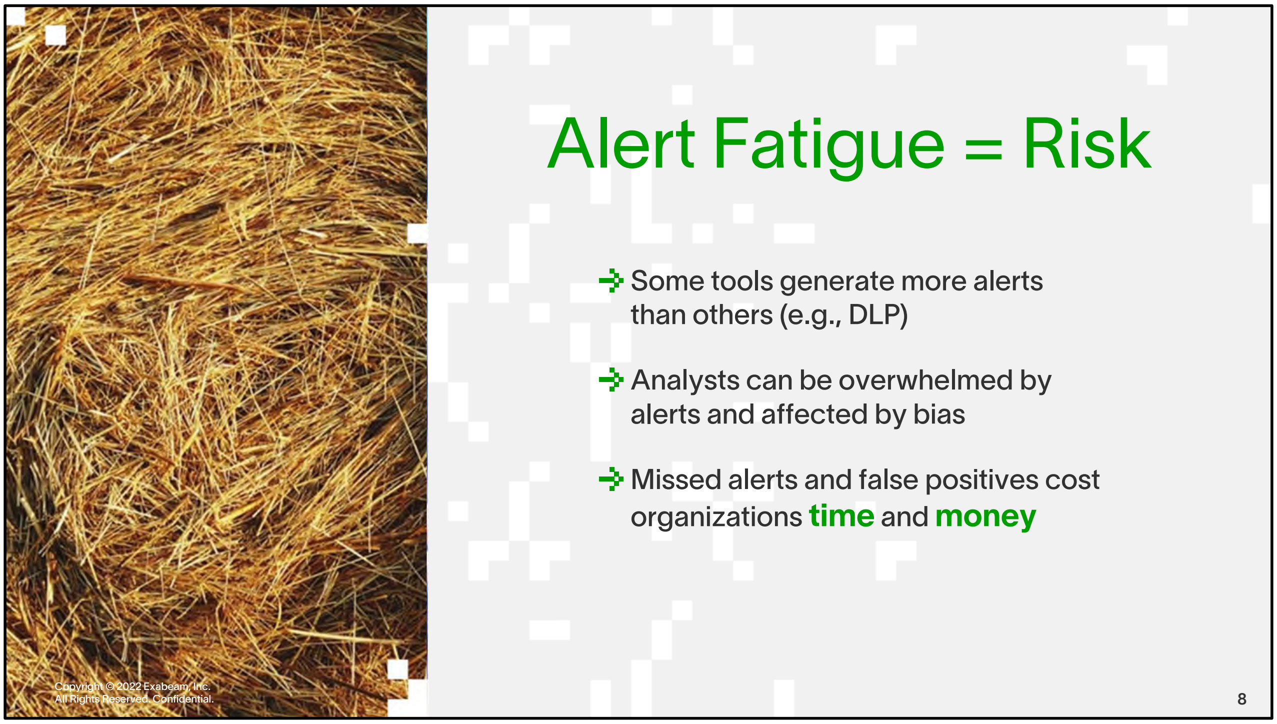
7:31 Account switch to sa on colo-sysdb-wp1

9:03 Remote logon to srv_sql05

Student Notes

Behavior Analytics is a unique way of detecting threats because it does not look for a specific recognizable process or pattern – rather it relies on data modeling to determine normal activity and then triggers anomalies and assigns risk based on these deviations from normal.

Reference:
https://www.exabeam.com/ueba/advanced-analytics-and-mitre-detect-and-stop-threats/



Alert Fatigue = Risk

- Some tools generate more alerts than others (e.g., DLP)
- Analysts can be overwhelmed by alerts and affected by bias
- Missed alerts and false positives cost organizations **time** and **money**

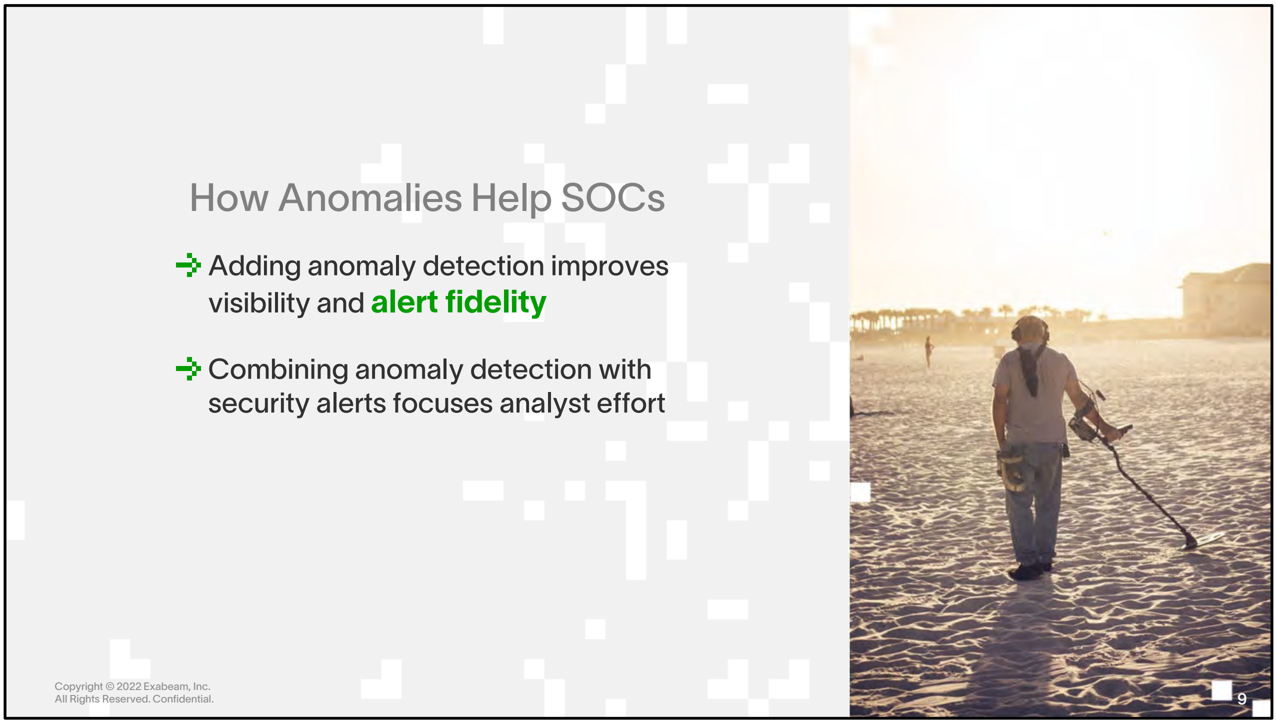
Student Notes

- When asked to identify their top incident response challenges, 36% of the cybersecurity professionals surveyed said, “keeping up with the volume of security alerts.”
- 42% of cybersecurity professionals say that their organization ignores a significant number of security alerts because they can’t keep up with the volume.
- When asked to estimate the percentage of security alerts ignored at their organization, 34% say between 26% and 50%, 20% of cybersecurity professionals say their organization ignores between 50% and 75% of security alerts, and 11% say their organization ignores more than 75% of security alerts. Mama Mia, that’s a lot of security alerts left on the cutting room floor.

Source:
https://www.esg-global.com/blog/dealing-with-overwhelming-volume-of-security-alerts

More Information:
https://www.healthcareitnews.com/news/alert-fatigue-big-problem-cybersecurity-professionals-too
https://www.csoonline.com/article/3191379/false-positives-still-cause-alert-fatigue.html
https://alertops.com/eliminate-alert-fatigue/

{Photo by Lucas Gallone on Unsplash}



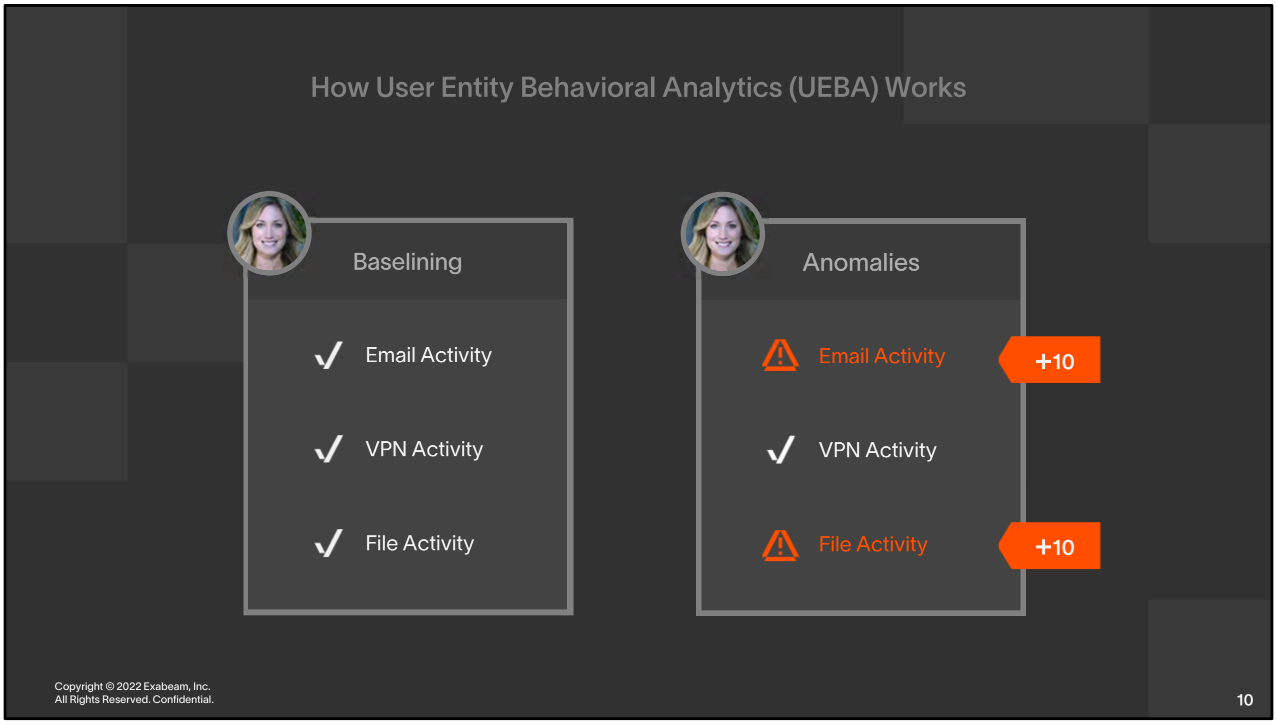
How Anomalies Help SOCs

- Adding anomaly detection improves visibility and **alert fidelity**
- Combining anomaly detection with security alerts focuses analyst effort

Student Notes
Anomaly detection improves detection and increases alert fidelity by showing risky behavior in and around events. Context and meaning are added to third party alerts and focuses analysts allowing them to make critical security decisions.

More Information:
https://www.healthcareitnews.com/news/alert-fatigue-big-problem-cybersecurity-professionals-too
https://www.csoonline.com/article/3191379/false-positives-still-cause-alert-fatigue.html

{Photo by NICO BHLR on Unsplash}



How User Entity Behavioral Analytics (UEBA) Works

Baselining

- ✓ Email Activity
- ✓ VPN Activity
- ✓ File Activity

Anomalies

- ⚠ Email Activity +10
- ✓ VPN Activity
- ⚠ File Activity +10

10

Student Notes

UEBA solutions are based on a concept called baselining. They build profiles that model standard behavior for users, hosts, and devices (called entities) in an IT environment.

Using primarily machine learning techniques, they identify activity that is anomalous, compared to the established baselines, and detect security incidents. The primary advantage of UEBA over traditional security solutions is that it can detect unknown or elusive threats, such as zero-day attacks and insider threats. In addition, UEBA reduces the number of false positives because it adapts and learns actual system behavior, rather than relying on predetermined rules which may not be relevant in the current context.

Source: https://www.exabeam.com/siem-guide/siem-analytics/

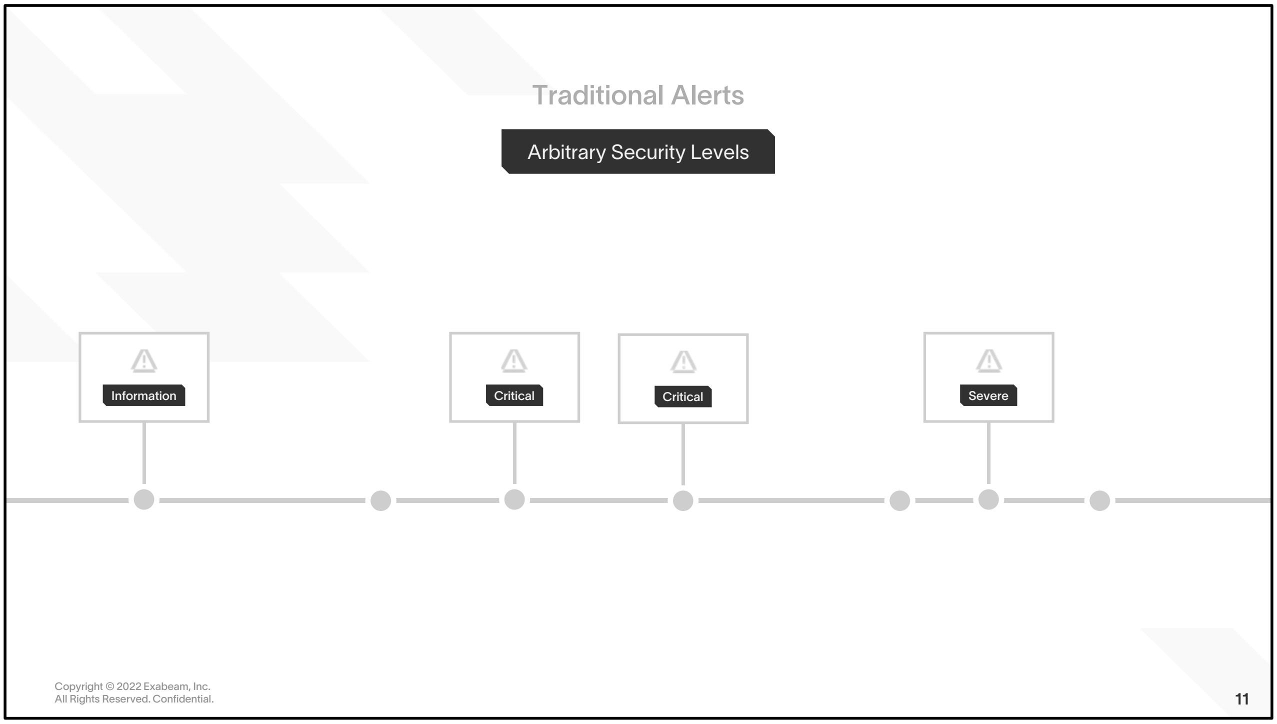
Another term that is sometimes used in conjunction with UEBA is *next-generation SIEM.* In *Gartner's vision* of a next-generation SIEM solution, a SIEM should include built-in UEBA functionality. The report lists the following as critical capabilities of a modern SIEM:

- **User monitoring**, including baselining and advanced analytics to analyze access and authentication data, establish user context, and report on suspicious behavior.
- **Advanced analytics** – applying sophisticated statistical and quantitative models, such as machine learning and deep learning, on security log and event data to detect anomalous activity. Advanced analytics should complement the traditional rule and correlation-based analytics available in traditional SIEMs.

Advanced analytics, which is the hallmark of UEBA tools, involves several modern technologies that can help identify abnormal behavior even in the absence of known patterns:

- **Supervised machine learning** – sets of known good behavior and known bad behavior are fed into the system. The tool learns to analyze new behavior and determine if it is "similar to" the known good or known bad behavior set.
- **Bayesian networks** – can combine supervised machine learning and rules to create behavioral profiles.
- **Unsupervised learning** – the system learns normal behavior and is able to detect and alert on abnormal behavior. It will not be able to tell if the abnormal behavior is good or bad, only that it deviates from normal.
- **Reinforced / semi-supervised machine learning** – a hybrid model where the basis is unsupervised learning, and actual alert resolutions are fed back into the system to allow fine tuning of the model and reduce the signal-to-noise ratio.
- **Deep learning** – enables virtual alert triage and investigation. The system trains on data sets representing security alerts and their triage outcomes, performs self-identification of features, and is able to predict triage outcomes for new sets of security alerts.

Source: https://www.exabeam.com/siem-guide/ueba/



Traditional Alerts

Arbitrary Security Levels

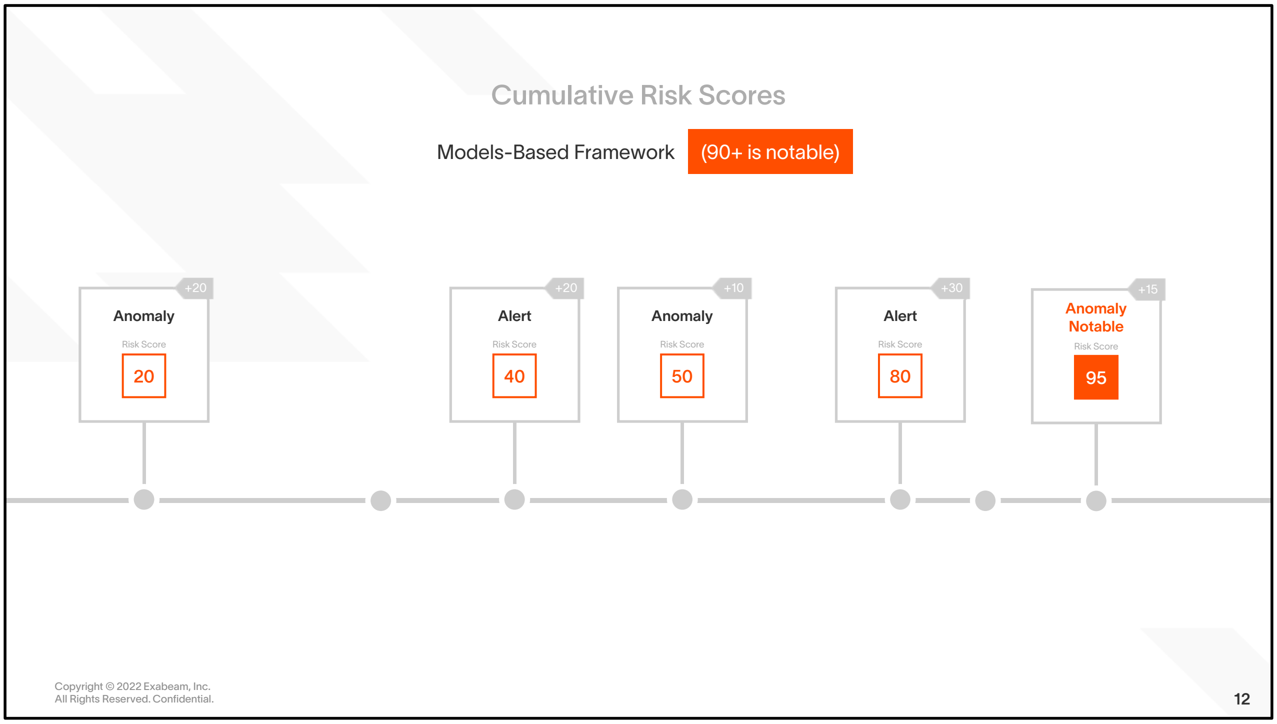
Information

Critical

Critical

Severe

Student Notes
Alerts fire in response to a direct response to a known behavior. Each alert on its own carries its own severity level, which may mean that many low informational level alerts are ignored even though they are a part of the larger picture.



Cumulative Risk Scores

Models-Based Framework (90+ is notable)

+20
Anomaly
Risk Score
20

+20
Alert
Risk Score
40

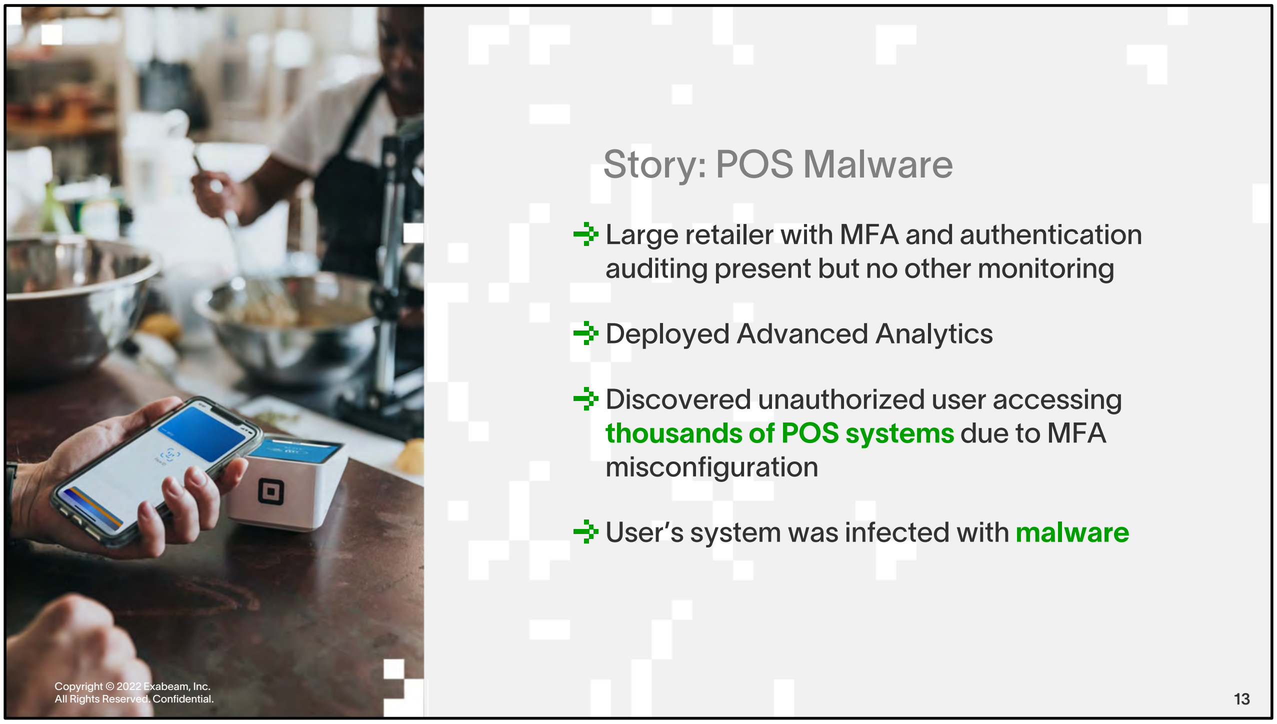
+10
Anomaly
Risk Score
50

+30
Alert
Risk Score
80

+15
Anomaly
Notable
Risk Score
95

Student Notes

Risk scores are assigned based on responses to alerts and other anomalies noticed in a session and are cumulative, allowing for analysts to focus on aggregates rather than individual alerts that are missing context. Anomalies are not as black and white as alerts which is why there is so much value in this aggregation.



Story: POS Malware

- Large retailer with MFA and authentication auditing present but no other monitoring
- Deployed Advanced Analytics
- Discovered unauthorized user accessing **thousands of POS systems** due to MFA misconfiguration
- User’s system was infected with **malware**

{Photo by Nathan Dumlao on Unsplash}

Introducing the

XDR Alliance™

14

Student Notes

XDR Alliance – what?

The XDR Alliance is a group of security technology providers who have organized to help customers more easily define, implement, and operate effective threat detection, investigation, and response (TDIR) programs and technology stacks.

Our mission is to 1) collaborate on value-add, vendor-driven joint integrations and capabilities for the benefit of customers, and 2) promote an open XDR approach through market education and awareness activities.

XDR Alliance – how?

The XDR Alliance is founded on the acknowledgement that:

•Current approaches to SOC are not scaling and will keep failing.

•Tool integration and content development for most use cases is very hard for all but the most mature organizations, and should really be driven by vendors.

•The vendor community is very fragmented, yet vendors are willing and able to come together when duty calls.

Source

https://www.exabeam.com/information-security/introducing-the-xdr-alliance/

Reference

https://www.xdralliance.com/

Two Types of XDR

Native-XDR

Open-XDR

Copyright © 2022 Exabeam, Inc.
All Rights Reserved. Confidential.

15

Student Notes

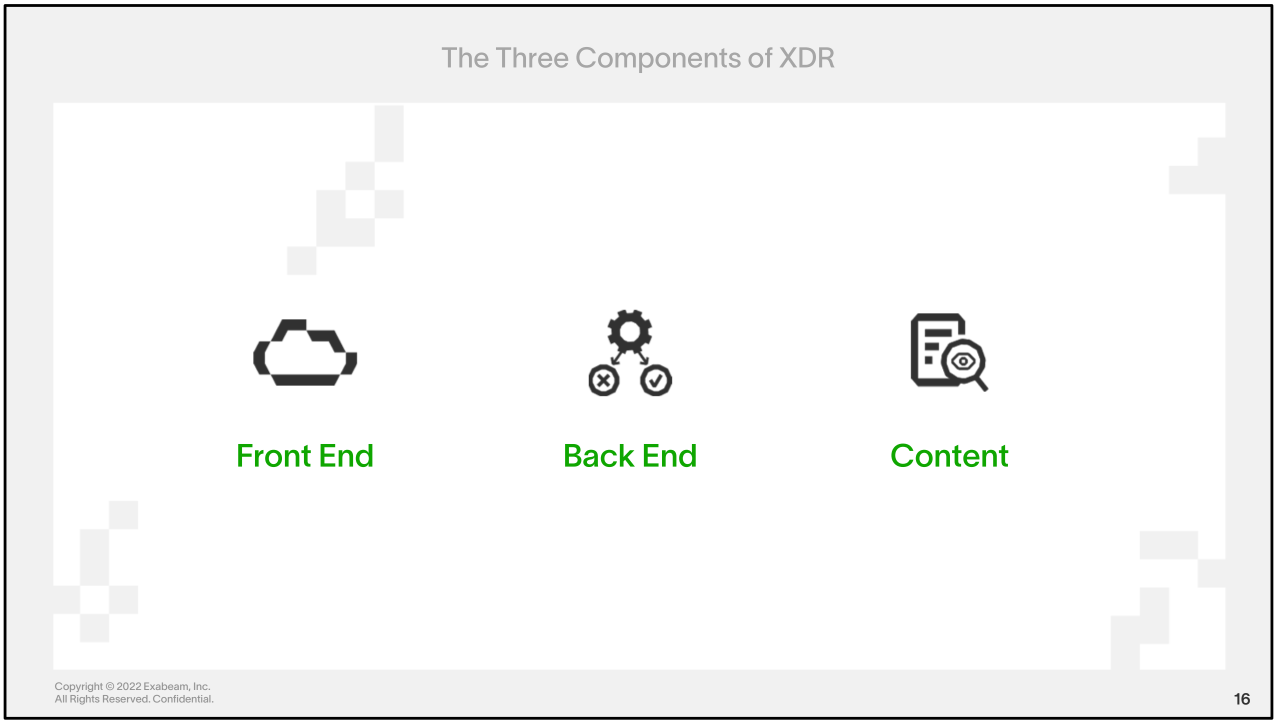
What is a native XDR?
A native XDR is a closed ecosystem that offers both the front-end solutions that generate data as well as the back-end capabilities of analysis and workflow. To be a native XDR solution, a vendor should ideally offer all required sensors needed for common XDR use cases, typically endpoint, network, cloud, identity, email, etc. as well as a back end capable of performing threat detection, investigation, and response with that data. Native XDR vendors can be EDR vendors who are expanding their portfolio to include more sensors and back-end capabilities such as efficient advanced analytics, or they can be platform vendors which have a wide portfolio of security tools that they are trying to more tightly integrate to provide XDR-like functionalities.

What is an open XDR?
Alternatively, open XDR vendors offer a solution that is predominantly focused on the back-end analytics and workflow engine. Leading open XDR vendors also add prescriptive content required across all the phases and the full lifecycle of threat detection, investigation and response (TDIR) to easily solve common SOC use cases out of the box. Open XDRs need to integrate with all of an organization's existing security and IT infrastructure, then correlate and analyze all relevant data, and finally automate and optimize TDIR workflows, making it easier for SOC teams to respond to incidents quicker. As security stacks have grown more complex and disjointed in organizations, open XDRs act as a single control plane across multiple products and vendors. This provides visibility and allows orchestration and automation of actions (similar to SIEM and SOAR functionality) so that SOC teams don't have to run manual workflows across a myriad of tools.

Exabeam's take on XDR
We believe the open XDR approach best positions most security teams for success and reduces their cybersecurity risks. While the native approach may, in theory, offer the major pieces of a security program and the simplicity of a single vendor, we believe this will inevitably lead to vendor lock-in and a lack of depth and breadth of coverage for organizations. Security teams will find it difficult to get best-in-class capabilities across email, DLP, identity, cloud all from a single vendor.

In addition, organizations selecting a native XDR may find it very difficult to add a security tool from another vendor that covers a new attack vector or more advanced threats. Because native XDRs are usually focused on their own portfolio, little to no capabilities and support exist to efficiently integrate with sensors from other infosec tools. The flexibility offered by an open XDR allows security teams to keep existing investments in best-of-breed security tools while allowing desired changes to their tech stack. Open XDRs are made to integrate with other products — so they can comprehensively take all information and combine weak signals from multiple products to find complex threats missed by other tools.

Source
https://www.exabeam.com/information-security/open-versus-native-xdr/



The Three Components of XDR

Front End

Back End

Content

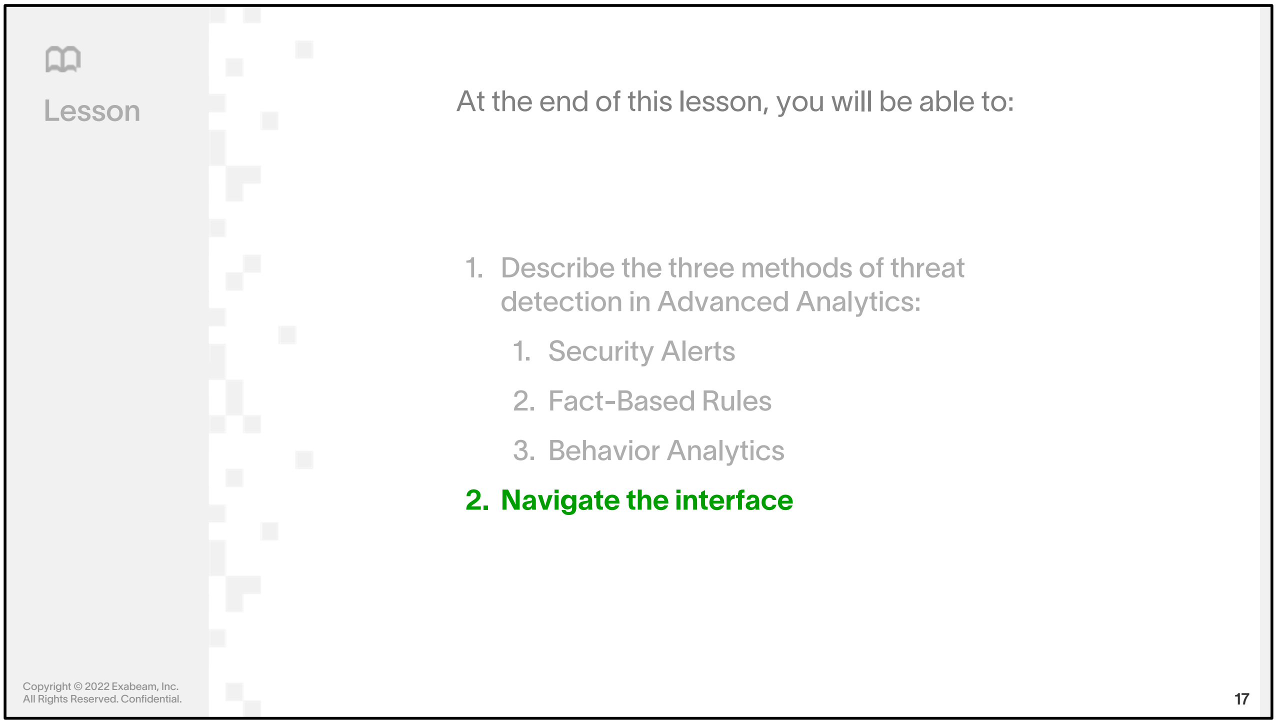
Student Notes

XDR is typically made up of three major feature sets: front end, back end and content. The front end consists of the “sensors” that generate security telemetry data, like CASBs, EDRs, IAM, DLP solutions, and others. The back end ingests all the collected telemetry data, logs and context information, then conducts all the data correlation, advanced analytics, threat detection, investigation, tool orchestration, and response automation.

The third critical component of any successful XDR is content. XDRs should be able to offer a closed-loop solution that encompasses the entire security operations workflows of threats. XDRs are supposed to be turnkey solutions with immediate time to value and minimum/no configuration, regardless of the expertise level of the SOC — so instead of tuning, SOCs should be able to use XDRs to address immediate concerns from start to finish. By this, we mean focusing on one use case and expanding from thereafter each one is addressed. Without this capability, XDRs will not be able to fulfill their value prop: turn-key TDIR that works immediately, without customization.

Without prescriptive, prepackaged content that ties these pieces together around specific use cases, it’s impossible to achieve the value props of simplicity, automation, and successful outcomes that XDR promises.

Source
https://www.exabeam.com/information-security/open-versus-native-xdr/
https://www.exabeam.com/information-security/an-xdr-prerequisite-prescriptive-threat-centric-use-cases/



Lesson

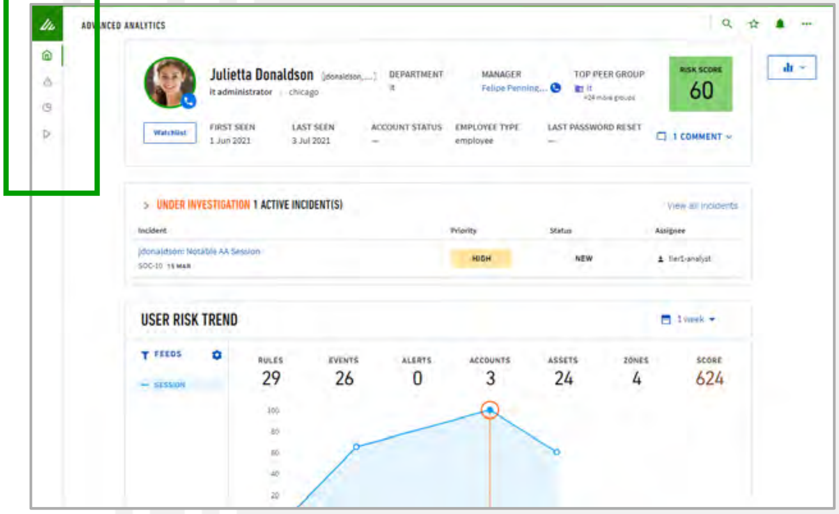
At the end of this lesson, you will be able to:

1. Describe the three methods of threat detection in Advanced Analytics:
   1. Security Alerts
   2. Fact-Based Rules
   3. Behavior Analytics
2. **Navigate the interface**

Demo

Touring the Interface

NEW



ADVANCED ANALYTICS

Julietta Donaldson [jdonaldson,...]
it administrator | chicago

DEPARTMENT	MANAGER	TOP PEER GROUP	RISK SCORE
it	Felipe Penning...	it +24 more groups	60

Watchlist

FIRST SEEN	LAST SEEN	ACCOUNT STATUS	EMPLOYEE TYPE	LAST PASSWORD RESET
1 Jun 2021	3 Jul 2021	—	employee	—

1 COMMENT

> UNDER INVESTIGATION 1 ACTIVE INCIDENT(S)

View all incidents

Incident	Priority	Status	Assignee
jdonaldson: Notable AA Session SOC-10 15 MAR	HIGH	NEW	tier1-analyst

USER RISK TREND

1 week

FEEDS

SESSION

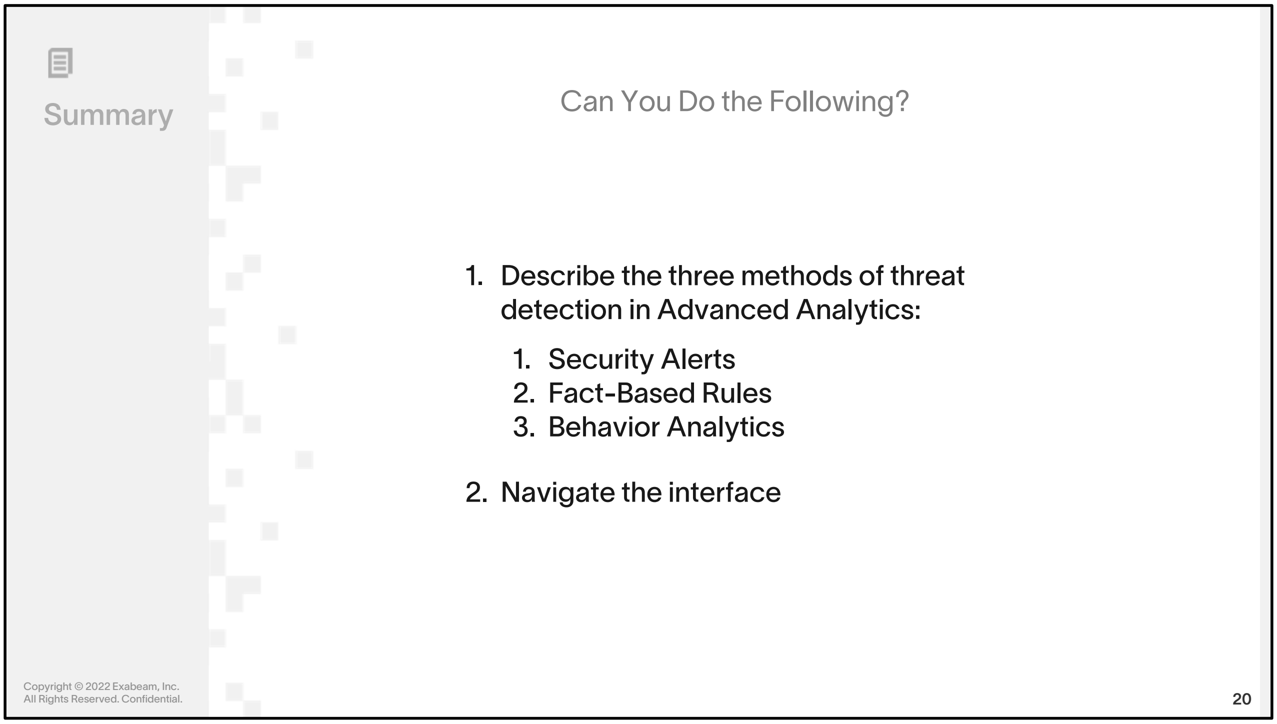
RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES	SCORE
29	26	0	3	24	4	624

Activity

EXPLORE ADVANCED ANALYTICS

Objectives:

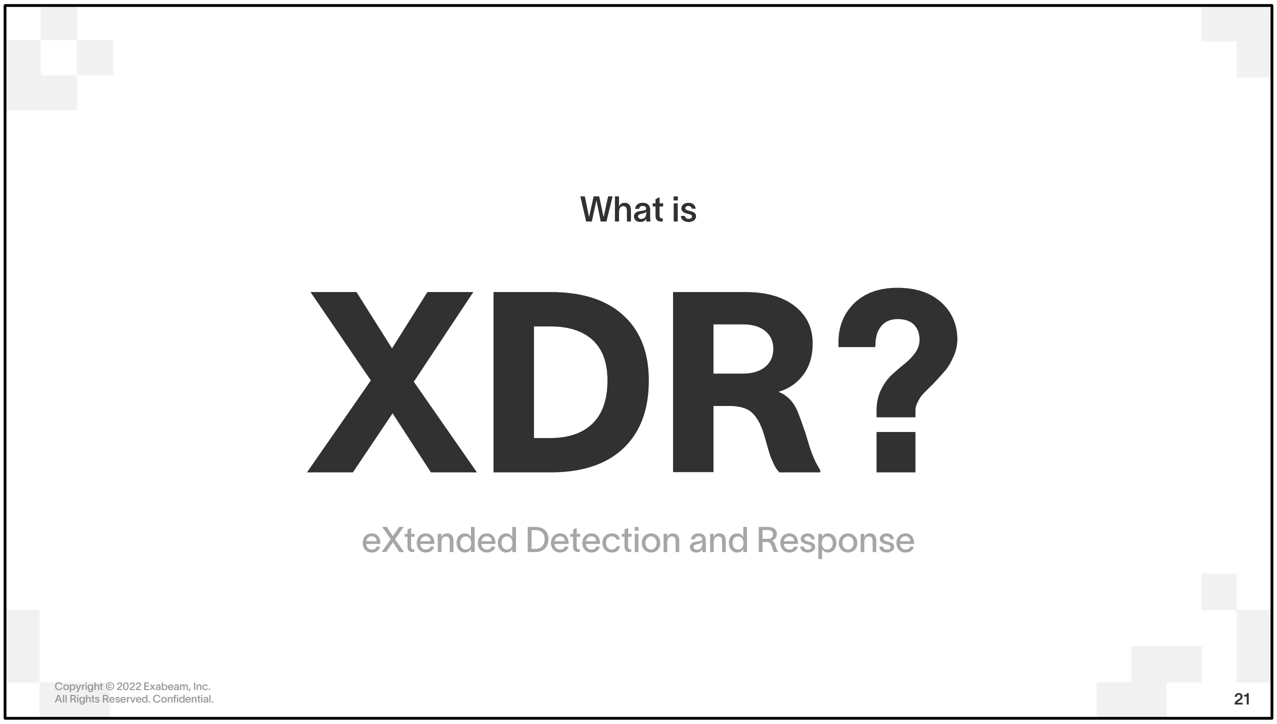
1. Become familiar with the Advanced Analytics home page, user and entity profile pages, Risk reasons, and the Smart Timeline™



Summary

Can You Do the Following?

1. Describe the three methods of threat detection in Advanced Analytics:
    1. Security Alerts
    2. Fact-Based Rules
    3. Behavior Analytics
2. Navigate the interface



What is

XDR?

eXtended Detection and Response

Student Notes

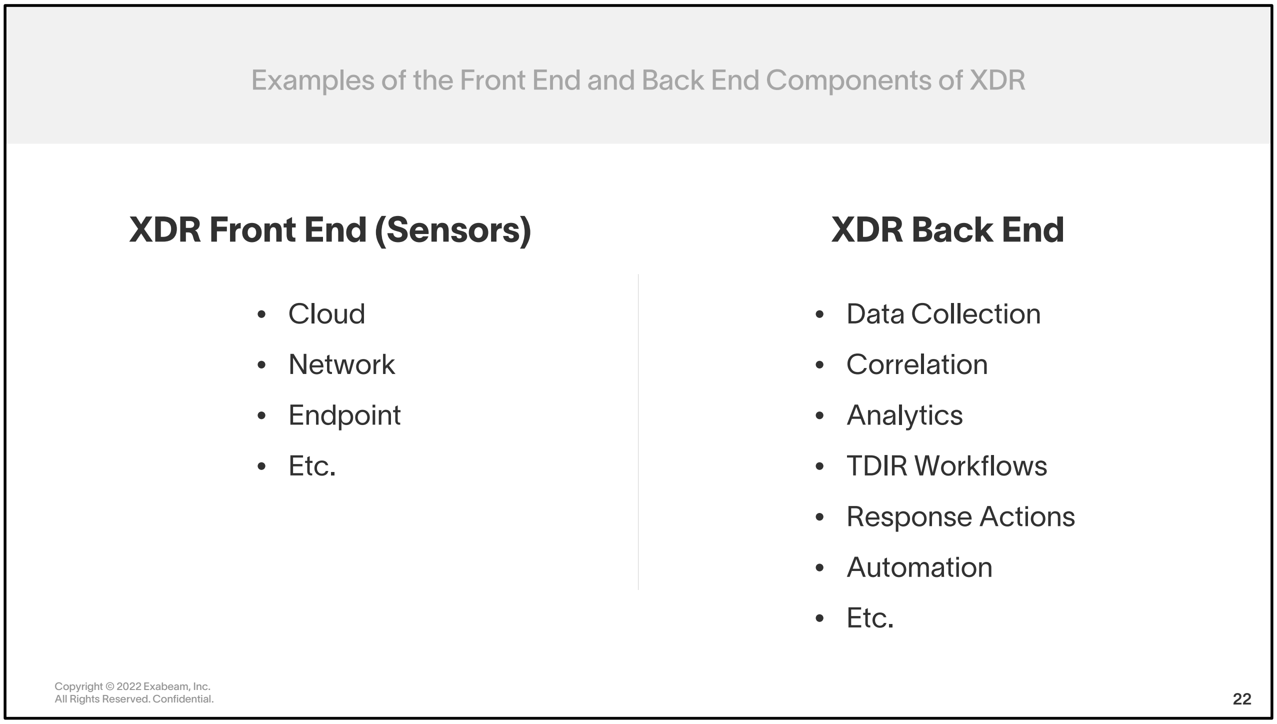
XDR is a set of technologies that can help security teams perform more effective threat detection, as well as rapid investigation and response.

Unlike previous-generation security solutions, XDR is not limited to one security silo — it combines data from networks, endpoints, email, IoT devices, servers, cloud workloads, and identity systems. It combines data from all layers of the IT environment, and enriches them with threat intelligence, to detect sophisticated and evasive threats.

A primary value of XDR is that it provides prepackaged, automated threat detection, investigation and response (TDIR) for a variety of threats. XDR solutions are cloud delivered, suited for distributed, heterogeneous IT environments. They are turn-key solutions that immediately provide value and improve productivity for security teams.

Source

https://www.exabeam.com/information-security/what-is-xdr-transforming-threat-detection-and-response/



Examples of the Front End and Back End Components of XDR

XDR Front End (Sensors)

- Cloud
- Network
- Endpoint
- Etc.

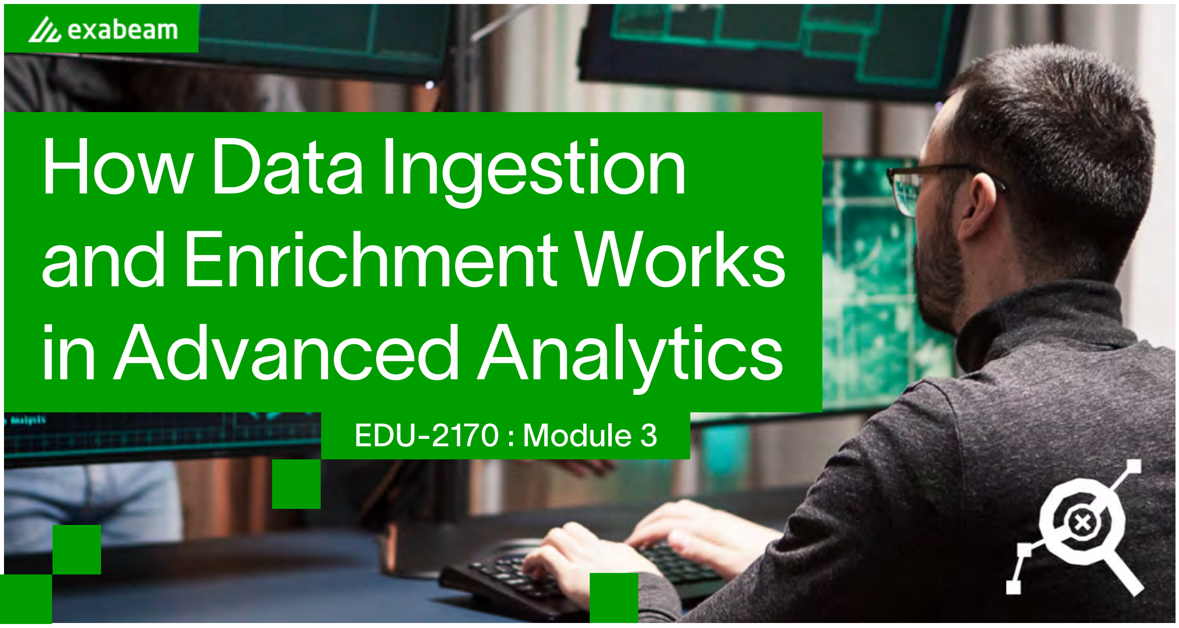
XDR Back End

- Data Collection
- Correlation
- Analytics
- TDIR Workflows
- Response Actions
- Automation
- Etc.

Student Notes

Source
https://www.exabeam.com/information-security/an-xdr-prerequisite-prescriptive-threat-centric-use-cases/

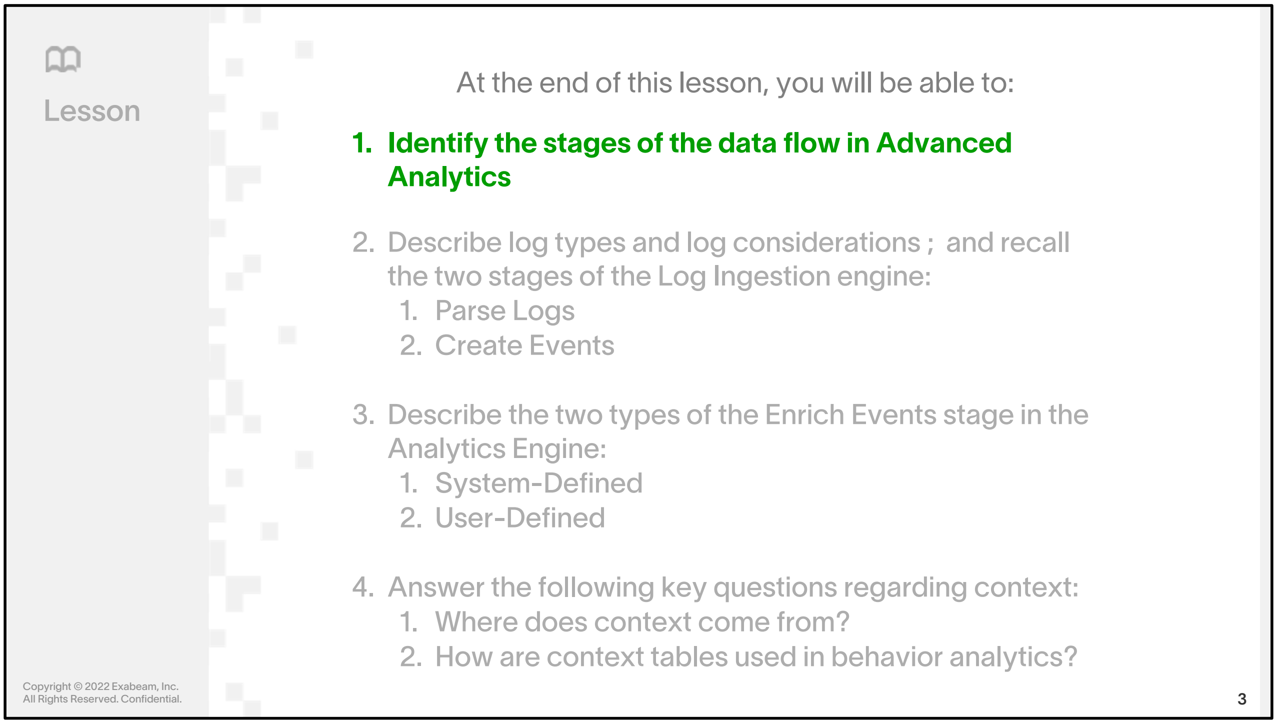
v4.00



How Data Ingestion and Enrichment Works in Advanced Analytics

EDU-2170 : Module 3

When investigating a threat, how do you gain context?



Lesson

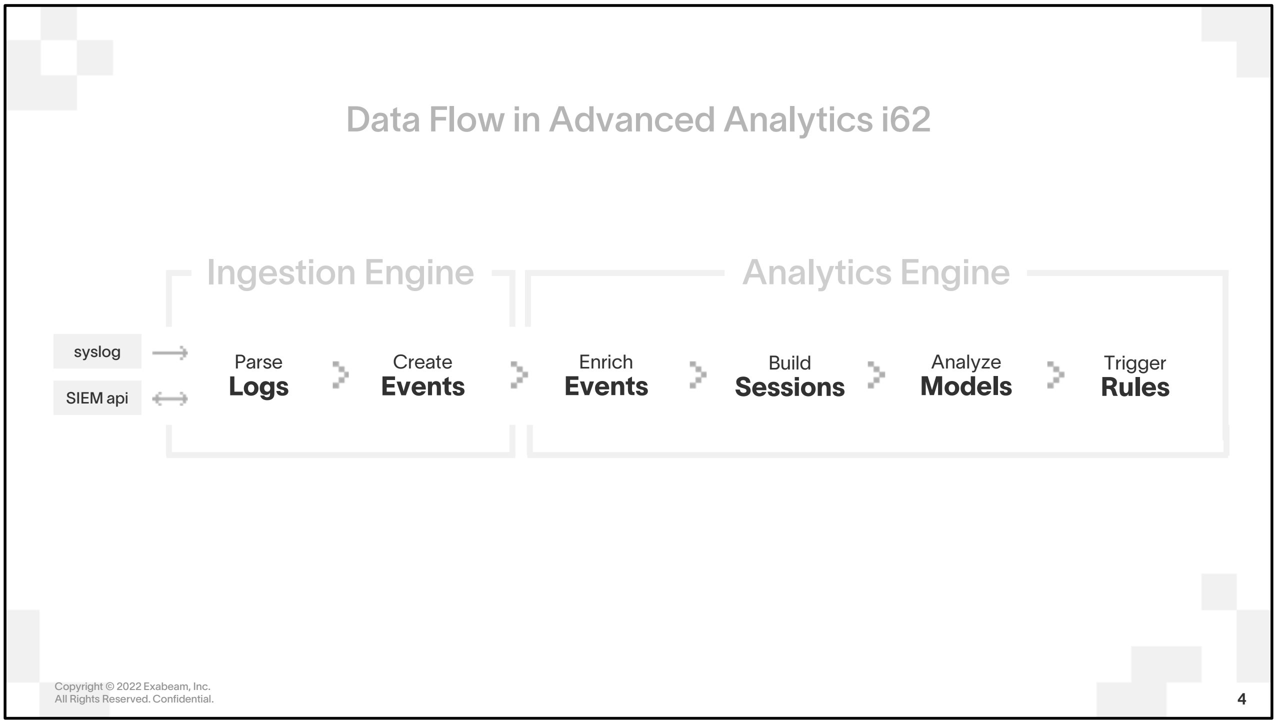
At the end of this lesson, you will be able to:

1. **Identify the stages of the data flow in Advanced Analytics**

2. Describe log types and log considerations ; and recall the two stages of the Log Ingestion engine:
   1. Parse Logs
   2. Create Events

3. Describe the two types of the Enrich Events stage in the Analytics Engine:
   1. System-Defined
   2. User-Defined

4. Answer the following key questions regarding context:
   1. Where does context come from?
   2. How are context tables used in behavior analytics?



Data Flow in Advanced Analytics i62

Ingestion Engine

Analytics Engine

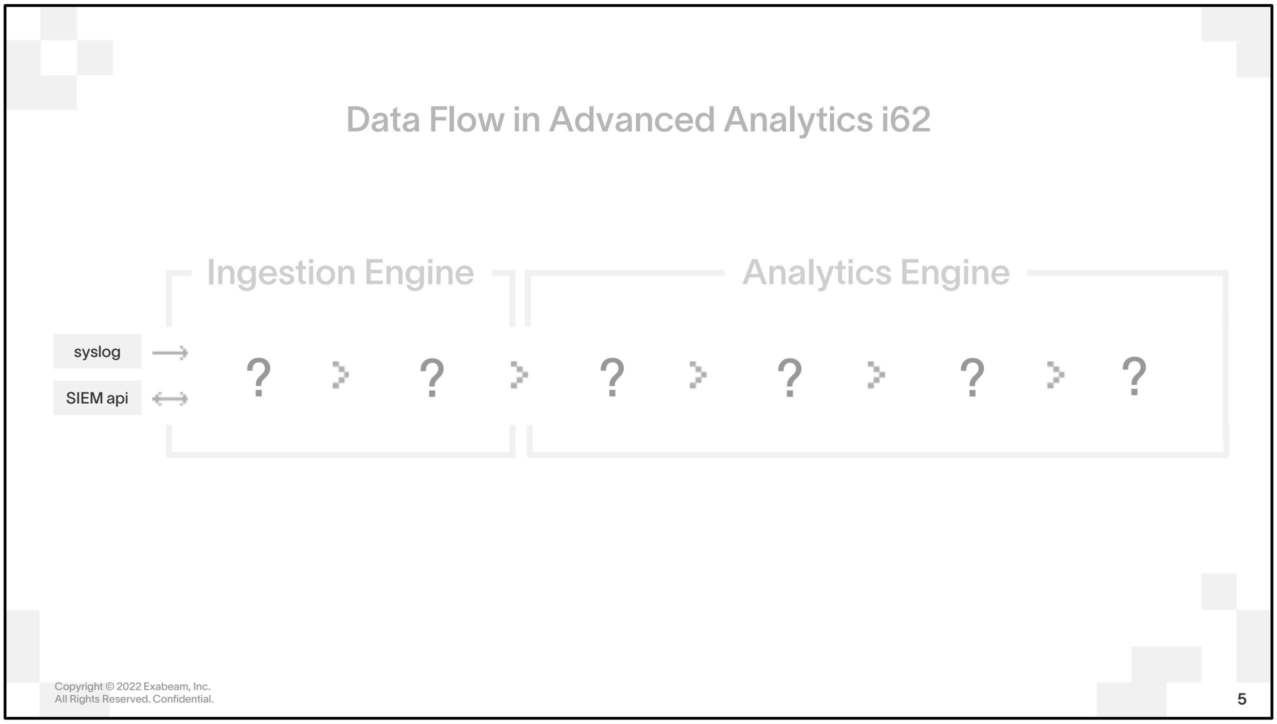
syslog

SIEM api

Parse **Logs** > Create **Events** > Enrich **Events** > Build **Sessions** > Analyze **Models** > Trigger **Rules**

Student Notes

In order to identify risky behavior from normal data Advanced Analytics uses several different processing engines to massage the mountain of raw data.



Data Flow in Advanced Analytics i62

Ingestion Engine

Analytics Engine

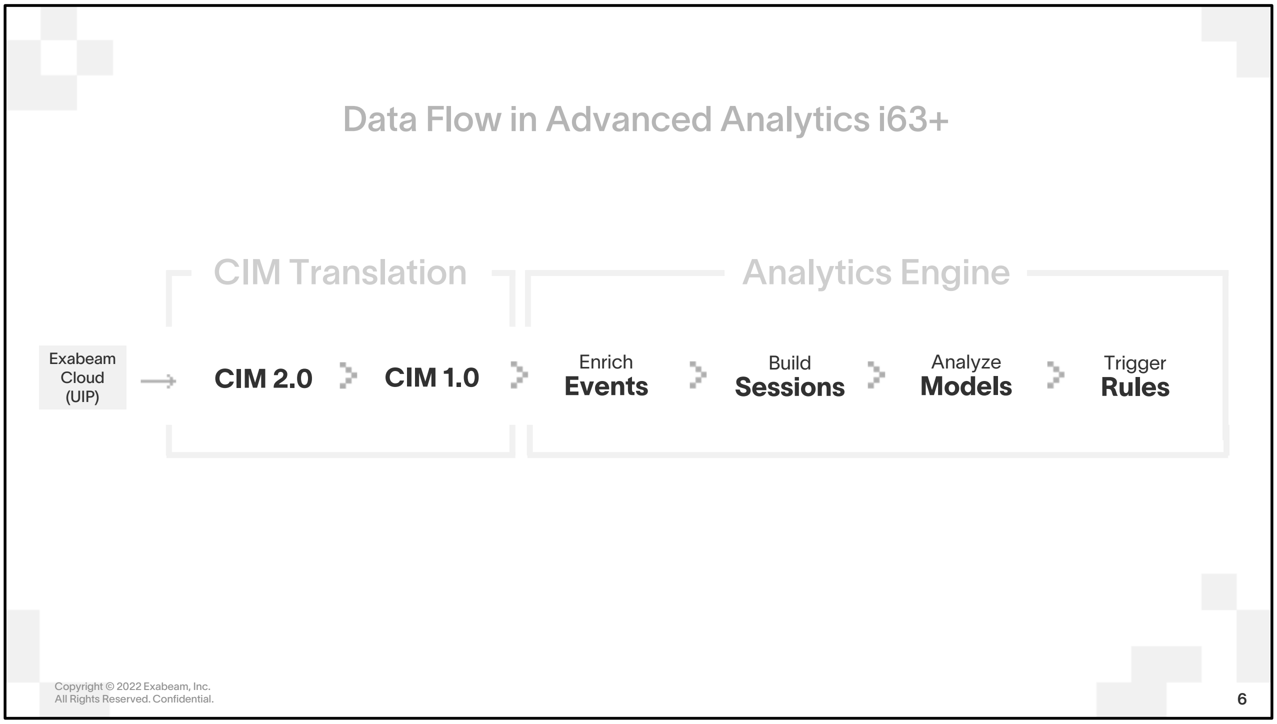
syslog

SIEM api

? › ? › ? › ? › ? › ?

Student Notes

In order to identify risky behavior from normal data Advanced Analytics uses several different processing engines to massage the mountain of raw data

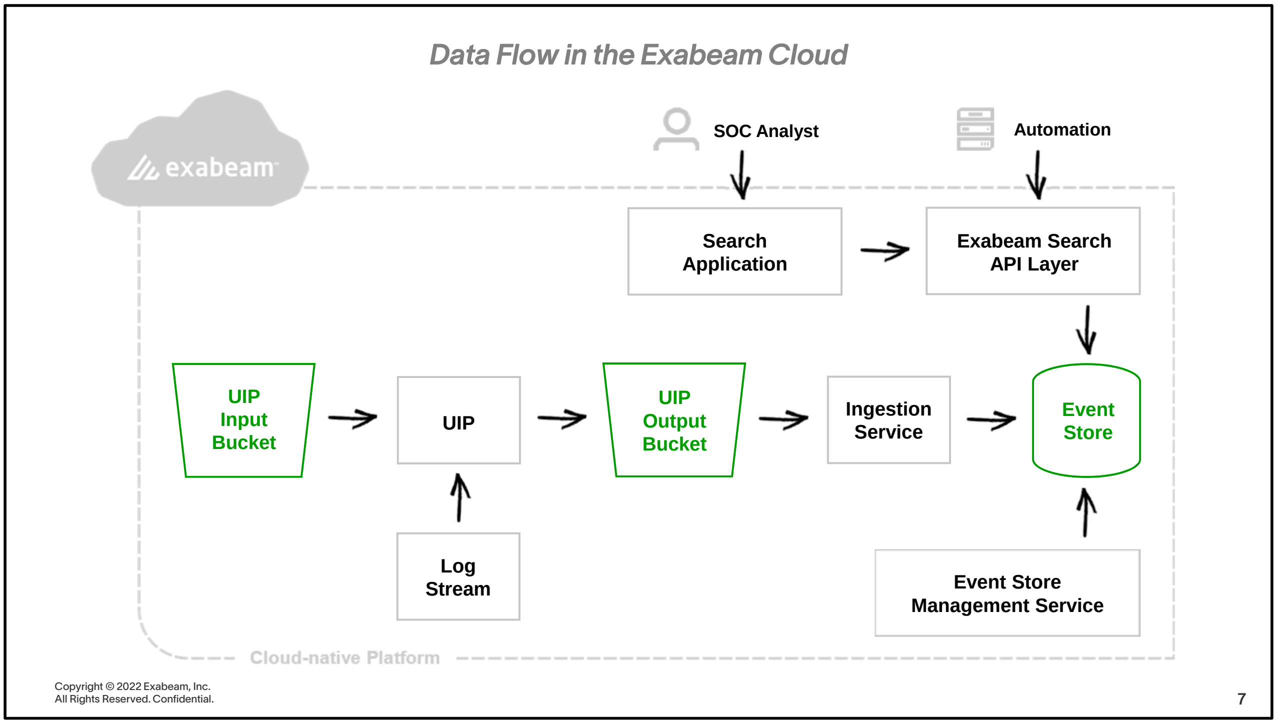


Data Flow in Advanced Analytics i63+

Exabeam Cloud (UIP) → CIM 2.0 > CIM 1.0 > Enrich **Events** > Build **Sessions** > Analyze **Models** > Trigger **Rules**

CIM Translation

Analytics Engine



Data Flow in the Exabeam Cloud

exabeam

SOC Analyst

Automation

Search Application

Exabeam Search API Layer

UIP Input Bucket

UIP

UIP Output Bucket

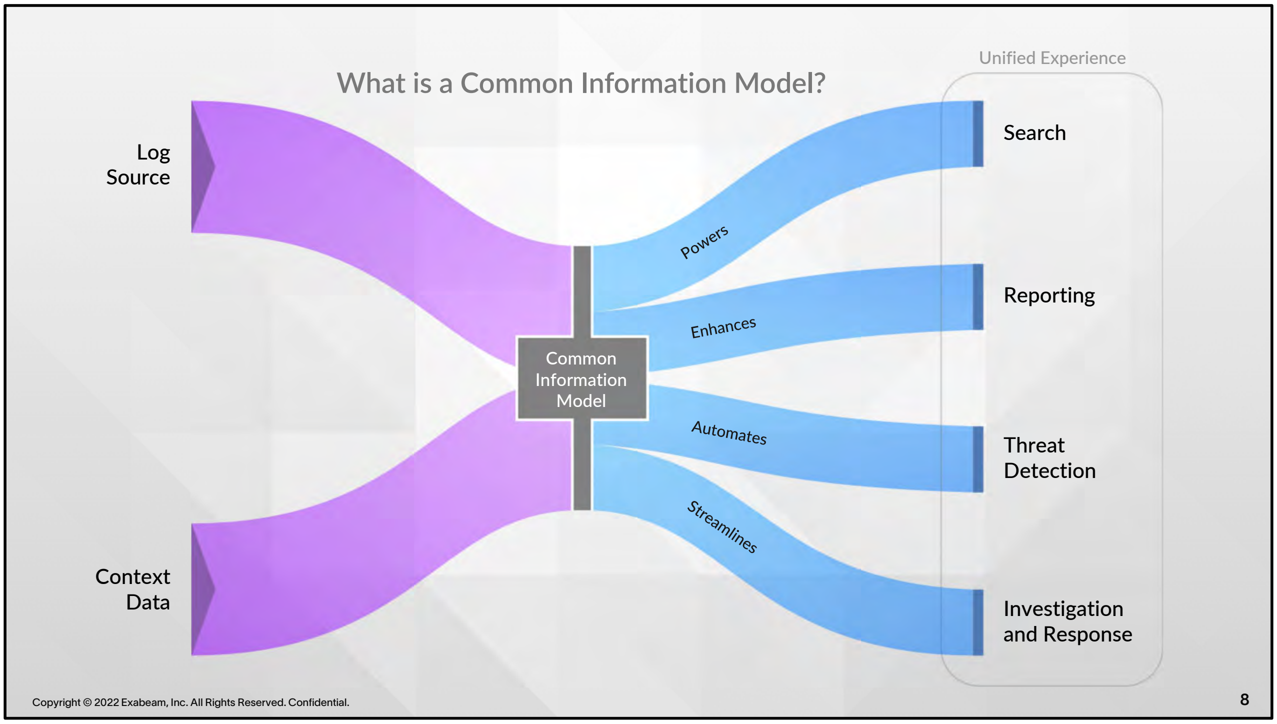
Ingestion Service

Event Store

Log Stream

Event Store Management Service

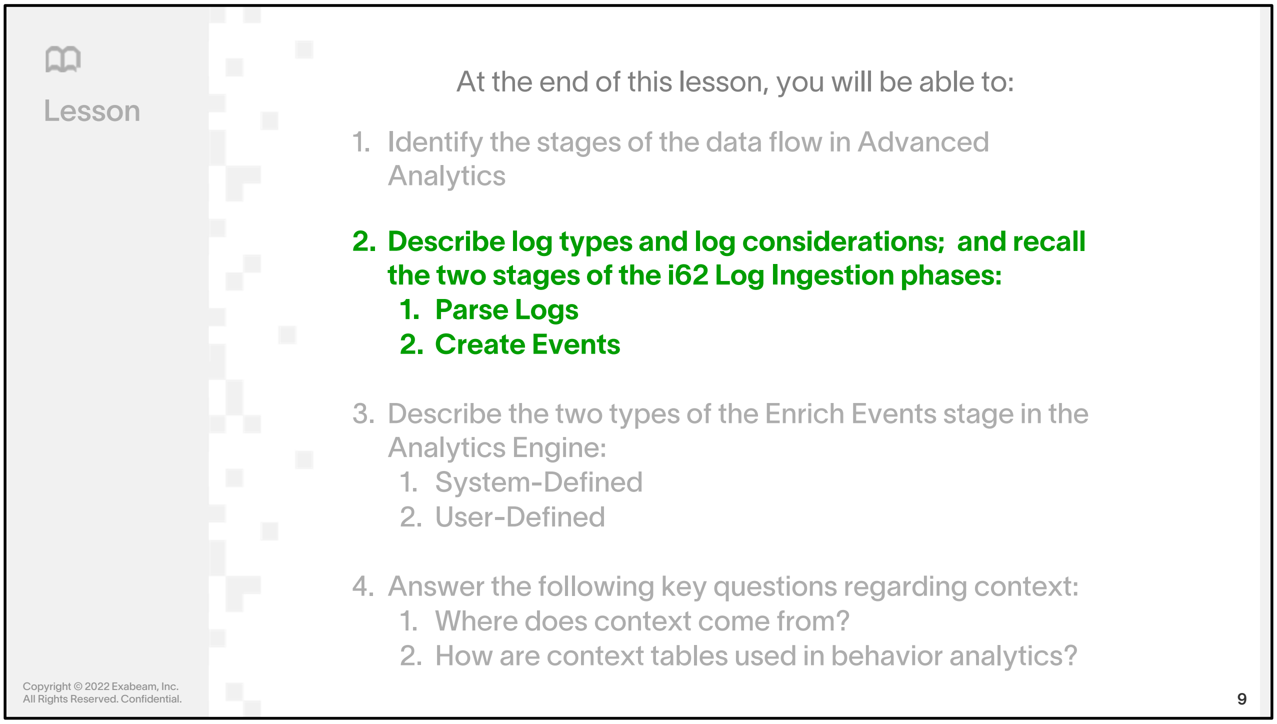
Cloud-native Platform



What is a Common Information Model?

8

References
https://exabeam.atlassian.net/wiki/spaces/TR/pages/2417722301/CIM+2.0+-+Framework+Background+Guiding+Principles



Lesson

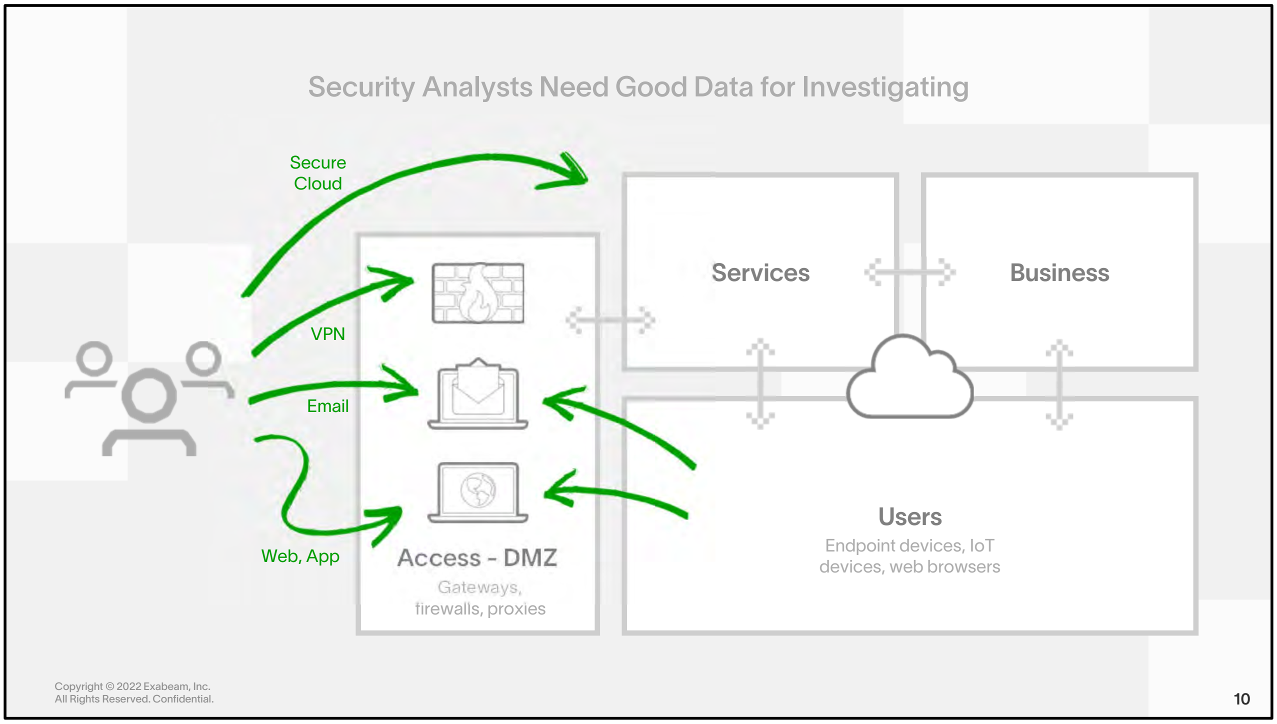
At the end of this lesson, you will be able to:

1. Identify the stages of the data flow in Advanced Analytics

2. **Describe log types and log considerations; and recall the two stages of the i62 Log Ingestion phases:**
   1. **Parse Logs**
   2. **Create Events**

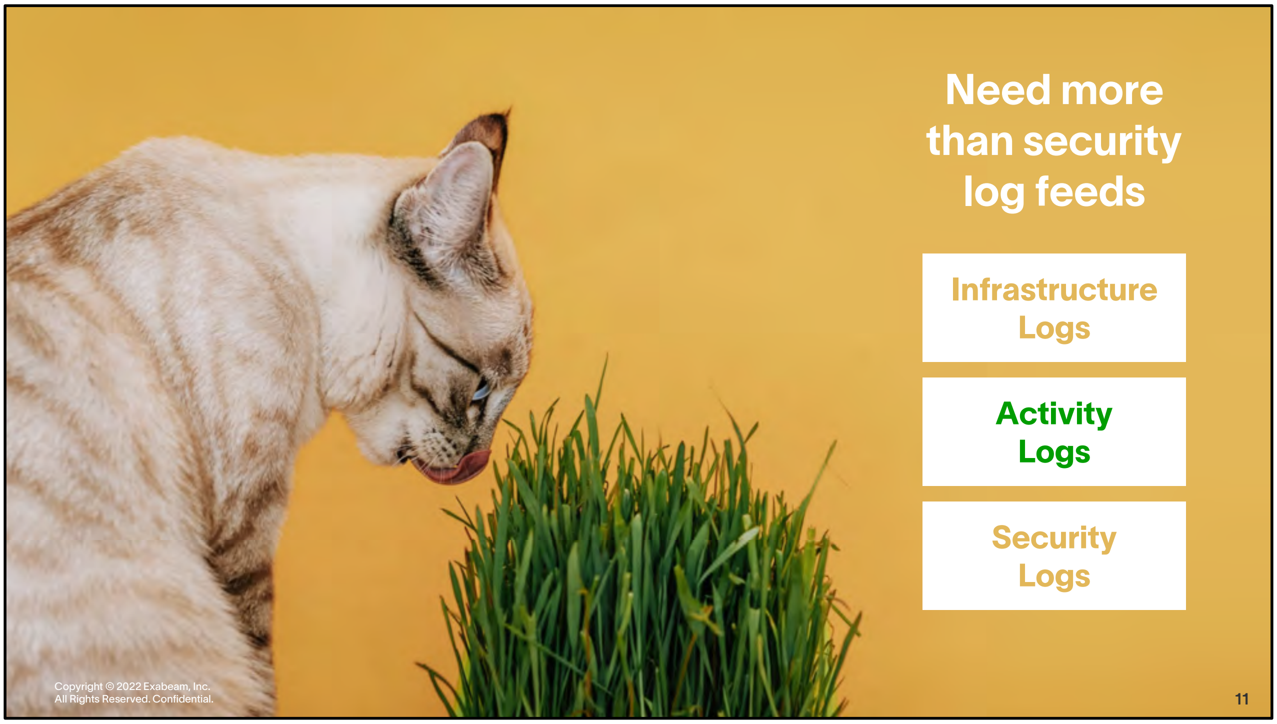
3. Describe the two types of the Enrich Events stage in the Analytics Engine:
   1. System-Defined
   2. User-Defined

4. Answer the following key questions regarding context:
   1. Where does context come from?
   2. How are context tables used in behavior analytics?



Security Analysts Need Good Data for Investigating

Secure Cloud
VPN
Email
Web, App
Access - DMZ
Gateways, firewalls, proxies
Services
Business
Users
Endpoint devices, IoT devices, web browsers



Need more than security log feeds

Infrastructure Logs

Activity Logs

Security Logs

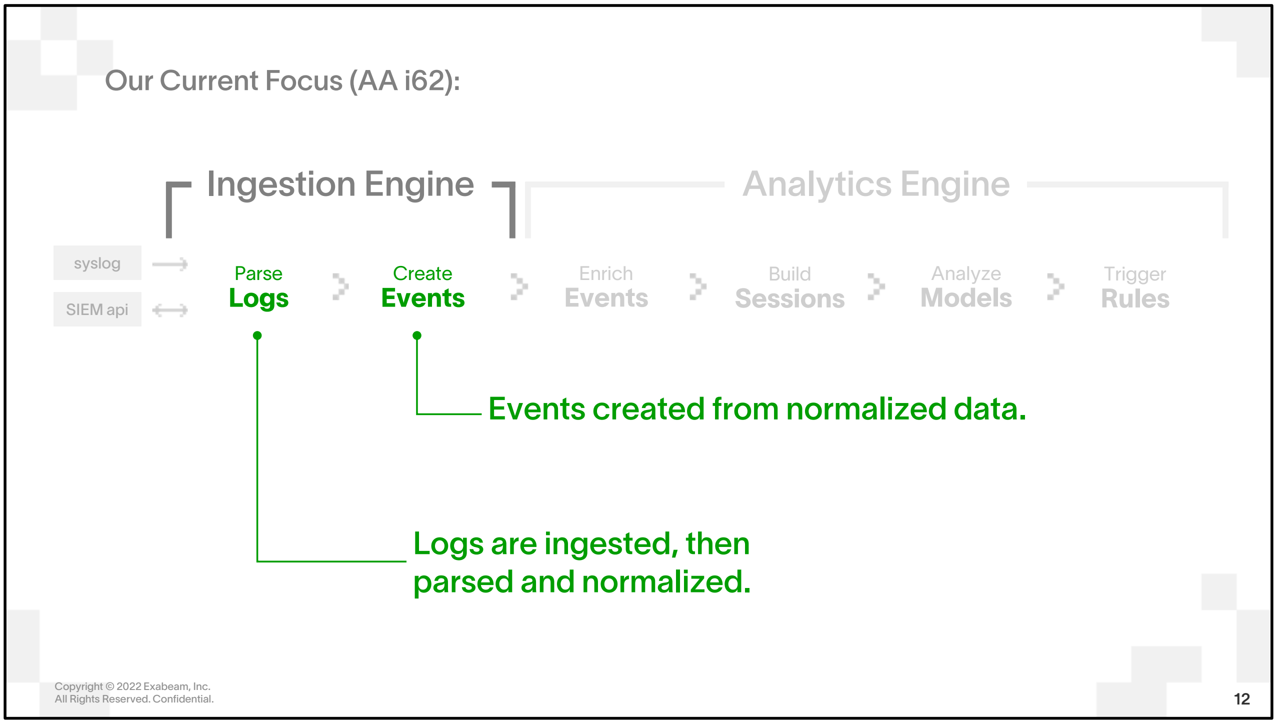
Student Notes
Compatible with thousands of log sources out of the box
Dedicated content team for rapid turnaround on new sources

Along with thousands of potential cyber security log sources that are categorized as seen below…we also have our Cloud Connector.

INFRASTRUCTURE LOGS – Server logs, firewall logs, system health logs. These are not as useful as the other types of logs but can be ingested for certain use cases. Infrastructure logs are also helpful for enriching context.
ACTIVITY LOGS – These are *essential* to UEBA analytics and context setting.
SECURITY LOGS – Traditional alerting and alarm systems like firewalls, proxies, endpoint, etc. These are valuable to Advanced Analytics.

Example log sources:

- Network Security, firewall, monitoring & forensics, IDS, UTM
- Endpoint Security, prevention, detection and response
- Application Security, WAF and Vulnerability Assessment
- Web Security
- Messaging Security
- Risk & Compliance
- Security Ops and Incident Response
- Data Security
- Mobile Security
- IAM
- Threat Analysis and Protection
- Fraud Prevention & Transaction Security



Our Current Focus (AA i62):

Ingestion Engine

Analytics Engine

syslog

SIEM api

Parse **Logs**

Create **Events**

Enrich **Events**

Build **Sessions**

Analyze **Models**

Trigger **Rules**

Events created from normalized data.

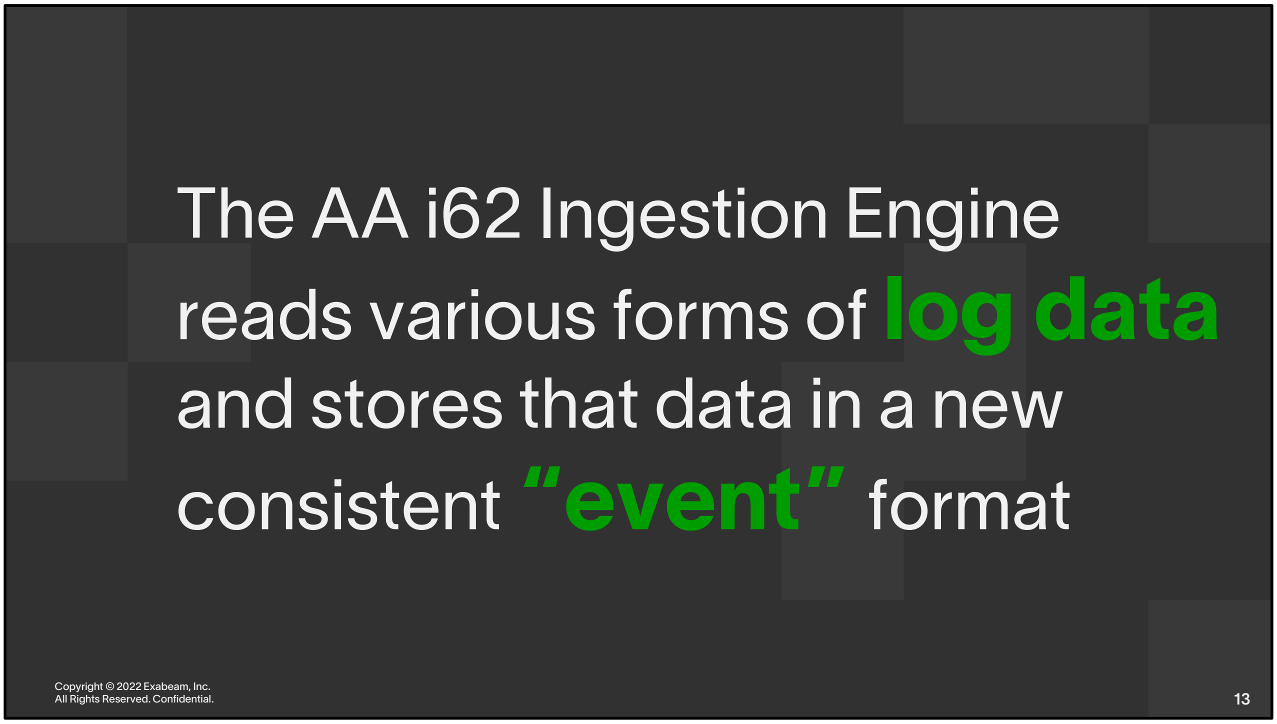
Logs are ingested, then parsed and normalized.

Student Notes

The Advanced Analytics Ingestion Engine performs the following:

- Typically ingests most logs via Syslog, maximizing local processing efficiency since Advanced Analytics is not adding a processing workload.
- In some cases, API can be configured to fetches logs from SIEM log repositories such as Splunk and Qradar (with infrastructure prerequisites)
- Normalizes raw logs into an internally consistent event format used for the rest of the pipeline.

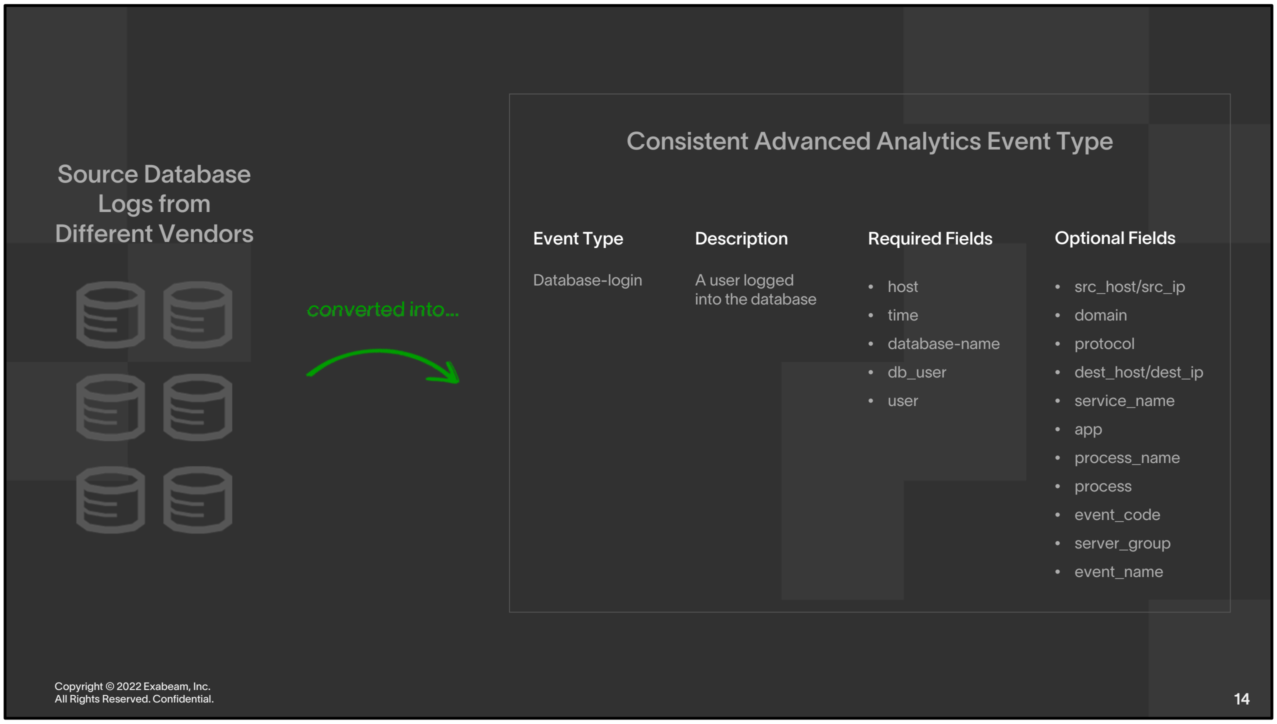
The Ingestion Engine of Advanced Analytics is going to process log data obtained directly through Syslog or through a SIEM API connected to such as Exabeam Data Lake, Splunk, Microfocus ArcSight, and many more. Different sources may identify fields of data differently, so raw log items are normalized so that there are consistent field names and types for common pieces of information such usernames, hostnames, or source IP addresses.



The AA i62 Ingestion Engine reads various forms of **log data** and stores that data in a new consistent **“event”** format

Student Notes

The log data that will be used to create actionable information in Advanced Analytics can have many variances. Different vendors and SIEMs being used as a data source may use different field names to reference the same field, such as “IP”, “IP Address”, “Network Address” and so forth.

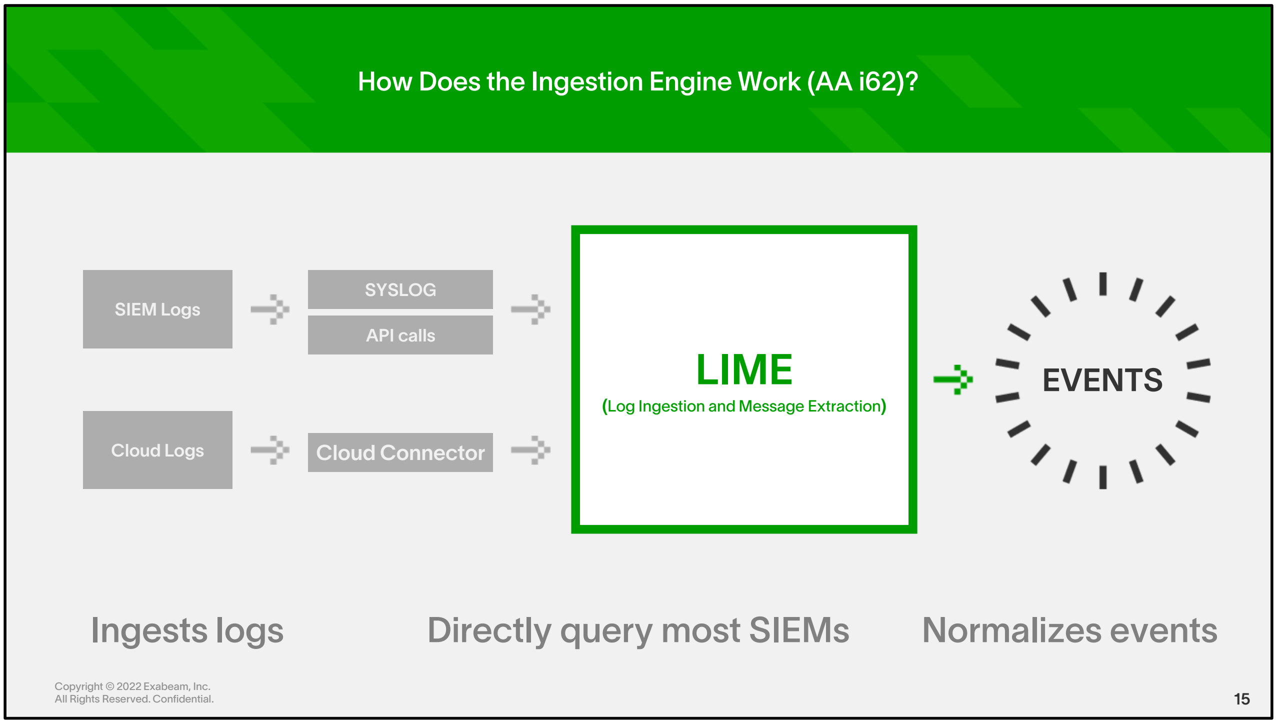


Source Database Logs from Different Vendors

converted into…

Consistent Advanced Analytics Event Type

Event Type	Description	Required Fields	Optional Fields
Database-login	A user logged into the database	• host • time • database-name • db_user • user	• src_host/src_ip • domain • protocol • dest_host/dest_ip • service_name • app • process_name • process • event_code • server_group • event_name



How Does the Ingestion Engine Work (AA i62)?

SIEM Logs

SYSLOG

API calls

Cloud Logs

Cloud Connector

LIME

(Log Ingestion and Message Extraction)

EVENTS

Ingests logs

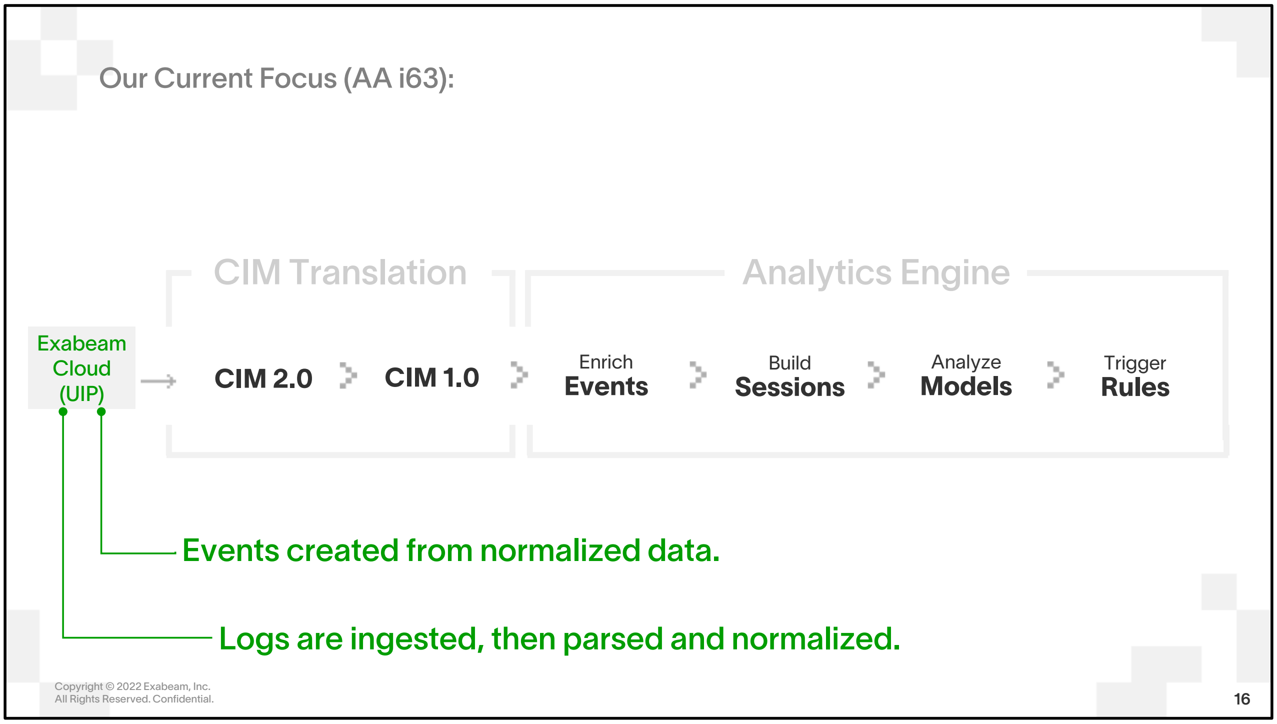
Directly query most SIEMs

Normalizes events

Student Notes

LIME is the Ingestion engine, processing logs and directly querying most SIEMs.

It then normalizes the event into a consistent format and creates event content files that are stored on an HDFS (Hadoop Distributed File System)



Our Current Focus (AA i63):

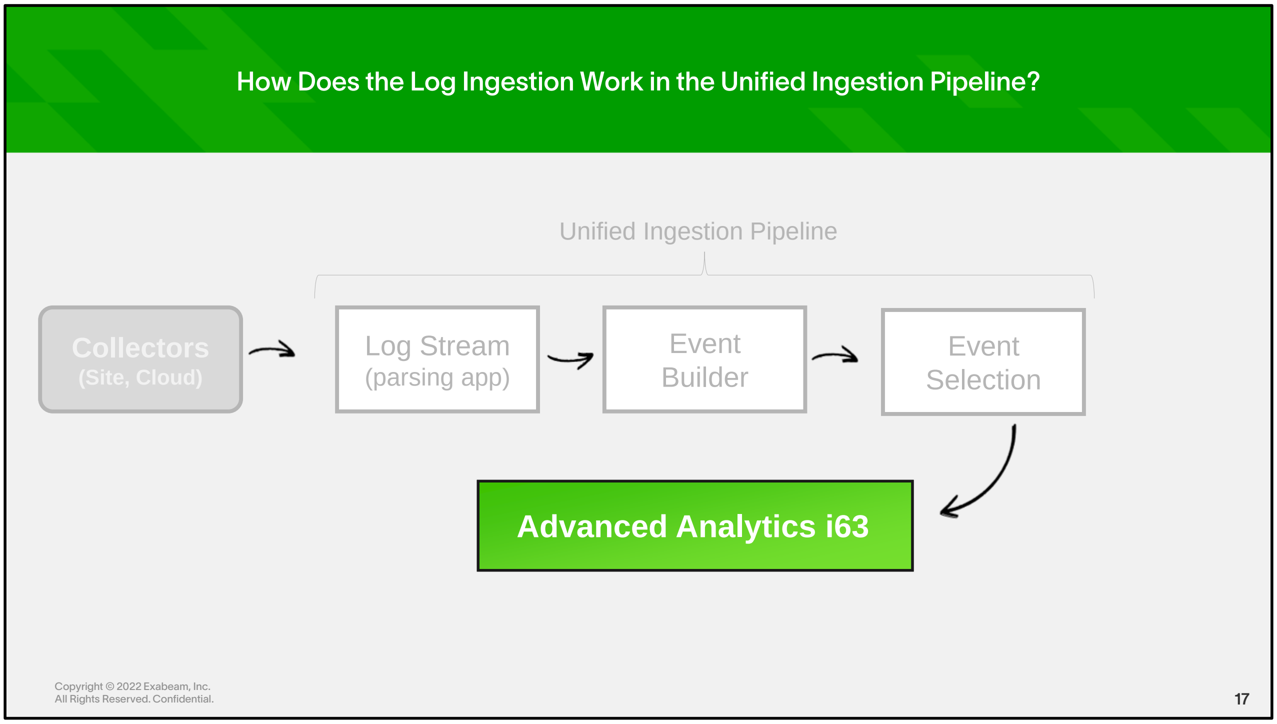
CIM Translation

Analytics Engine

Exabeam Cloud (UIP) → CIM 2.0 › CIM 1.0 › Enrich **Events** › Build **Sessions** › Analyze **Models** › Trigger **Rules**

Events created from normalized data.

Logs are ingested, then parsed and normalized.



How Does the Log Ingestion Work in the Unified Ingestion Pipeline?

Unified Ingestion Pipeline

Collectors
(Site, Cloud)

Log Stream
(parsing app)

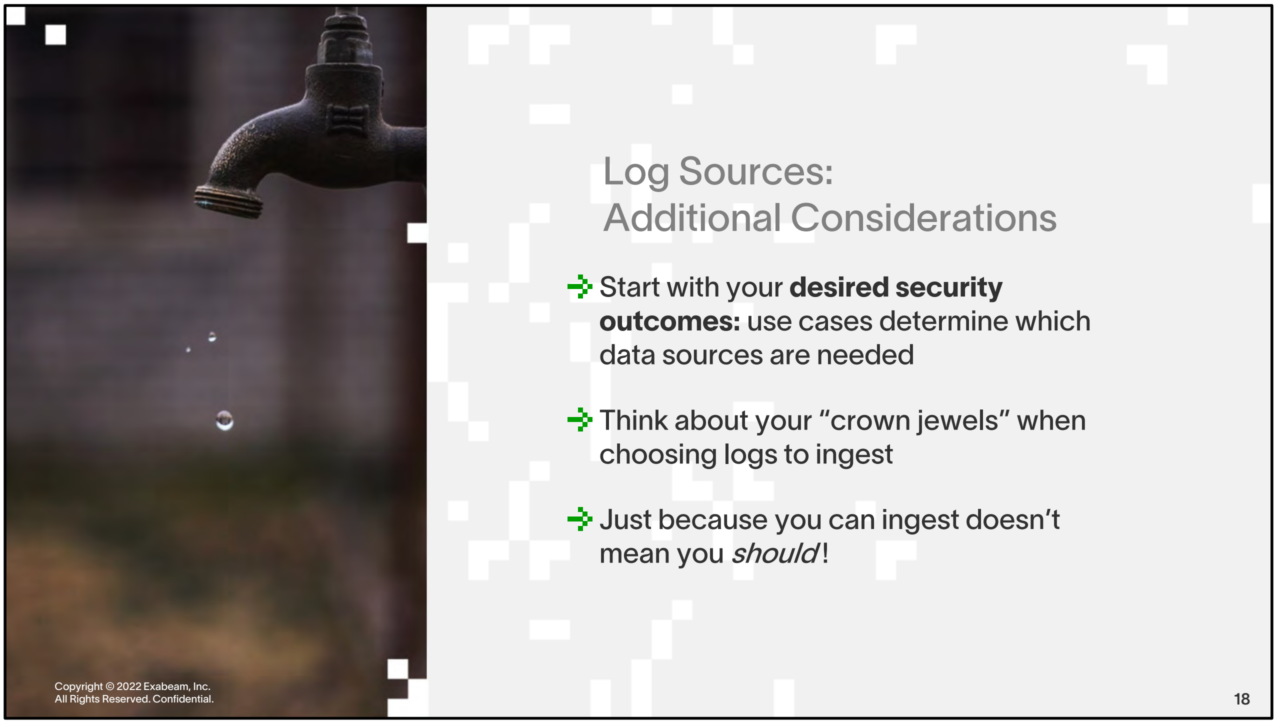
Event
Builder

Event
Selection

Advanced Analytics i63

Student Notes

LIME is the Ingestion engine, processing logs and directly querying most SIEMs.
It then normalizes the event into a consistent format and creates event content files that are stored on an HDFS (Hadoop Distributed File System)



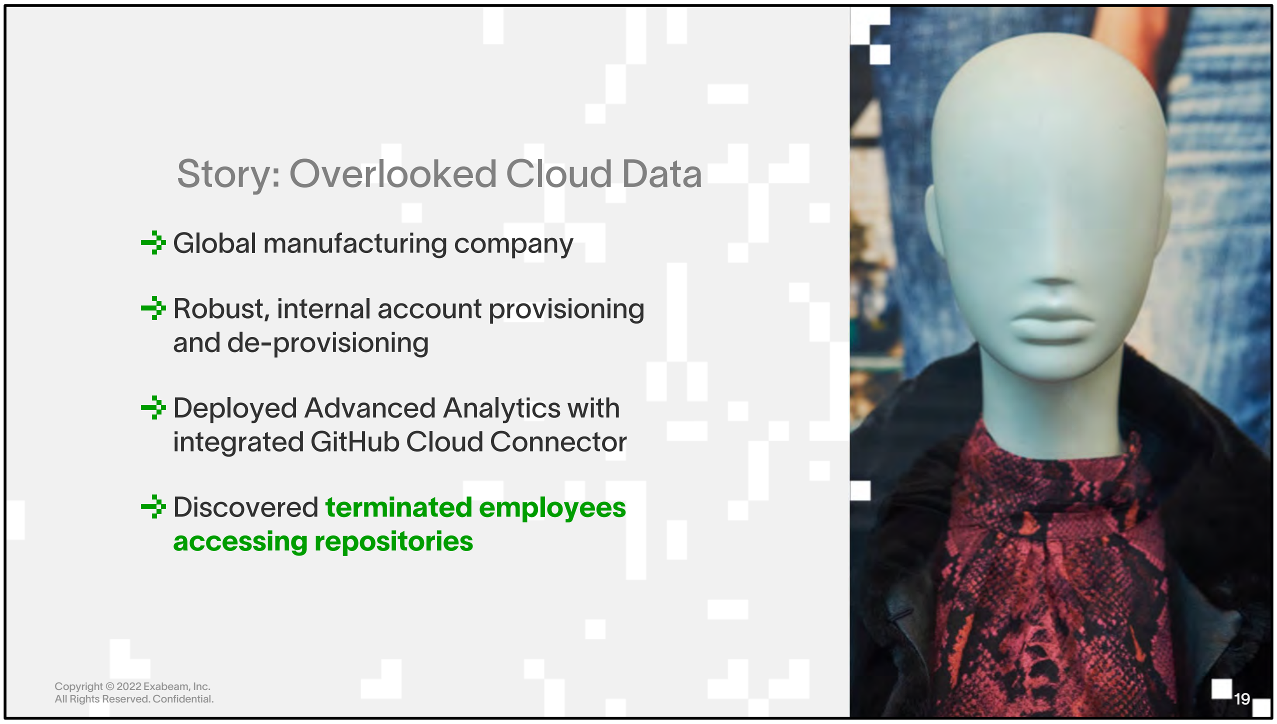
Log Sources: Additional Considerations

- Start with your **desired security outcomes:** use cases determine which data sources are needed
- Think about your “crown jewels” when choosing logs to ingest
- Just because you can ingest doesn’t mean you *should*!

Student Notes

Different types of data are needed if your goal is to track compromised credentials than phishing or malware. Identifying who and where are the sources of greatest risk because of likelihood and value will help you identify the logs that surround those resources or people. Having the logs that accomplish those goals without weighing down Advanced Analytics with the job of working through data sources that are irrelevant is crucial for an environment that provides relevant data in a timely way.

{Photo by Walter Randlehoff on Unsplash}

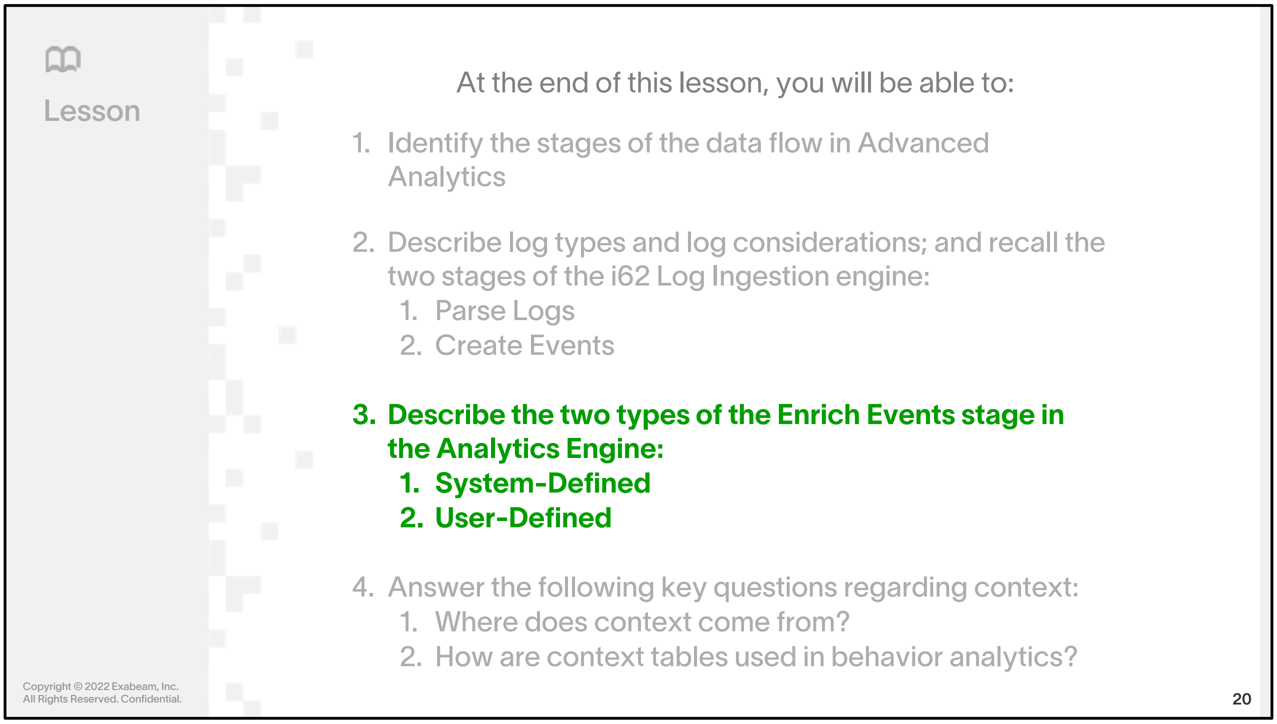


Story: Overlooked Cloud Data

- Global manufacturing company
- Robust, internal account provisioning and de-provisioning
- Deployed Advanced Analytics with integrated GitHub Cloud Connector
- Discovered **terminated employees accessing repositories**

Student Notes
Read the full story here - https://www.exabeam.com/information-security/cloud-source-code-theft/

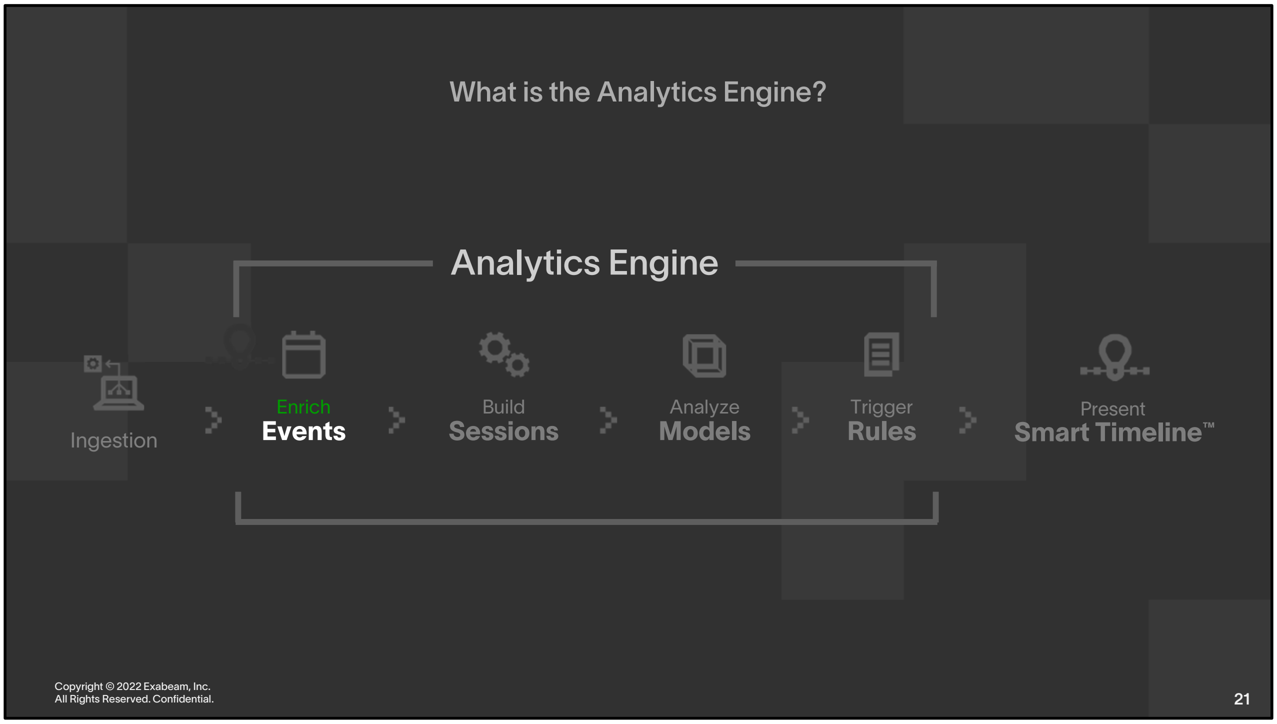
{Photo by Martin Adams on Unsplash}



Lesson

At the end of this lesson, you will be able to:

1. Identify the stages of the data flow in Advanced Analytics
2. Describe log types and log considerations; and recall the two stages of the i62 Log Ingestion engine:
   1. Parse Logs
   2. Create Events
3. **Describe the two types of the Enrich Events stage in the Analytics Engine:**
   1. **System-Defined**
   2. **User-Defined**
4. Answer the following key questions regarding context:
   1. Where does context come from?
   2. How are context tables used in behavior analytics?



What is the Analytics Engine?

Analytics Engine

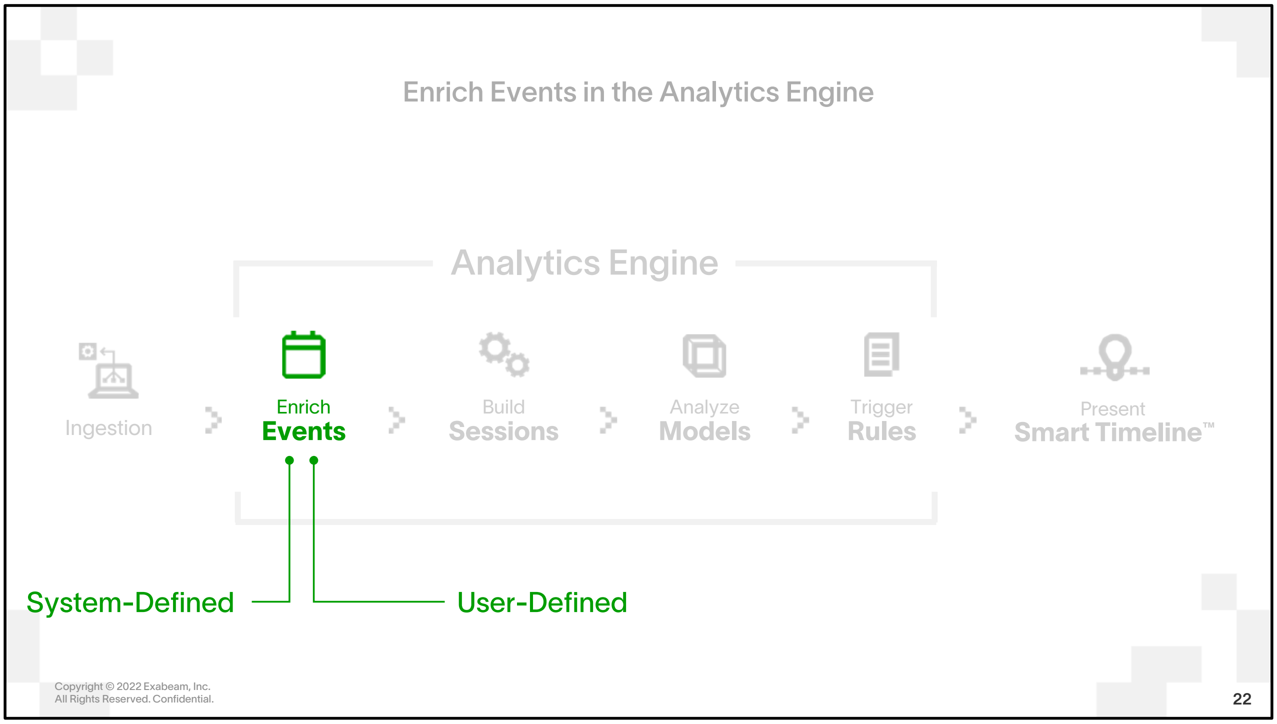
Ingestion → Enrich **Events** → Build **Sessions** → Analyze **Models** → Trigger **Rules** → Present **Smart Timeline™**

21

Student Notes

Analytics Engine Tasks:

- Enriches the events with contextual data
- Build sessions out of user and entity activity.
- Models analyze the events for machine-learning.
- Evaluate this activity using rules to trigger against anomalous, abnormal events and assign risk scores.
- Build Smart Timelines, showing normal and abnormal activity chronologically.



Enrich Events in the Analytics Engine

Analytics Engine

Ingestion > Enrich **Events** > Build **Sessions** > Analyze **Models** > Trigger **Rules** > Present **Smart Timeline™**

System-Defined

User-Defined

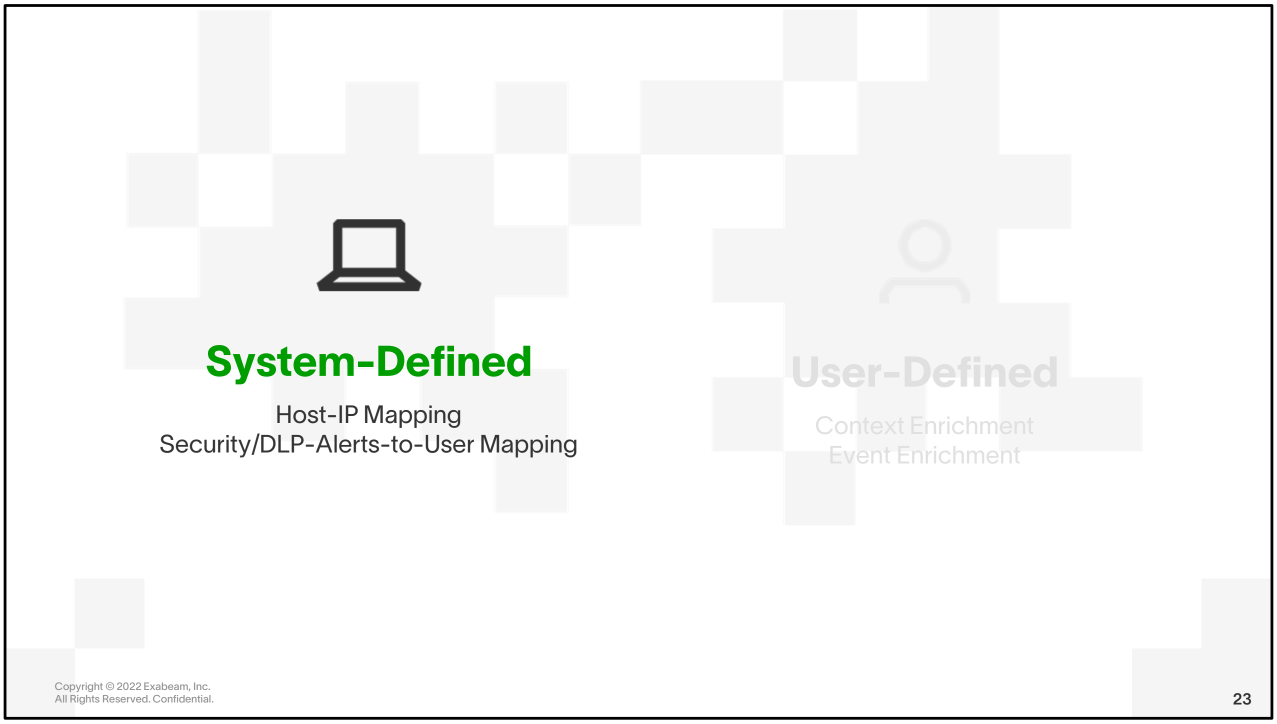
Student Notes

There are two types of enrichment, system- and user-defined:

- SYSTEM-DEFINED
- USER-DEFINED

Source

Exabeam How Content Works Guide (Exabeam Enrichment)



System-Defined

Host-IP Mapping
Security/DLP-Alerts-to-User Mapping

User-Defined

Context Enrichment
Event Enrichment

Student Notes

SYSTEM-DEFINED

This type of enrichment is done automatically by Advanced Analytics in the backend and can be slightly tuned by custom_exabeam_config.conf.

•**Host-IP Mapping** – If a user or hostname is detected without the other, this enrichment feature populates the missing field based on previously seen data.

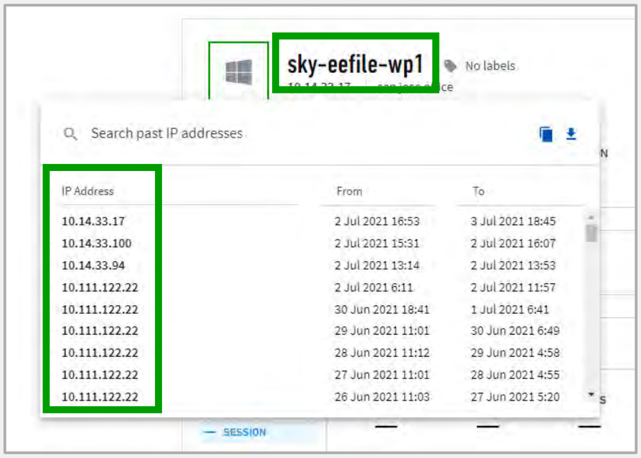
•**Security/DLP-Alerts-to-User Mapping** – When security or DLP alerts do not have the user information, this enrichment feature populates the user field based on previously seen data.

Source

Exabeam How Content Works Guide (Exabeam Enrichment)

System-Defined Enrichment Example

Host-to-IP Mappings



sky-eefile-wp1

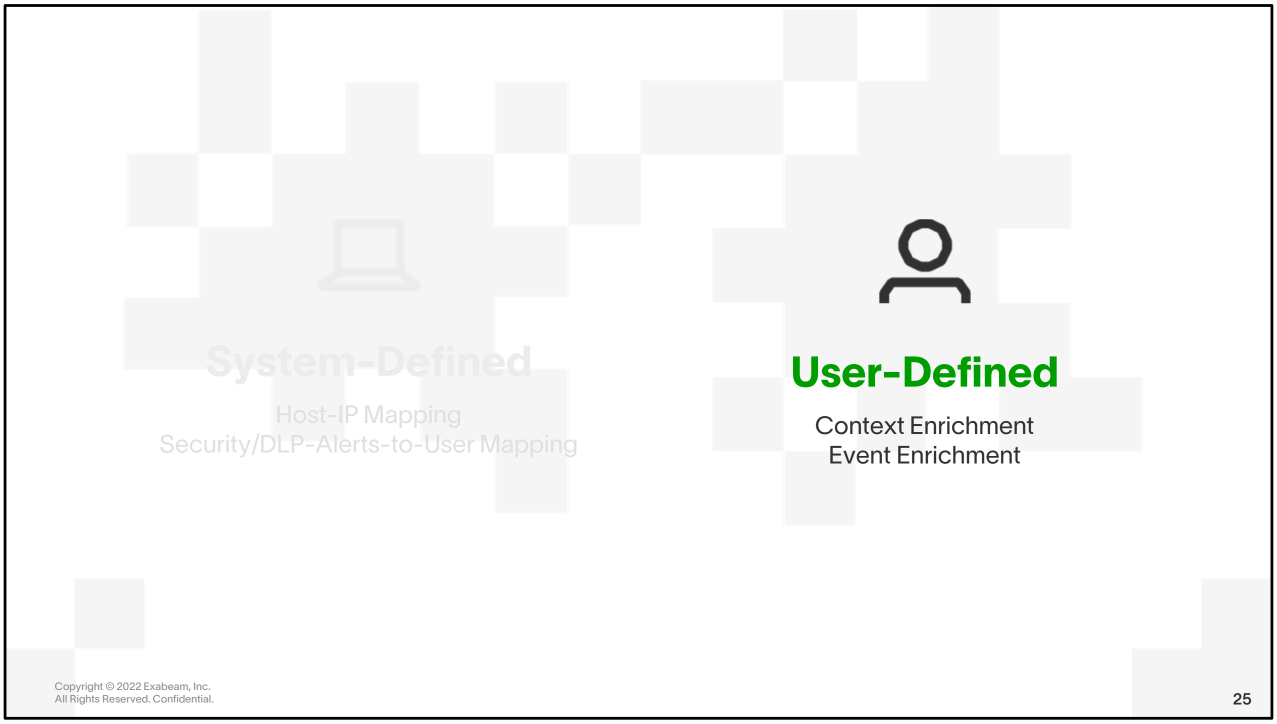
IP Address	From	To
10.14.33.17	2 Jul 2021 16:53	3 Jul 2021 18:45
10.14.33.100	2 Jul 2021 15:31	2 Jul 2021 16:07
10.14.33.94	2 Jul 2021 13:14	2 Jul 2021 13:53
10.111.122.22	2 Jul 2021 6:11	2 Jul 2021 11:57
10.111.122.22	30 Jun 2021 18:41	1 Jul 2021 6:41
10.111.122.22	29 Jun 2021 11:01	30 Jun 2021 6:49
10.111.122.22	28 Jun 2021 11:12	29 Jun 2021 4:58
10.111.122.22	27 Jun 2021 11:01	28 Jun 2021 4:55
10.111.122.22	26 Jun 2021 11:03	27 Jun 2021 5:20

Student Notes

Mapping host to IP manually is time consuming and difficult. Advanced Analytics simplifies and automatics this tedious task as part of Enrich Events.

More Information

https://docs.exabeam.com/en/content/all/how-content-works-guide/56894-introduction-to-how-content-works.html



System-Defined

Host-IP Mapping
Security/DLP-Alerts-to-User Mapping

User-Defined

Context Enrichment
Event Enrichment

Student Notes

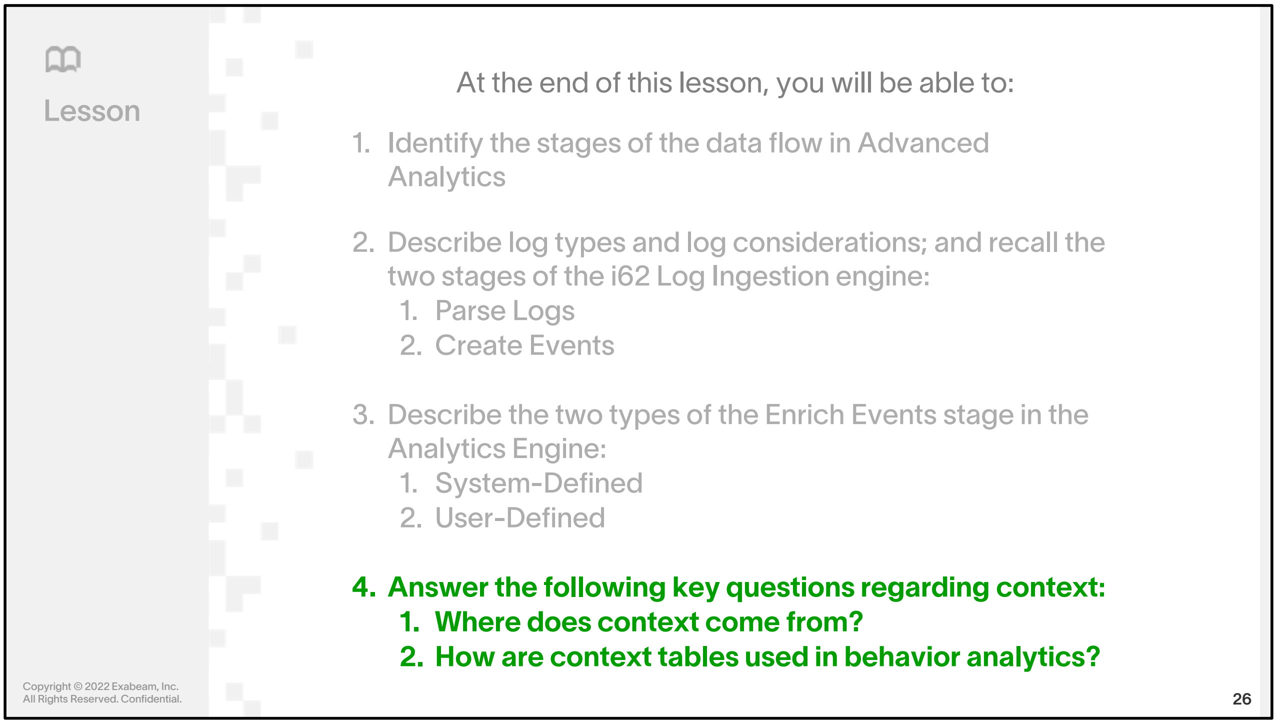
USER-DEFINED

This type of enrichment can be granularly controlled by the user.

•**Context Enrichment** – Performs a lookup from a context table to populate a field.

•**Event Enrichment** – Modifies/adds/removes fields. This is the most common type of enrichment, defined the same way context enrichment is defined. All logical expressions available in the analytics engine, excluding model/session expressions, can be used in the Event Enricher.

•**Event Duplicator** – Duplicates an event for the purpose of adding to a different user/asset timeline.



Lesson

At the end of this lesson, you will be able to:

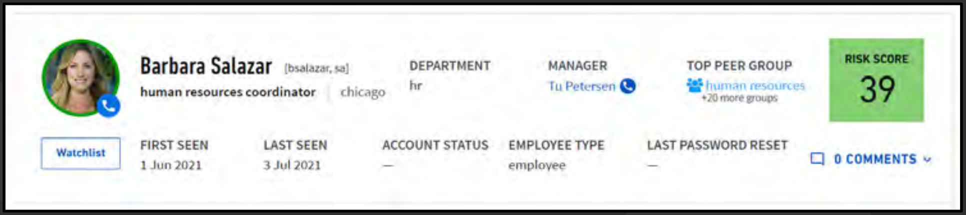
1. Identify the stages of the data flow in Advanced Analytics

2. Describe log types and log considerations; and recall the two stages of the i62 Log Ingestion engine:
    1. Parse Logs
    2. Create Events

3. Describe the two types of the Enrich Events stage in the Analytics Engine:
    1. System-Defined
    2. User-Defined

4. **Answer the following key questions regarding context:**
    1. **Where does context come from?**
    2. **How are context tables used in behavior analytics?**

What is Context?



Barbara Salazar [bsalazar, sa]
human resources coordinator | chicago

DEPARTMENT
hr

MANAGER
Tu Petersen

TOP PEER GROUP
human resources
+20 more groups

RISK SCORE
39

Watchlist

FIRST SEEN
1 Jun 2021

LAST SEEN
3 Jul 2021

ACCOUNT STATUS
—

EMPLOYEE TYPE
employee

LAST PASSWORD RESET
—

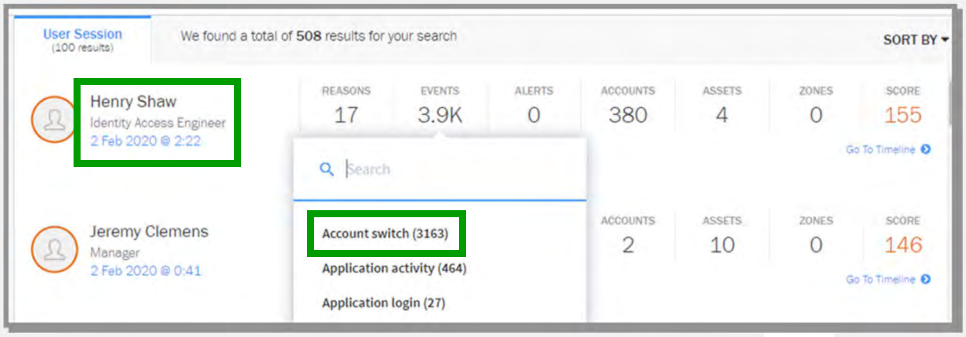
0 COMMENTS

Context provides additional details, thus enabling analysts to make deductions, determine intent, and infer other **relevant insights** during an investigation.

Student Notes
What is Context? Context provides additional details, thus enabling analysts to make deductions, determine intent, and infer other relevant insights during an investigation. Context can come from multiple sources, including context tables.

Example of How Context Accelerates Decisions:

Is Henry Shaw's behavior a security risk?



User Session (100 results)

We found a total of **508** results for your search

SORT BY

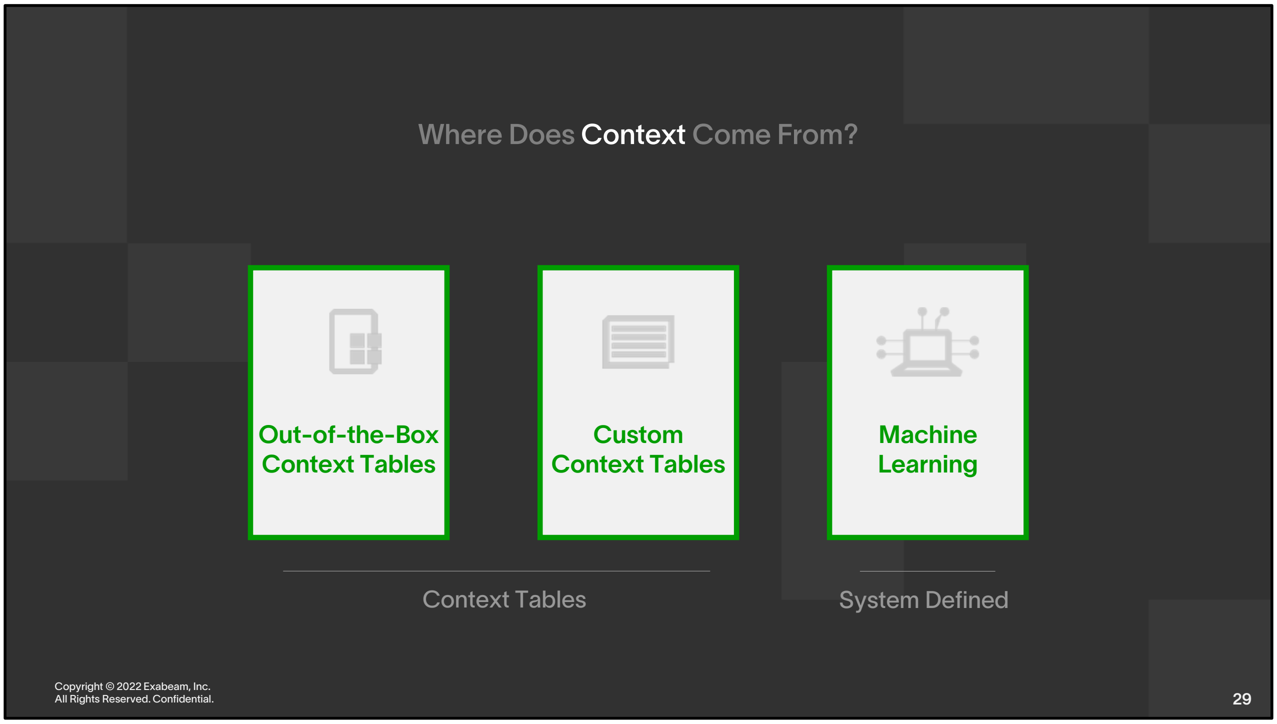
User	REASONS	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES	SCORE
Henry Shaw Identity Access Engineer 2 Feb 2020 @ 2:22	17	3.9K	0	380	4	0	155
Jeremy Clemens Manager 2 Feb 2020 @ 0:41				2	10	0	146

Search

- Account switch (3163)
- Application activity (464)
- Application login (27)

Student Notes

How do Henry Shaw’s position and their number of account switches correlate?



Where Does **Context** Come From?

Out-of-the-Box Context Tables

Custom Context Tables

Machine Learning

Context Tables

System Defined

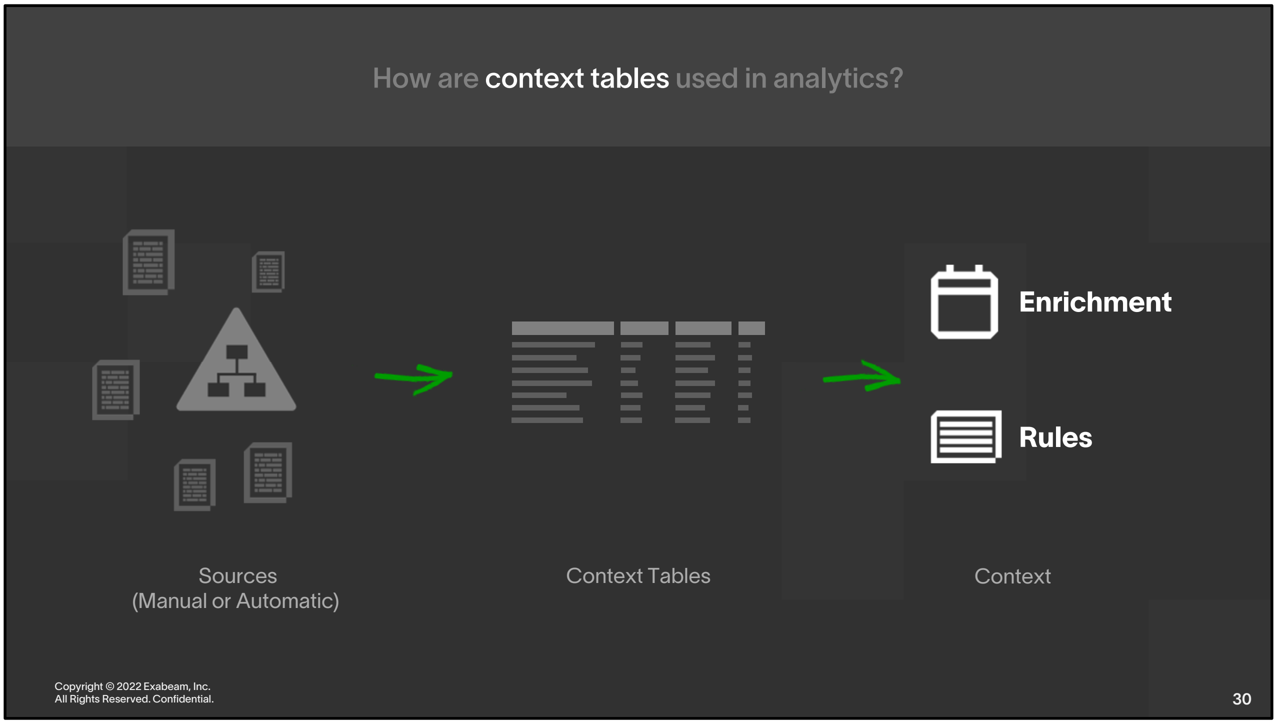
29

Student Notes

Context comes from multiple sources. The analytics engine can produce context with things like Risk Score, the Smart Timeline, and Dynamic Peer Grouping. Context data can also come from context tables.

Context tables are lists of resources. For example, these resources can range from assets (i.e., computers, servers) or users (employees of the company) to a list of IPs and Internet domains. While logs show what users and entities are doing, context tables can provide context by showing **who** the users and entities are. Some context tables come out-of-the-box. Others can be created and managed by administrators.

References:
https://docs.exabeam.com/en/advanced-analytics/i56/advanced-analytics-administration-guide/125371-configure-advanced-analytics.html#UUID-c64778c2-4af7-96fd-8ea6-7a43aa7c9d8e
https://docs.exabeam.com/en/advanced-analytics/i56/advanced-analytics-administration-guide/125371-configure-advanced-analytics.html#UUID-c64778c2-4af7-96fd-8ea6-7a43aa7c9d8e
https://community.exabeam.com/s/article/Context-Tables



How are context tables used in analytics?

Sources
(Manual or Automatic)

Context Tables

Context

Enrichment

Rules

Student Notes
Context tables enrich the logs by fusing multiples sources containing additional details into the Exabeam SOC Platform, thus adding context. Context tables may also be used by rules and watchlists.

How are context tables used in analytics?

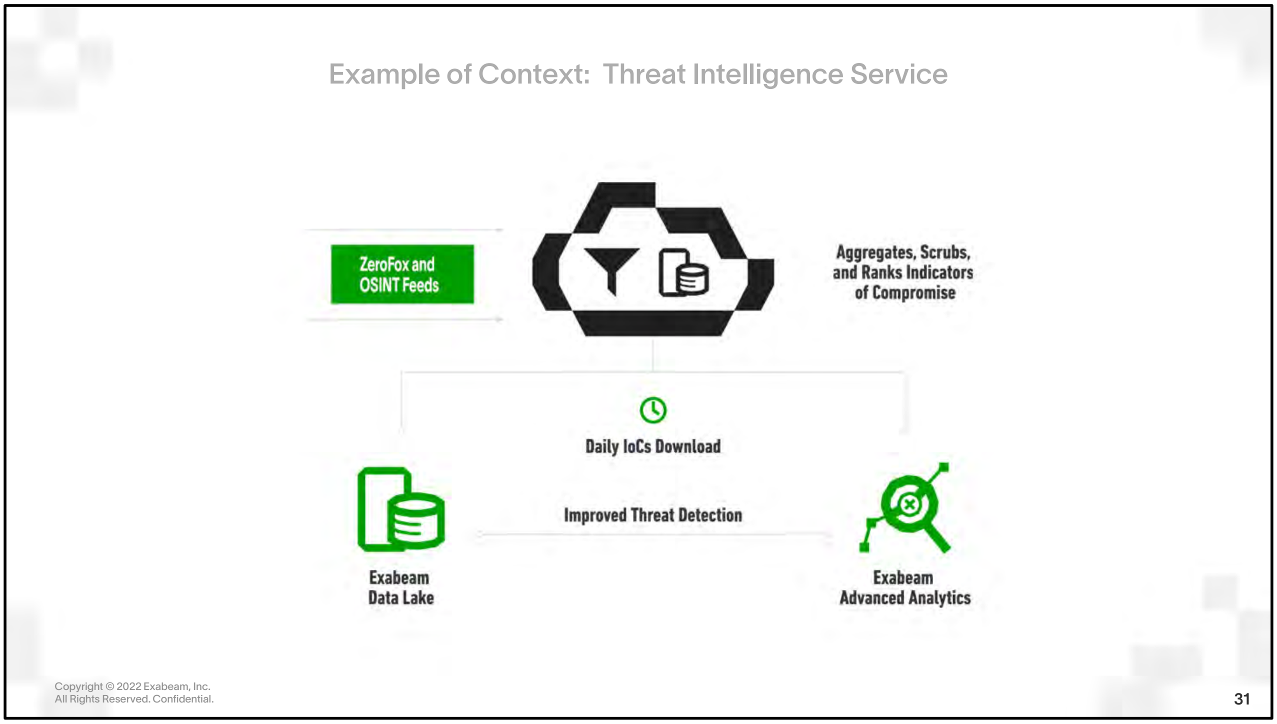
Two ways:
- Enrich logs to help with the anomaly detection process
- Used directly by the risk engine layer for many rules

Context tables may also be used to populate key fields in the User Profile and Asset pages.

An example of when context tables could be used is when you want to customize rules and models that are in AA. You can create a list of specific users and have a rule that will check if an event is related to one of the users listed in that context table.

Administrators can view and edit Exabeam's out-of-the-box context tables as well as create their own custom tables. They can select a specific table, such as Executive Users, Service Accounts, etc. and see the details of the table and all of the objects within the table. Edits can be performed on objects individually or through CSV uploads.

Source
https://community.exabeam.com/s/article/Context-Tables
https://docs.exabeam.com/en/advanced-analytics/cloud-delivered/advanced-analytics-administration-guide/127389-configure-advanced-analytics.html



Example of Context: Threat Intelligence Service

ZeroFox and OSINT Feeds

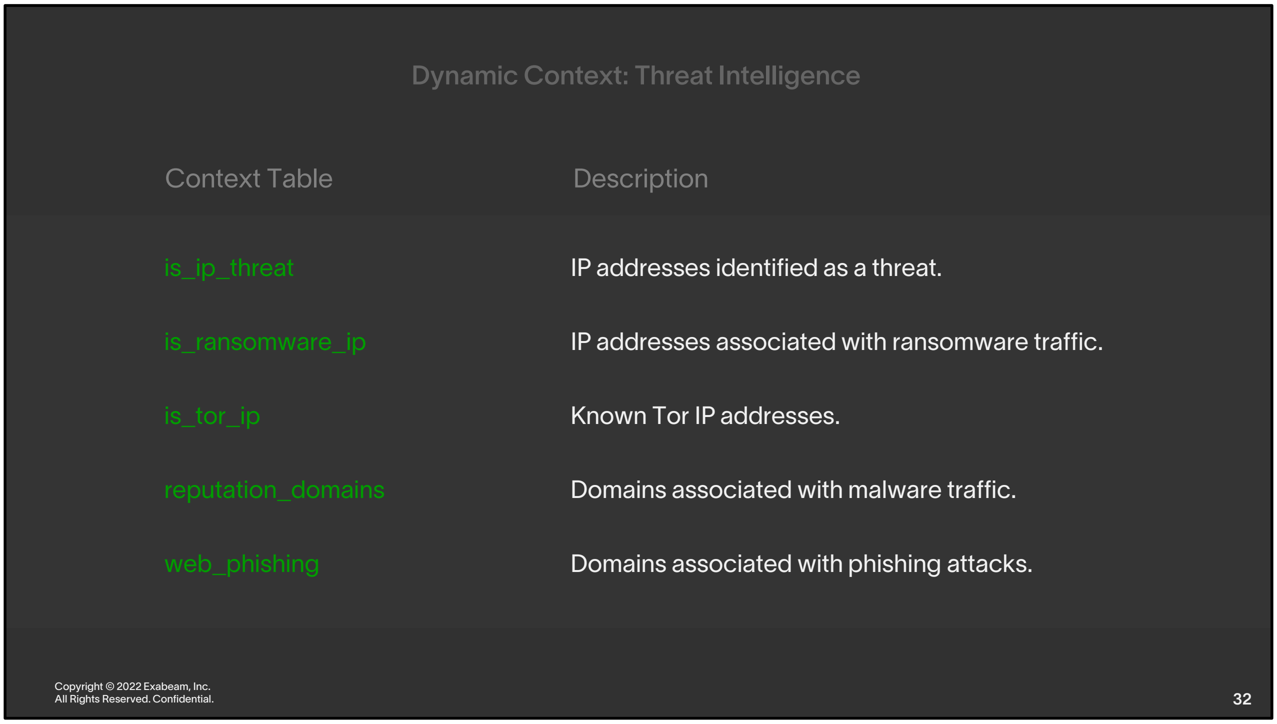
Aggregates, Scrubs, and Ranks Indicators of Compromise

Daily IoCs Download

Improved Threat Detection

Exabeam Data Lake

Exabeam Advanced Analytics



Dynamic Context: Threat Intelligence

Context Table	Description
is_ip_threat	IP addresses identified as a threat.
is_ransomware_ip	IP addresses associated with ransomware traffic.
is_tor_ip	Known Tor IP addresses.
reputation_domains	Domains associated with malware traffic.
web_phishing	Domains associated with phishing attacks.

Student Notes

The Exabeam Threat Intelligence Service delivers a constant stream of up-to-date threat indicators to Advanced Analytics deployments. Data Lake customers can also leverage these indicators by filtering searches using key-only context tables.

The categories of indicators affected are the following:

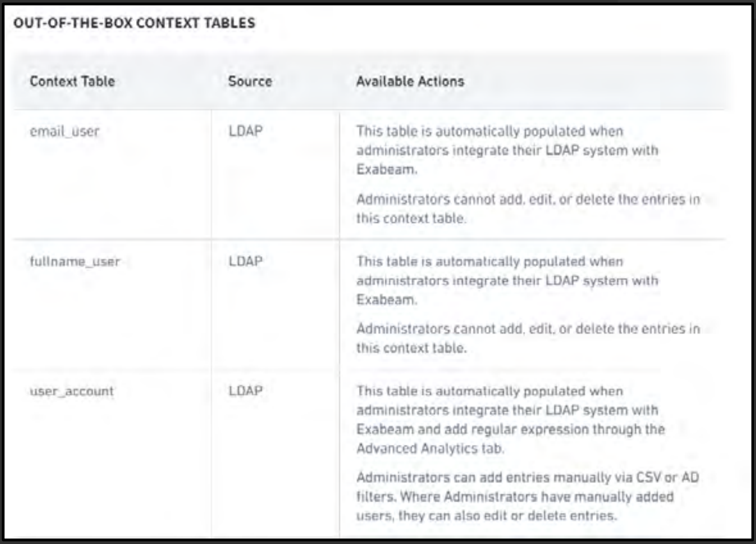
- IP addresses associated with Ransomware or Malware attacks
- IP addresses associated with the TOR network
- Domain names associated with Ransomware, Phishing, or Malware attacks

Indicators are downloaded by the Exabeam SOC platform from Threat Intelligence Service on a daily basis.

Advanced Analytics and Data Lake connect to Threat Intelligence Service through a cloud connector service that provides authentication and establishes a secure connection to Threat Intelligence Service. The cloud connector service then collects updated threat indicators from Threat Intelligence Service daily.
These indicators are then made available within Advanced Analytics to provide enhanced risk scoring based on curated threat intelligence.
This product does not require a separate license.

References
https://www.exabeam.com/wp-content/uploads/DATASHEET-Threat-Intelligence-Service.pdf

Examples of Context Tables



OUT-OF-THE-BOX CONTEXT TABLES

Context Table	Source	Available Actions
email_user	LDAP	This table is automatically populated when administrators integrate their LDAP system with Exabeam. Administrators cannot add, edit, or delete the entries in this context table.
fullname_user	LDAP	This table is automatically populated when administrators integrate their LDAP system with Exabeam. Administrators cannot add, edit, or delete the entries in this context table.
user_account	LDAP	This table is automatically populated when administrators integrate their LDAP system with Exabeam and add regular expression through the Advanced Analytics tab. Administrators can add entries manually via CSV or AD filters. Where Administrators have manually added users, they can also edit or delete entries.

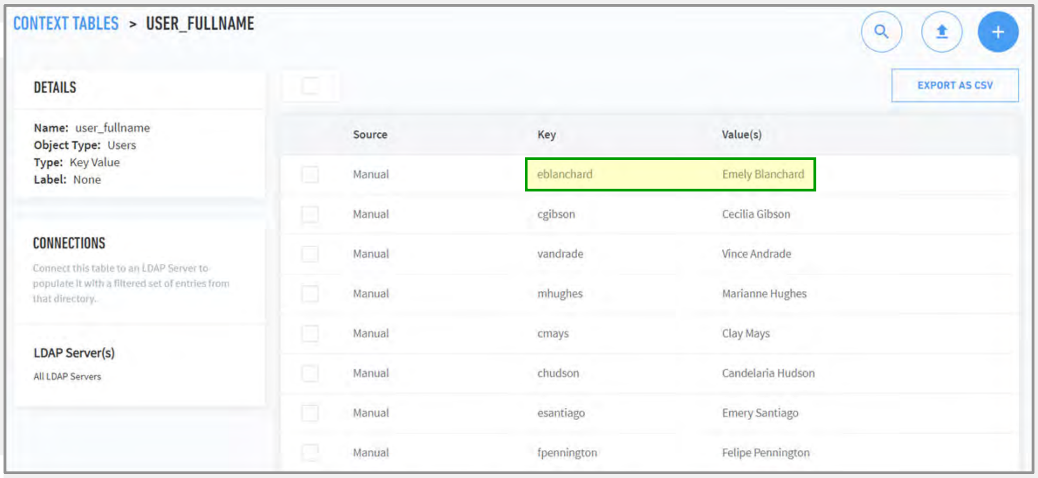
Source: Administration Guide

Student Notes

This is an example of out-of-the-box context tables. See the Administration Guide for more information.

Source:
https://community.exabeam.com/s/article/Context-Tables
https://docs.exabeam.com/en/advanced-analytics/cloud-delivered/advanced-analytics-administration-guide/127389-configure-advanced-analytics.html

The Power of Context Tables



DETAILS

Name: user_fullname
Object Type: Users
Type: Key Value
Label: None

CONNECTIONS

Connect this table to an LDAP Server to populate it with a filtered set of entries from that directory.

LDAP Server(s)

All LDAP Servers

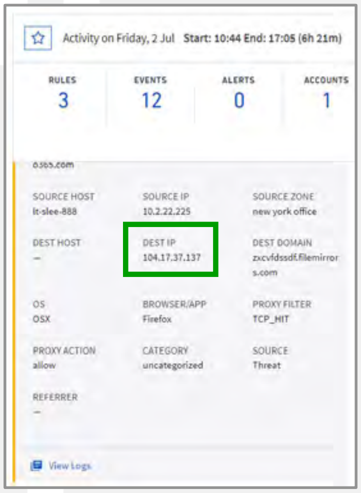
Source	Key	Value(s)
Manual	eblanchard	Emely Blanchard
Manual	cgibson	Cecilia Gibson
Manual	vandrade	Vince Andrade
Manual	mhughes	Marianne Hughes
Manual	cmays	Clay Mays
Manual	chudson	Candelaria Hudson
Manual	esantiago	Emery Santiago
Manual	fpennington	Felipe Pennington

Which information is more likely to be in a log?
Are there other ways a log might store a reference to a user?
What value does the context table do in looking up the full username for an analyst?

Student Notes

Context tables are stored in Advanced Analytics in order to map to user profile fields and enrich events, models, and rules using the most up to date contextual information. Some tables can be automatically populated. For example, many tables can be populated automatically from Active Directory. Some tables must be manually populated. Custom tables can also be created to create watchlists or reference lists for assets, threat intelligence indicators, or users and groups that don't fit in typical deployment categories.

Context Tables Are Also Used in Rules!



Activity on Friday, 2 Jul Start: 10:44 End: 17:05 (6h 21m)

RULES	EVENTS	ALERTS	ACCOUNTS
3	12	0	1

o365.com

SOURCE HOST
lt-slee-888

SOURCE IP
10.2.22.225

SOURCE ZONE
new york office

DEST HOST
–

DEST IP
104.17.37.137

DEST DOMAIN
zxcvfdssdf.filemirrors.com

OS
OSX

BROWSER/APP
Firefox

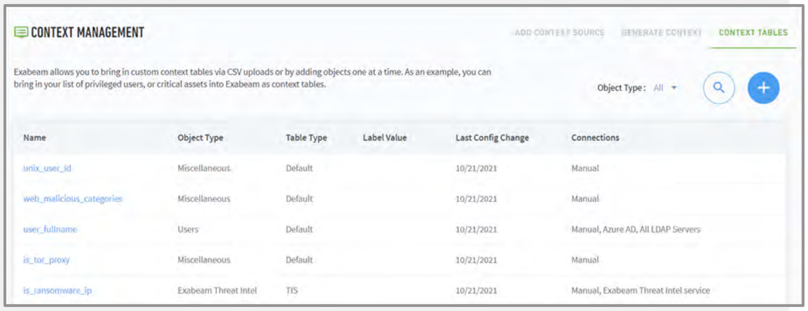
PROXY FILTER
TCP_HIT

PROXY ACTION
allow

CATEGORY
uncategorized

SOURCE
Threat

REFERRER
–



CONTEXT MANAGEMENT

Exabeam allows you to bring in custom context tables via CSV uploads or by adding objects one at a time. As an example, you can bring in your list of privileged users, or critical assets into Exabeam as context tables.

Object Type: All

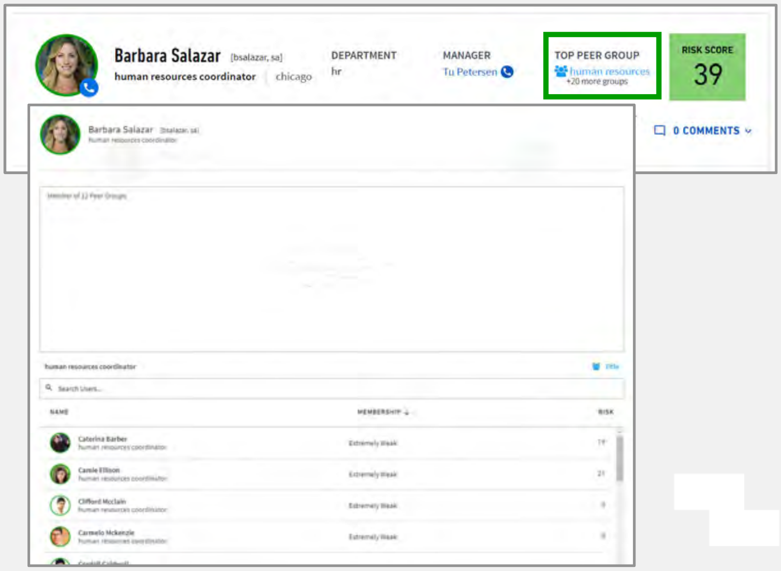
Name	Object Type	Table Type	Label Value	Last Config Change	Connections
unix_user_id	Miscellaneous	Default		10/21/2021	Manual
web_malicious_categories	Miscellaneous	Default		10/21/2021	Manual
user_fullname	Users	Default		10/21/2021	Manual, Azure AD, All LDAP Servers
is_tor_proxy	Miscellaneous	Default		10/21/2021	Manual
is_ransomware_ip	Exabeam Threat Intel	TIS		10/21/2021	Manual, Exabeam Threat Intel service

Which context table could be used to quickly identify if a destination IP address was associated with a known ransomware locale?

Student Notes

Threat Intelligence feeds can also populate context tables. In this example, a table of IP addresses in “is_ransomware_ip” context table and can be used to trigger ransomware rules.

Another Type of Context: Peer Groups



Barbara Salazar [bsalazar, sa]
human resources coordinator | chicago

DEPARTMENT: hr

MANAGER: Tu Petersen

TOP PEER GROUP: human resources
+20 more groups

RISK SCORE: 39

0 COMMENTS

Barbara Salazar [bsalazar, sa]
human resources coordinator

Member of 12 Peer Groups

human resources coordinator

Search Users...

NAME	MEMBERSHIP	RISK
Caterina Barber human resources coordinator	Extremely Weak	19
Carrie Ellison human resources coordinator	Extremely Weak	21
Clifford Mcclain human resources coordinator	Extremely Weak	9
Carmelo Mckenzie human resources coordinator	Extremely Weak	9
Cordell Caldwell		

Student Notes

The small group icon identifies which element in the directory information has been defined as the peer group.

The peer group icon is next to the manager’s department.

Exabeam works with each organization to create its definition of a peer group.

Clicking on the Peer Group link opens a popup with the highest-scoring sessions for members of the peer group.

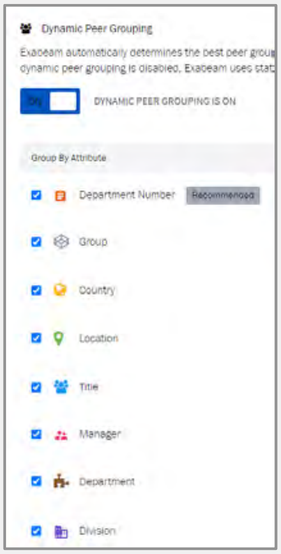
If dynamic peer grouping is enabled, we display the strongest relationship group.

References

https://www.exabeam.com/ueba/who-do-i-belong-to-dynamic-peer-analysis-for-ueba-explained/
https://docs.exabeam.com/en/advanced-analytics/cloud-delivered/advanced-analytics-user-guide/153664-get-to-know-a-user-profile.html
https://docs.exabeam.com/en/advanced-analytics/i56/advanced-analytics-administration-guide/125371-configure-advanced-analytics.html#UUID-471e24ff-903c-5af6-6901-21f028485ad9
https://community.exabeam.com/s/article/Dynamic-Multi-Peer-Groups

Another Type of Context: Two Types

Dynamic Peer Grouping



Dynamic Peer Grouping

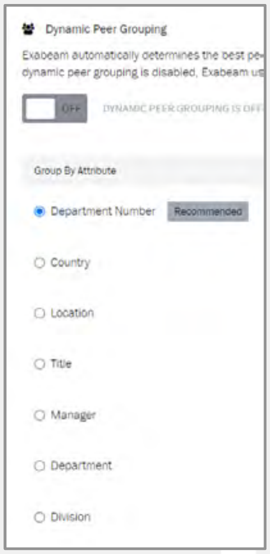
Exabeam automatically determines the best peer grou
dynamic peer grouping is disabled. Exabeam uses stat

ON DYNAMIC PEER GROUPING IS ON

Group By Attribute

- ☑ Department Number Recommended
- ☑ Group
- ☑ Country
- ☑ Location
- ☑ Title
- ☑ Manager
- ☑ Department
- ☑ Division

Static Peer Grouping



Dynamic Peer Grouping

Exabeam automatically determines the best pe
dynamic peer grouping is disabled. Exabeam us

OFF DYNAMIC PEER GROUPING IS OFF

Group By Attribute

- ● Department Number Recommended
- ○ Country
- ○ Location
- ○ Title
- ○ Manager
- ○ Department
- ○ Division

Student Notes

With dynamic peer grouping enabled, Advanced Analytics automatically determines the best possible peer group(s) for a user based on their activities. This allows for more accurate analysis and scoring of anomalies across multiple peer groups. With multi-peer grouping enabled, each user in an organization can belong to multiple peer groups. The groups can be any group in Active Directory. With multi-peer grouping turned off, users will belong to the peer group they are assigned in Active Directory. On the user page, Advanced Analytics displays all the peer groups for each user along with the degree of membership of the user to the groups; this appears in the form of a word cloud.

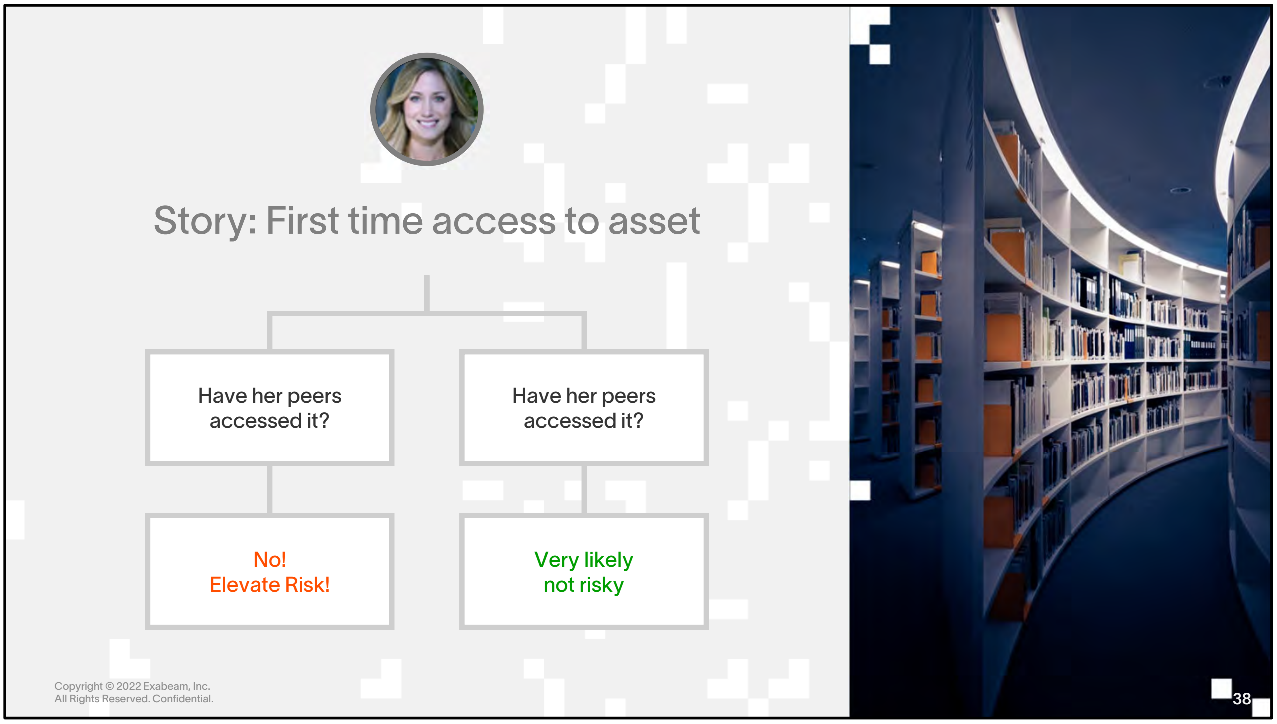
Peer group anomalies for a user session could be triggered due to anomalous behaviors across one or more peer groups. The risk score of a specific peer group rule within a session is aggregated on the risk reasons and the timeline page. The analyst can select a peer group based triggered rule, expand and get additional details on the possible peer groups, the degree of membership for each group and a visual indication of which peer groups generated anomalies. On a specific triggered rule, the analyst can see the histograms for all peer groups. When dynamic peer grouping is disabled, Advanced Analytics leverages existing static single peer group selection (such as Department, Division, Manager, Title etc.). NOTE Please read the knowledge base article titled Dynamic Multi-Peer Group Scoring for more detailed information on dynamic peer grouping as well as configuration information.

References

https://www.exabeam.com/ueba/who-do-i-belong-to-dynamic-peer-analysis-for-ueba-explained/

More Information

https://docs.exabeam.com/en/advanced-analytics/cloud-delivered/advanced-analytics-user-guide/153664-get-to-know-a-user-profile.html
https://docs.exabeam.com/en/advanced-analytics/i56/advanced-analytics-administration-guide/125371-configure-advanced-analytics.html#UUID-471e24ff-903c-5af6-6901-21f028485ad9



Story: First time access to asset

Have her peers accessed it?

Have her peers accessed it?

No!
Elevate Risk!

Very likely
not risky

More Information

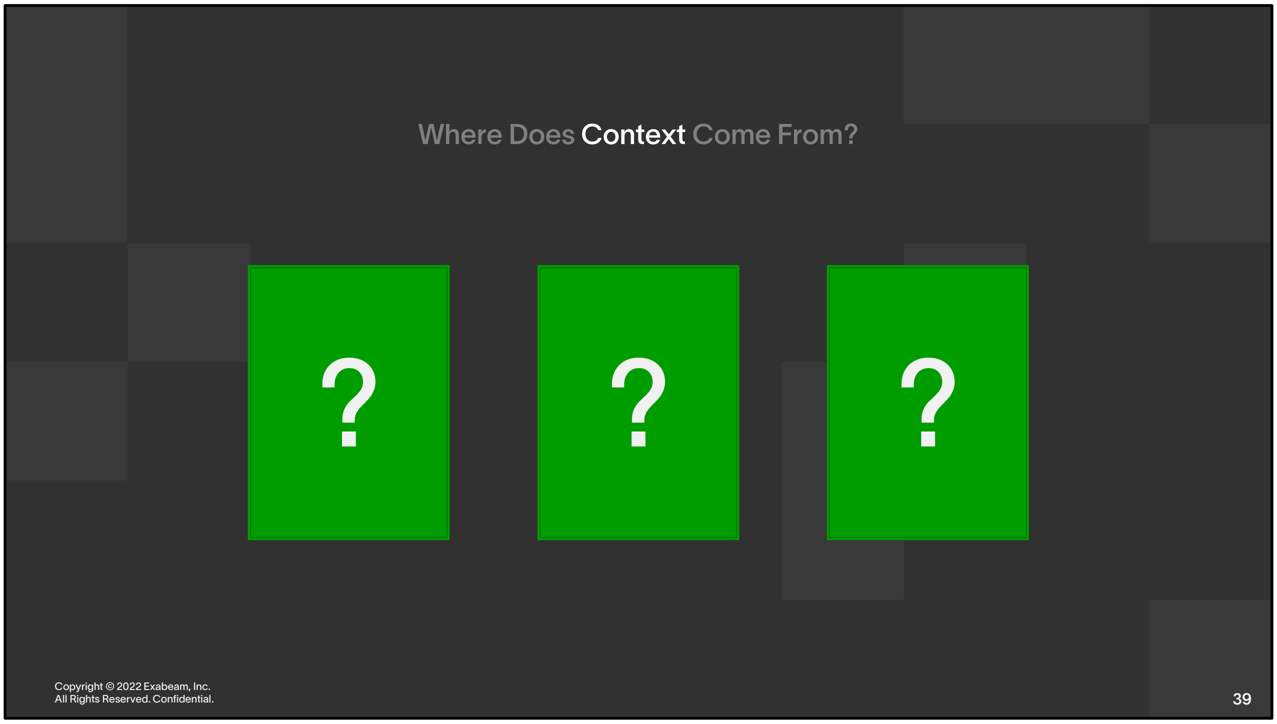
https://www.exabeam.com/information-security/first-time-access-asset-risky-not-machine-learning-question/

https://www.exabeam.com/ueba/who-do-i-belong-to-dynamic-peer-analysis-for-ueba-explained/

References

https://www.exabeam.com/ueba/who-do-i-belong-to-dynamic-peer-analysis-for-ueba-explained/
https://docs.exabeam.com/en/advanced-analytics/cloud-delivered/advanced-analytics-user-guide/153664-get-to-know-a-user-profile.html
https://docs.exabeam.com/en/advanced-analytics/i56/advanced-analytics-administration-guide/125371-configure-advanced-analytics.html#UUID-471e24ff-903c-5af6-6901-21f028485ad9
https://community.exabeam.com/s/article/Dynamic-Multi-Peer-Groups

{Photo by Martin Adams on Unsplash}



Where Does **Context** Come From?

?

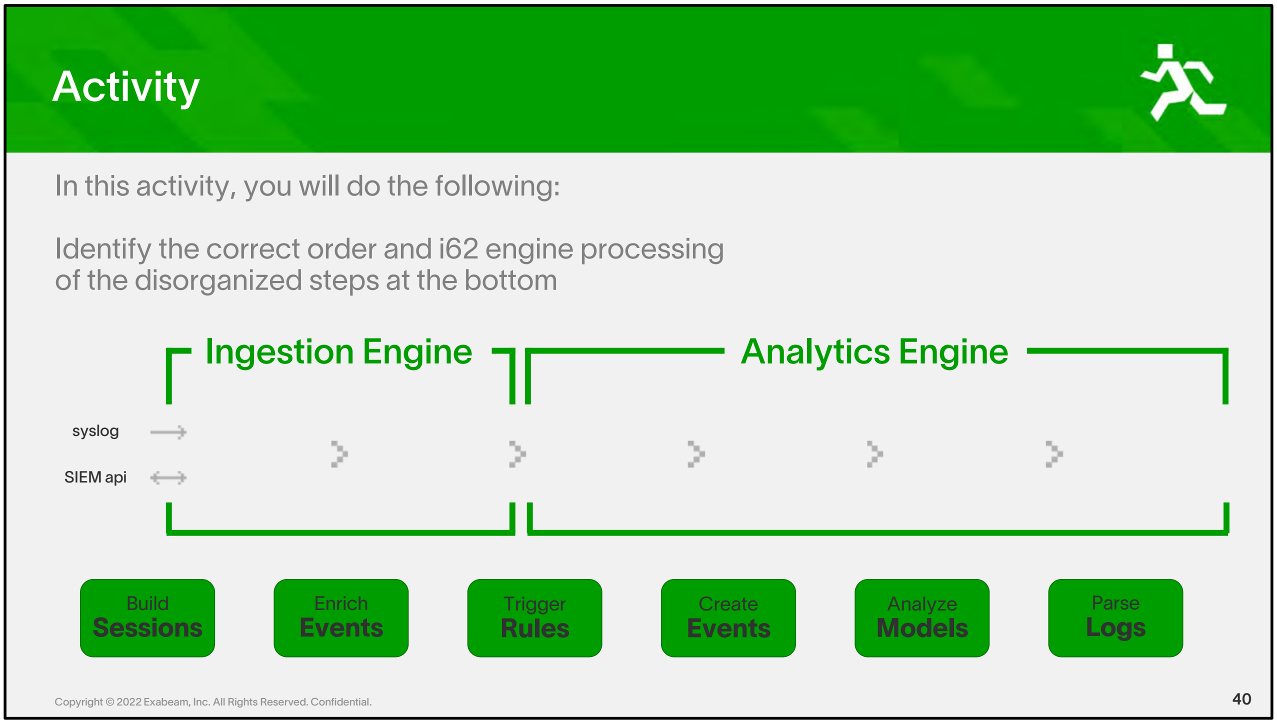
?

?

Student Notes
Context comes from multiple sources. The analytics engine can produce context with things like Risk Score, the Smart Timeline, and Dynamic Peer Grouping. Context data can also come from context tables.

Context tables are lists of resources. For example, these resources can range from assets (i.e., computers, servers) or users (employees of the company) to a list of IPs and Internet domains. While logs show what users and entities are doing, context tables can provide context by showing **who** the users and entities are. Some context tables come out-of-the-box. Others can be created and managed by administrators.

References
https://docs.exabeam.com/en/advanced-analytics/i56/advanced-analytics-administration-guide/125371-configure-advanced-analytics.html#UUID-c64778c2-4af7-96fd-8ea6-7a43aa7c9d8e
https://community.exabeam.com/s/article/Context-Tables



Activity

In this activity, you will do the following:

Identify the correct order and i62 engine processing of the disorganized steps at the bottom

Build **Sessions**

Enrich **Events**

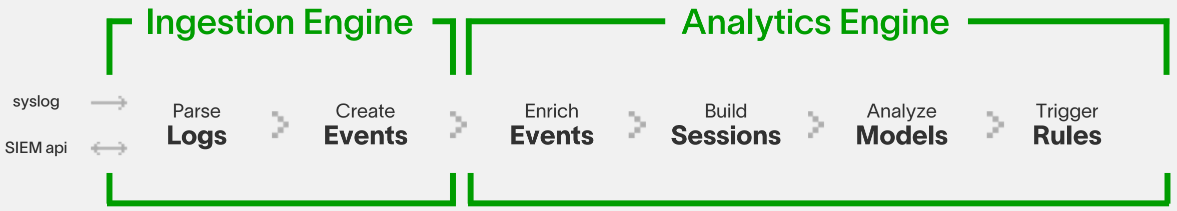
Trigger **Rules**

Create **Events**

Analyze **Models**

Parse **Logs**

Activity Answer



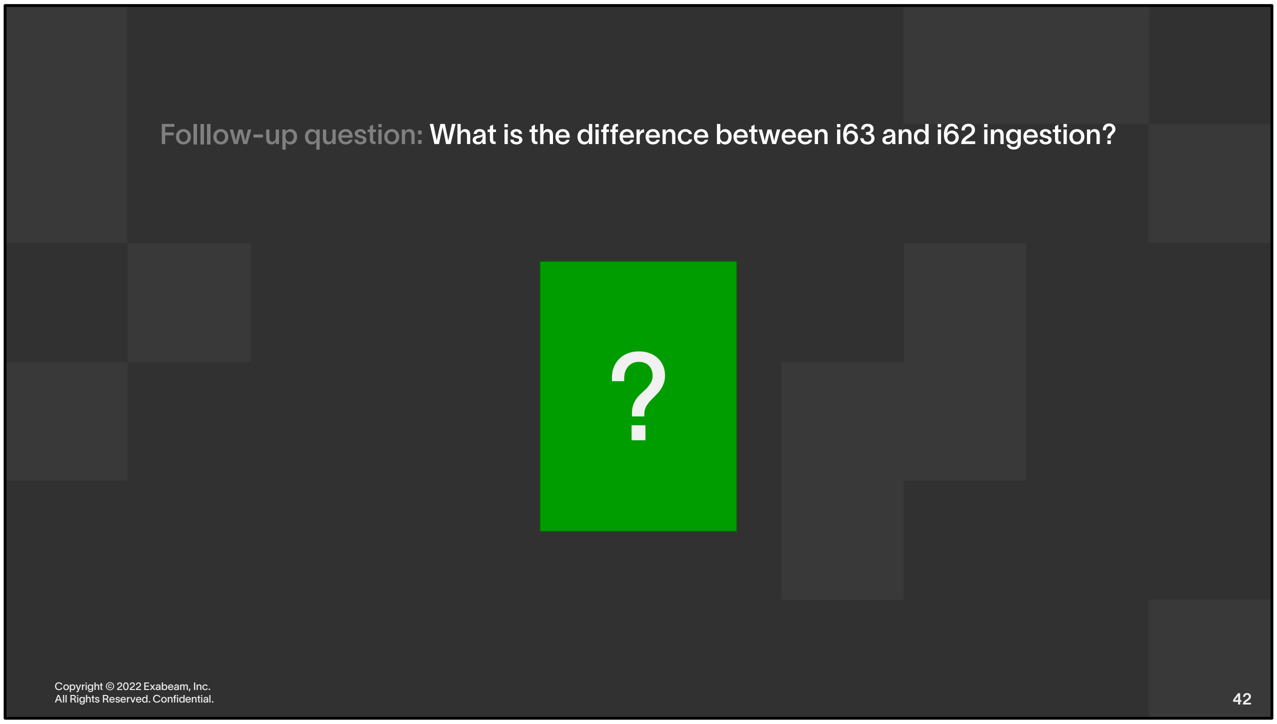
Ingestion Engine

syslog → SIEM api ↔

Parse **Logs** › Create **Events**

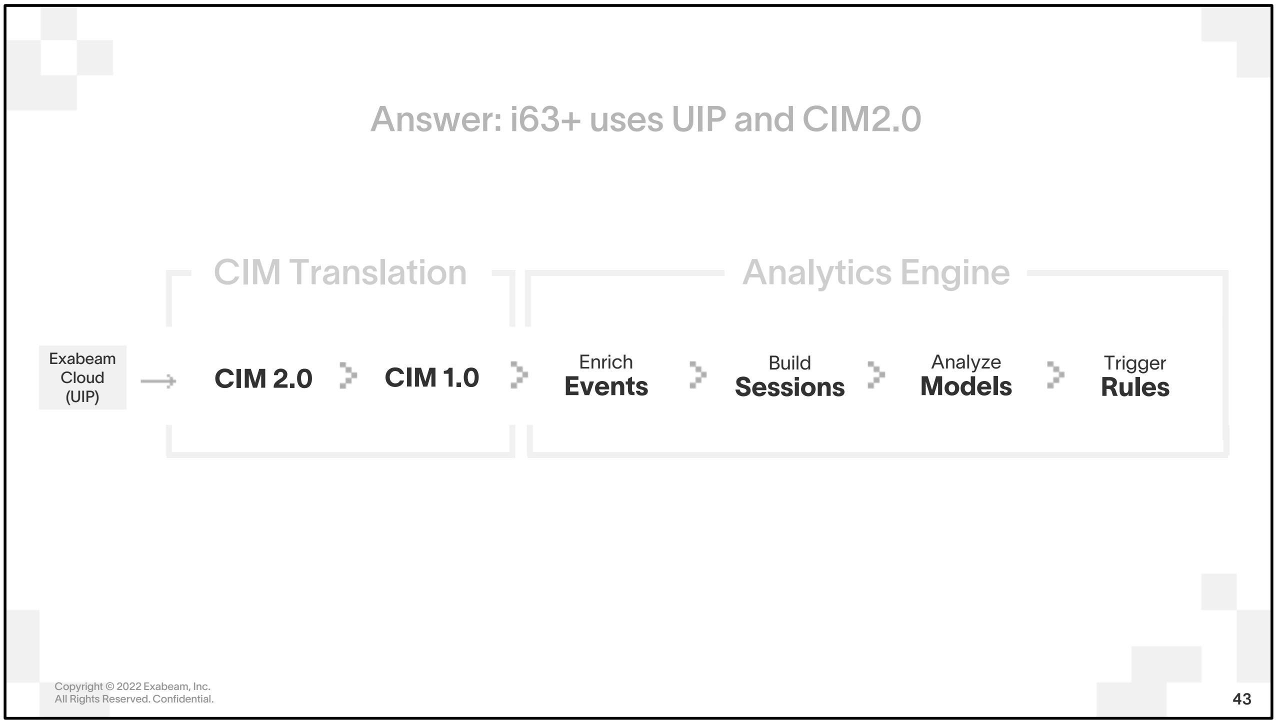
Analytics Engine

Enrich **Events** › Build **Sessions** › Analyze **Models** › Trigger **Rules**



Folllow-up question: What is the difference between i63 and i62 ingestion?

?

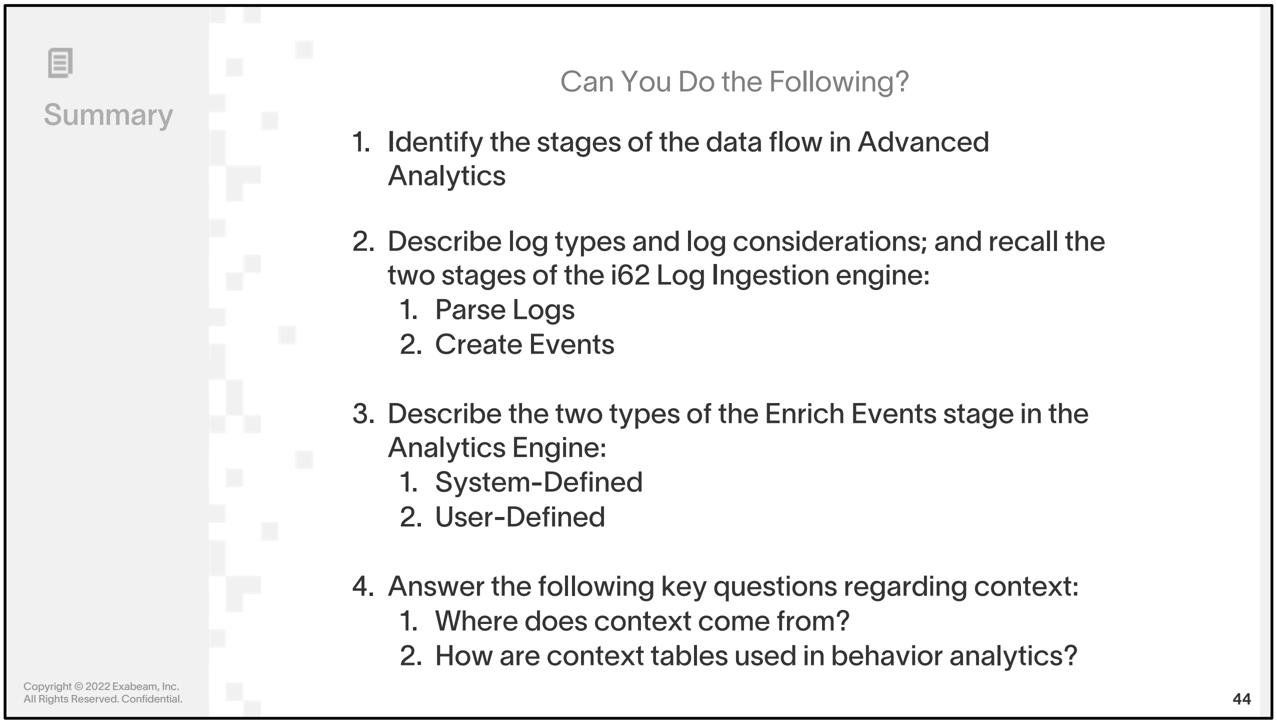


Answer: i63+ uses UIP and CIM2.0

CIM Translation

Analytics Engine

Exabeam Cloud (UIP) → CIM 2.0 › CIM 1.0 › Enrich **Events** › Build **Sessions** › Analyze **Models** › Trigger **Rules**



Summary

Can You Do the Following?

1. Identify the stages of the data flow in Advanced Analytics

2. Describe log types and log considerations; and recall the two stages of the i62 Log Ingestion engine:
   1. Parse Logs
   2. Create Events

3. Describe the two types of the Enrich Events stage in the Analytics Engine:
   1. System-Defined
   2. User-Defined

4. Answer the following key questions regarding context:
   1. Where does context come from?
   2. How are context tables used in behavior analytics?

v4.00

exabeam

How the Smart Timeline™ is Created in Advanced Analytics

EDU-2170 : Module 4

Are zero-day threats worth spending time on?

Copyright © 2022 Exabeam, Inc.
All Rights Reserved. Confidential.

2

Student Notes

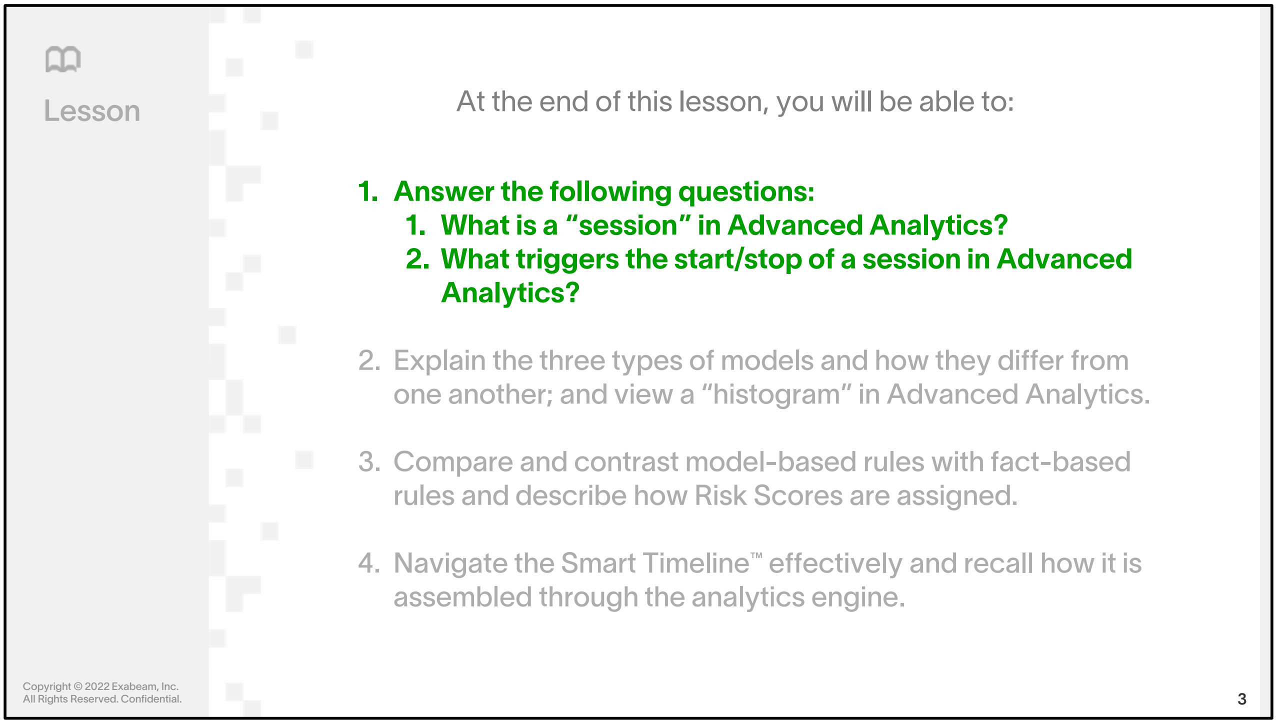
Zero-day attacks are difficult to detect, and many legacy security tools miss them, especially tools that are based on signatures. Because of this, some may think its silly to waste hours on zero days. However, some industries and regions spend a lot of time on zero days because they either have the expertise or do not have any risk tolerance. Because Advanced Analytics is focused on anomalies rather than alerts, it helps detect zero-days and unknown malware. Here are 10 ways that Advanced Analytics can help your organization, including against zero-day and unknown attacks:

1.Block attacks – Advanced Analytics provides AI-based analysis and behavioral threat protection that can help stop known and unknown attacks, including exploits, malware and fileless attacks.
2.Gain visibility – Advanced Analytics collects and correlates data across networks, endpoints, and cloud environments and applies it to detection, triaging, investigating, hunting and threat response processes.
3.24/7 automated detection – Advanced Analytics continuously applies AI-based analytics as well as custom rules that help detect advanced persistent threats (APTs) as well as any other covert attack such as lateral movement, malicious insiders, compromised insiders, etc.
4.Prevent alert fatigue – Advanced Analytics uses automated root cause analysis alongside a unified incident engine to triage alerts and dramatically reduce alerts. This can help prevent alert fatigue, avoid personnel turnover, and streamline incident response.
5.Increase SOC productivity – Advanced Analytics helps consolidate security policy management as well as monitoring, investigations and response across networks, endpoints and clouds into one console.
6.Eradicate threats – Advanced Analytics enables teams to shut down attacks with surgical precision without causing business disruption.
7.Eliminate advanced threats – Advanced Analytics can help protect the corporate network against malicious insiders, compromised insiders, external threats, policy violations, ransomware, advanced zero-day malware, and fileless and memory-only attacks.
8.Improve your security team – Advanced Analytics can help detect indicators of compromise (IOCs) as well as anomalous behavior. It can also prioritize analysis using incident scoring. This can help disrupt all stages of an attack
9.Restore hosts to a clean state – Advanced Analytics can provide remediation suggestions to help you quickly recover from an attack. For example, how to remove malicious files and registry keys, and how to restore damaged files and registry keys.

10. Analyze third party-data sources – Advanced Analytics enables you to extend detection, investigation and response to external sources. For example, performing behavioral analytics on logs collected from third-party firewalls.

Source

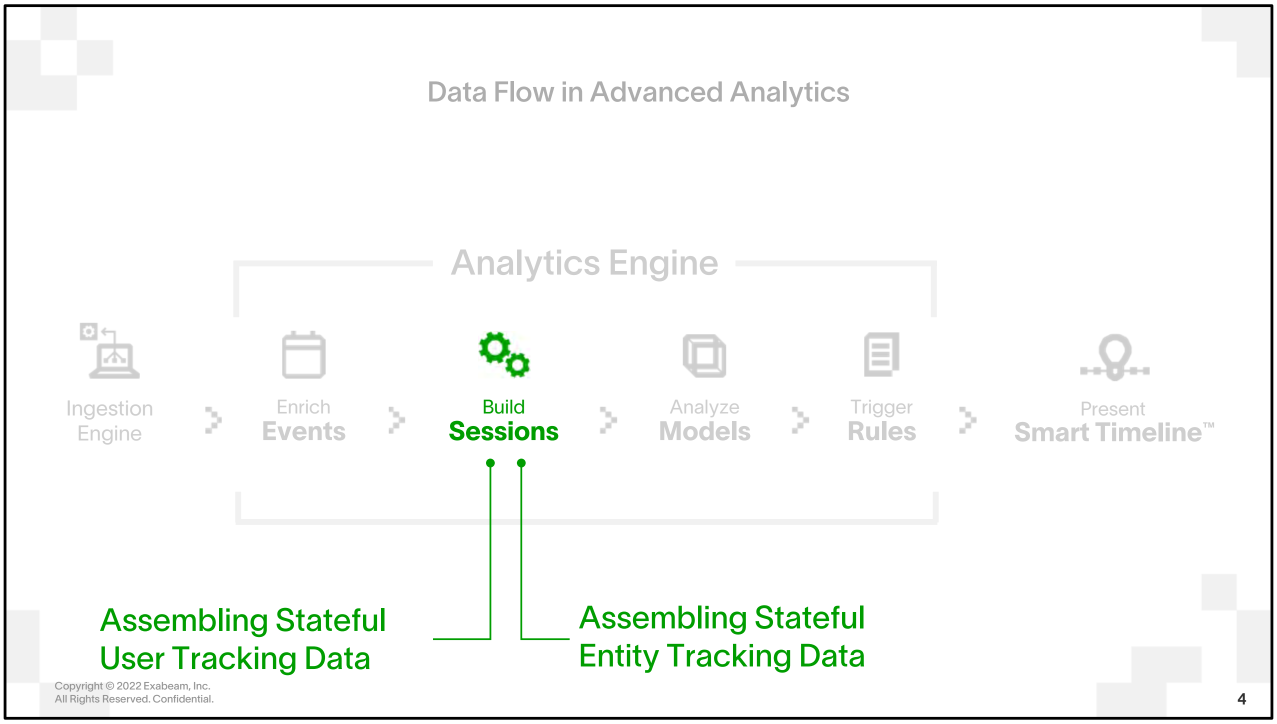
https://www.exabeam.com/information-security/Advanced Analytics-security-10-ways-Advanced Analytics-enhances-your-security-posture/



Lesson

At the end of this lesson, you will be able to:

1. **Answer the following questions:**
   1. **What is a "session" in Advanced Analytics?**
   2. **What triggers the start/stop of a session in Advanced Analytics?**
2. Explain the three types of models and how they differ from one another; and view a "histogram" in Advanced Analytics.
3. Compare and contrast model-based rules with fact-based rules and describe how Risk Scores are assigned.
4. Navigate the Smart Timeline™ effectively and recall how it is assembled through the analytics engine.



Data Flow in Advanced Analytics

Assembling Stateful User Tracking Data

Assembling Stateful Entity Tracking Data

Student Notes

Sessions are the buckets in which events are stitched together to form a coherent picture. Sessions are built for each user that has discovered events and for each entity (based on IP and host identifiers).

Sessions include stateful user tracking and entity tracking to weave into coherent timelines for investigation and context.

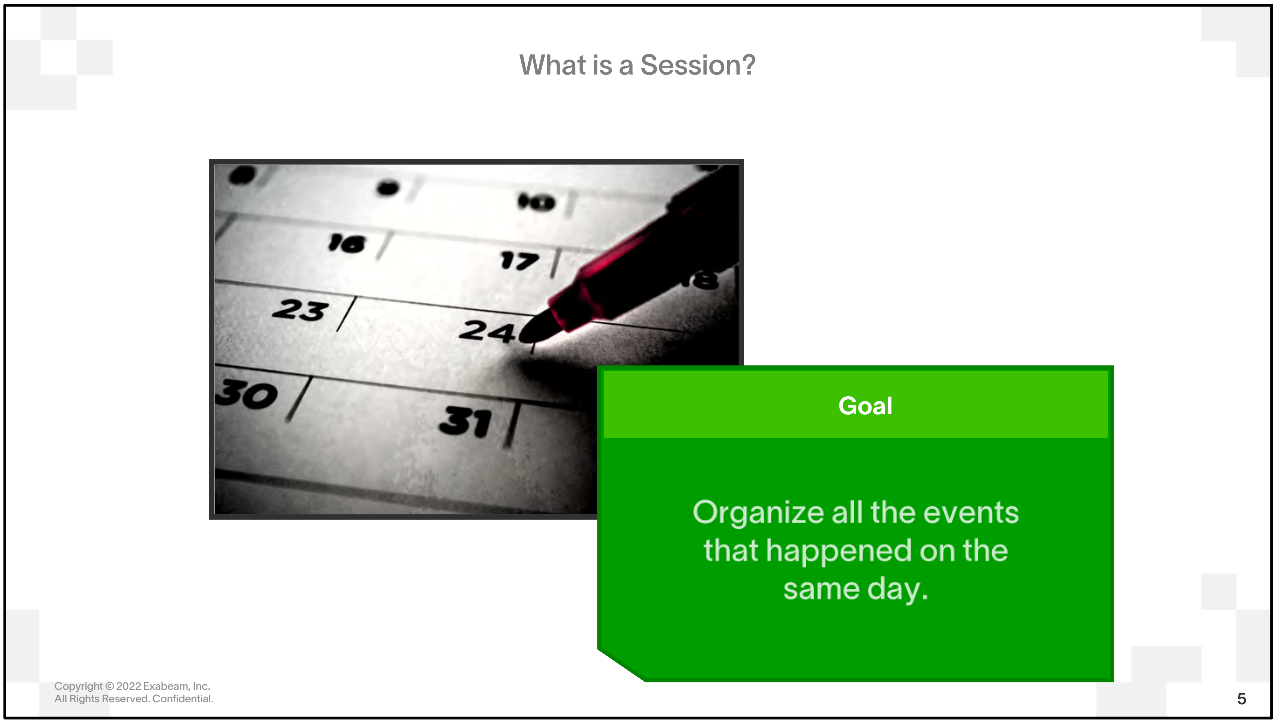
“**Security log data is stateless**…a platform must be able to piece events together to track the state of data, and ultimately, a user’s behavior.” -Derek Lin, Exabeam Chief Data Scientist

Source

https://www.exabeam.com/ueba/data-science-and-stateful-user-tracking-the-two-key-uba-enablers/

More information

https://www.exabeam.com/ueba/data-science-and-stateful-user-tracking-the-two-key-uba-enablers/



What is a Session?

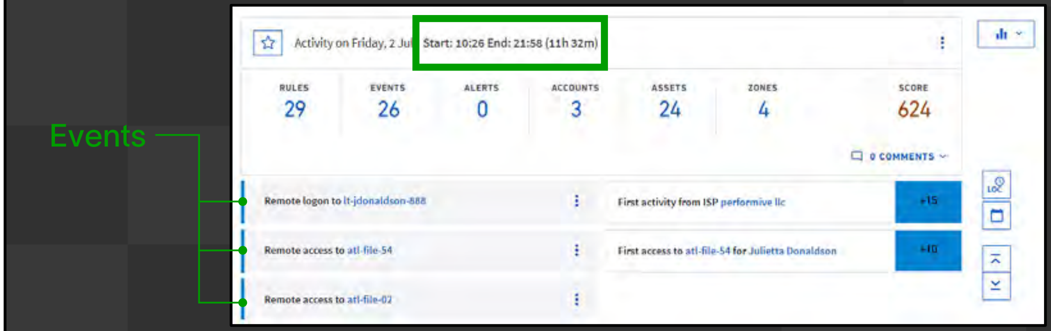
Goal

Organize all the events that happened on the same day.

Student Notes

When viewing a Smart Timeline in Advanced Analytics analysts want to be able to see information in a way that is organized in an easy to understand calendar like format. To define that format the analytics engine uses sessions.

What is a Session used for?



Activity on Friday, 2 Jul Start: 10:26 End: 21:58 (11h 32m)

RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES	SCORE
29	26	0	3	24	4	624

0 COMMENTS

Remote logon to lt-jdonaldson-888 — First activity from ISP performive llc +15

Remote access to atl-file-54 — First access to atl-file-54 for Julietta Donaldson +10

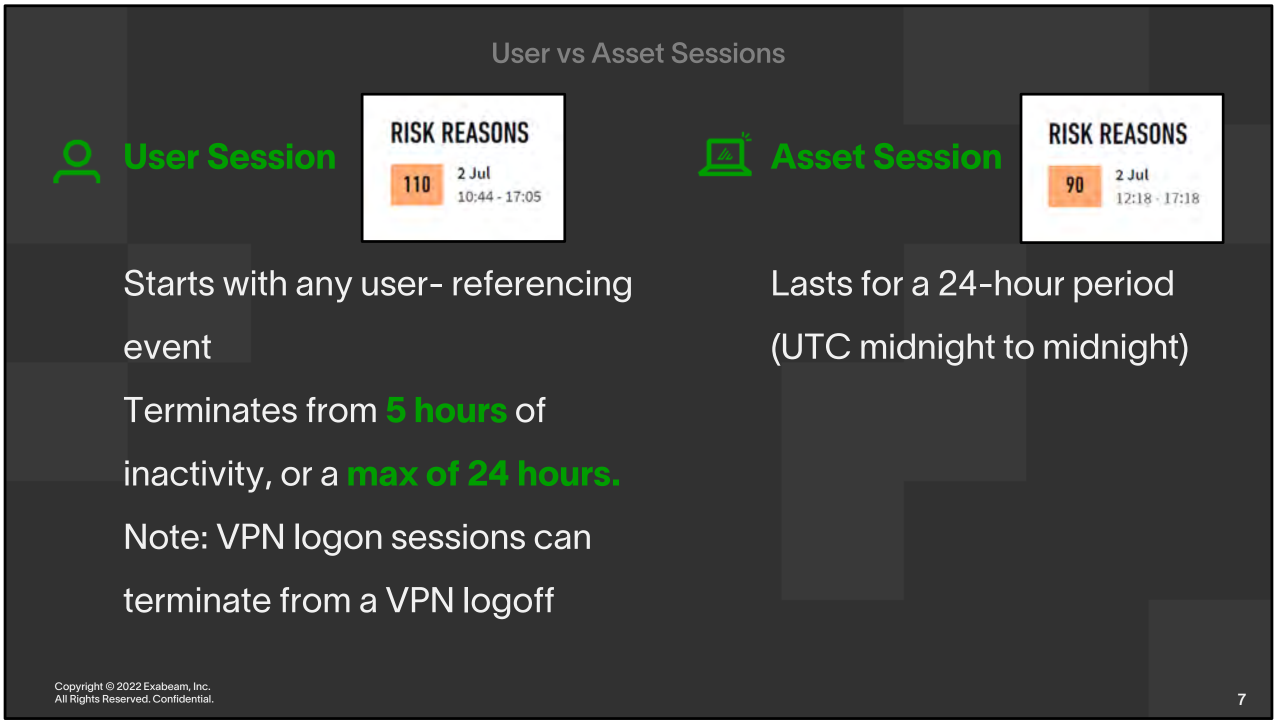
Remote access to atl-file-02

A logical **“container”** viewed in the Smart Timeline.

Student Notes:

Fundamental to the Smart Timeline and to user state tracking is the concept of a session.

A session is a kind of container that holds related events together.



User vs Asset Sessions

User Session

RISK REASONS
110 2 Jul 10:44 - 17:05

Starts with any user- referencing event

Terminates from **5 hours** of inactivity, or a **max of 24 hours.**

Note: VPN logon sessions can terminate from a VPN logoff

Asset Session

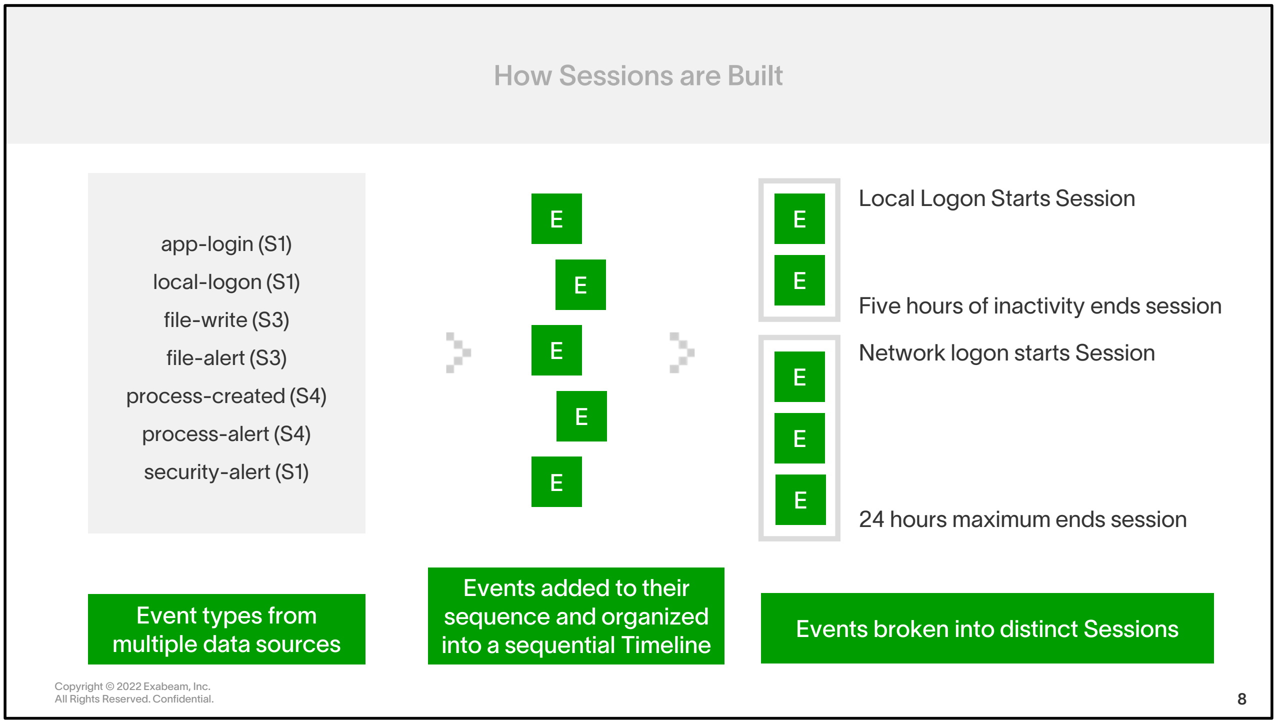
RISK REASONS
90 2 Jul 12:18 - 17:18

Lasts for a 24-hour period (UTC midnight to midnight)

Student Notes

User Session represents all the events that Exabeam attributes to an individual user in a timeframe (after 5 hours of user inactivity or 24 hours of maximum duration, Exabeam closes the user session). Typically, user sessions are one day of activity, but there can be multiple user sessions in a day. Exabeam collects event logs that relate to the user's assets and activities and defines these as a logical user session.

Asset Session represents all the events that Exabeam attributes to an individual asset in a timeframe. Asset Sessions are similar to User Sessions in that they are a logical container of event logs related to the asset's activities, however an Asset Session lasts for one 24-hour period, from midnight UTC to midnight UTC.



How Sessions are Built

app-login (S1)
local-logon (S1)
file-write (S3)
file-alert (S3)
process-created (S4)
process-alert (S4)
security-alert (S1)

Local Logon Starts Session

Five hours of inactivity ends session

Network logon starts Session

24 hours maximum ends session

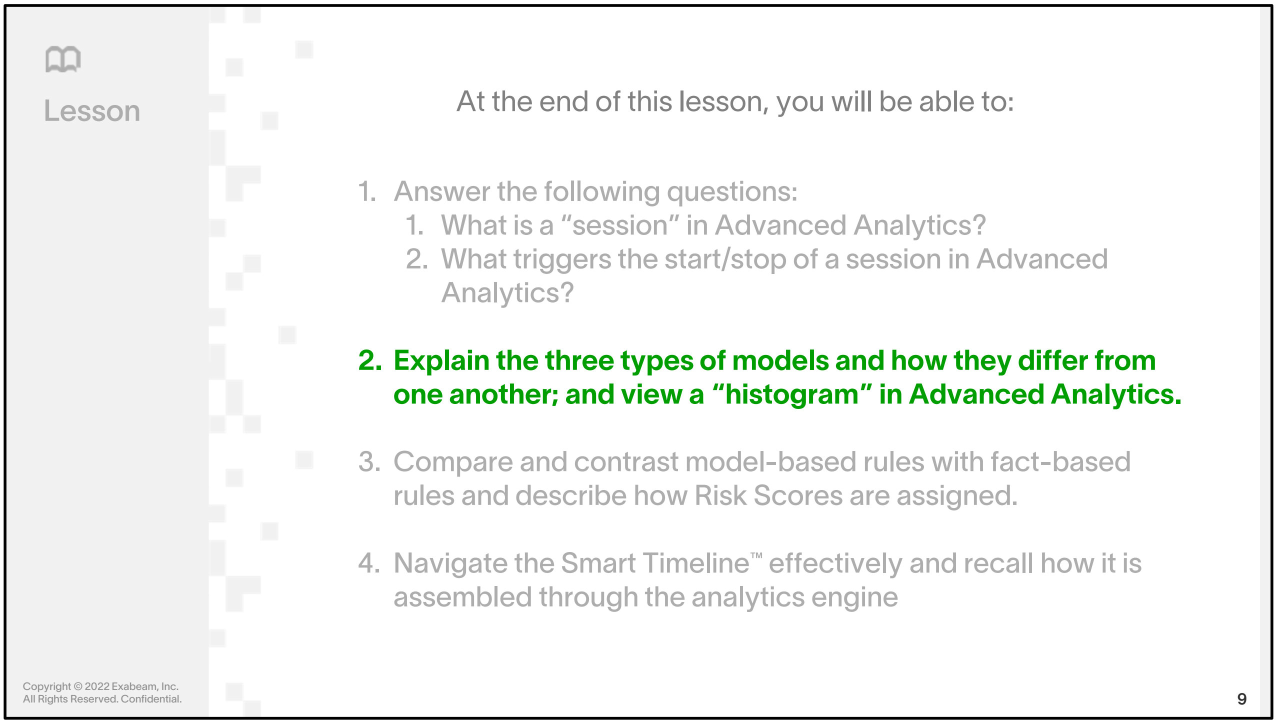
Event types from multiple data sources

Events added to their sequence and organized into a sequential Timeline

Events broken into distinct Sessions

Student Notes

Event data from one or more sources are parsed into events, enriched, and then grouped into sessions. Sessions are a bucket used to hold common events that belong together because they represent a day or activities followed by a five-hour period of inactivity.



Lesson

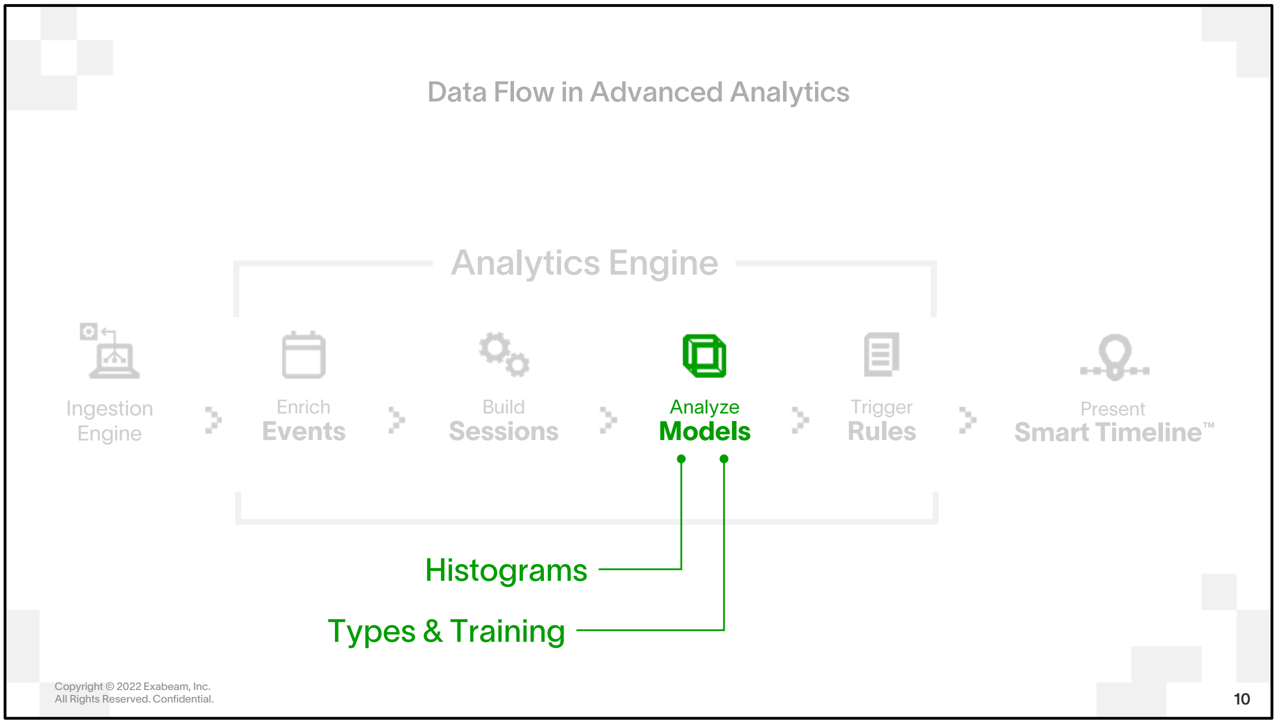
At the end of this lesson, you will be able to:

1. Answer the following questions:
    1. What is a “session” in Advanced Analytics?
    2. What triggers the start/stop of a session in Advanced Analytics?

2. **Explain the three types of models and how they differ from one another; and view a “histogram” in Advanced Analytics.**

3. Compare and contrast model-based rules with fact-based rules and describe how Risk Scores are assigned.

4. Navigate the Smart Timeline™ effectively and recall how it is assembled through the analytics engine



Data Flow in Advanced Analytics

Analytics Engine

Ingestion Engine

Enrich Events

Build Sessions

Analyze Models

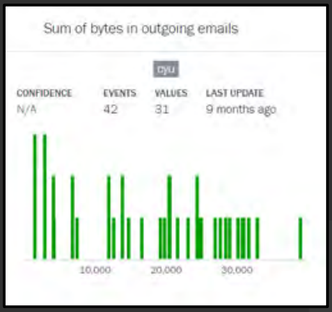
Trigger Rules

Present Smart Timeline™

Histograms

Types & Training

What are Models?



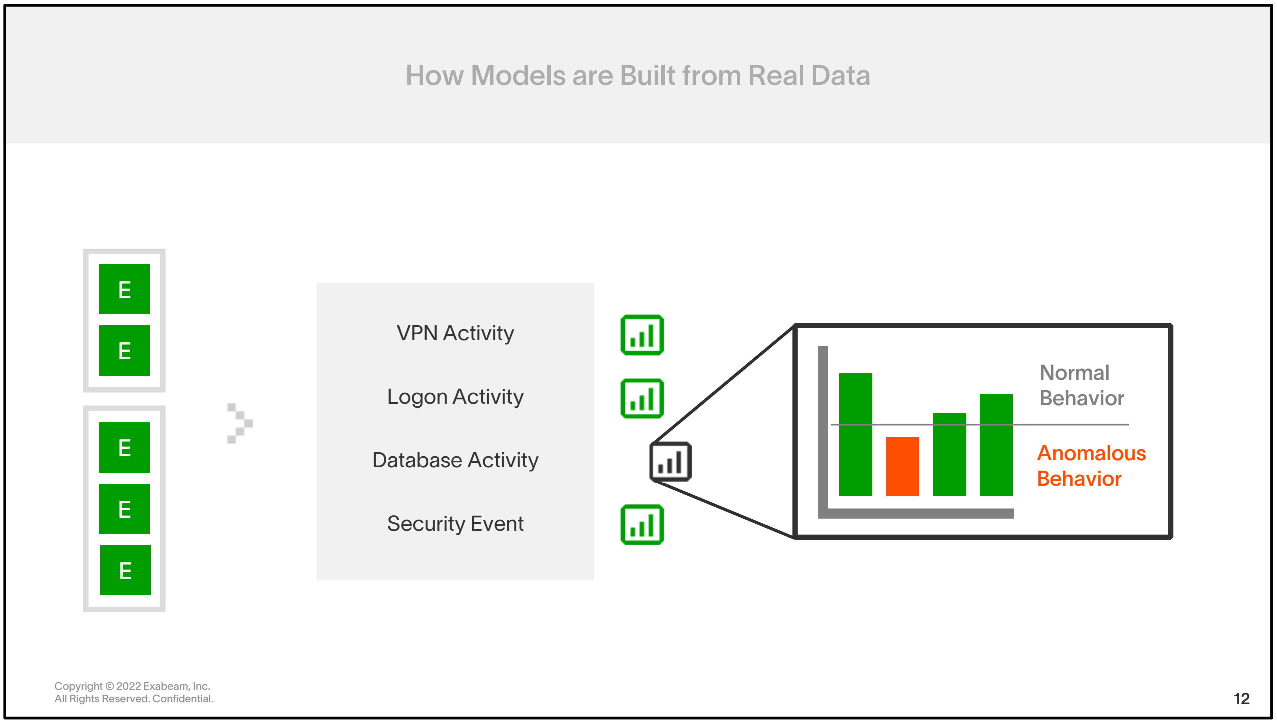
Sum of bytes in outgoing emails

cyu

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
N/A	42	31	9 months ago

Models are the mathematical key to
User And Entity Behavior Analytics (UEBA)

Student Notes
Advanced Analytics uses predictive analytics models. By gathering data from the past, it can be guessed as to what can be expected in the future.



How Models are Built from Real Data

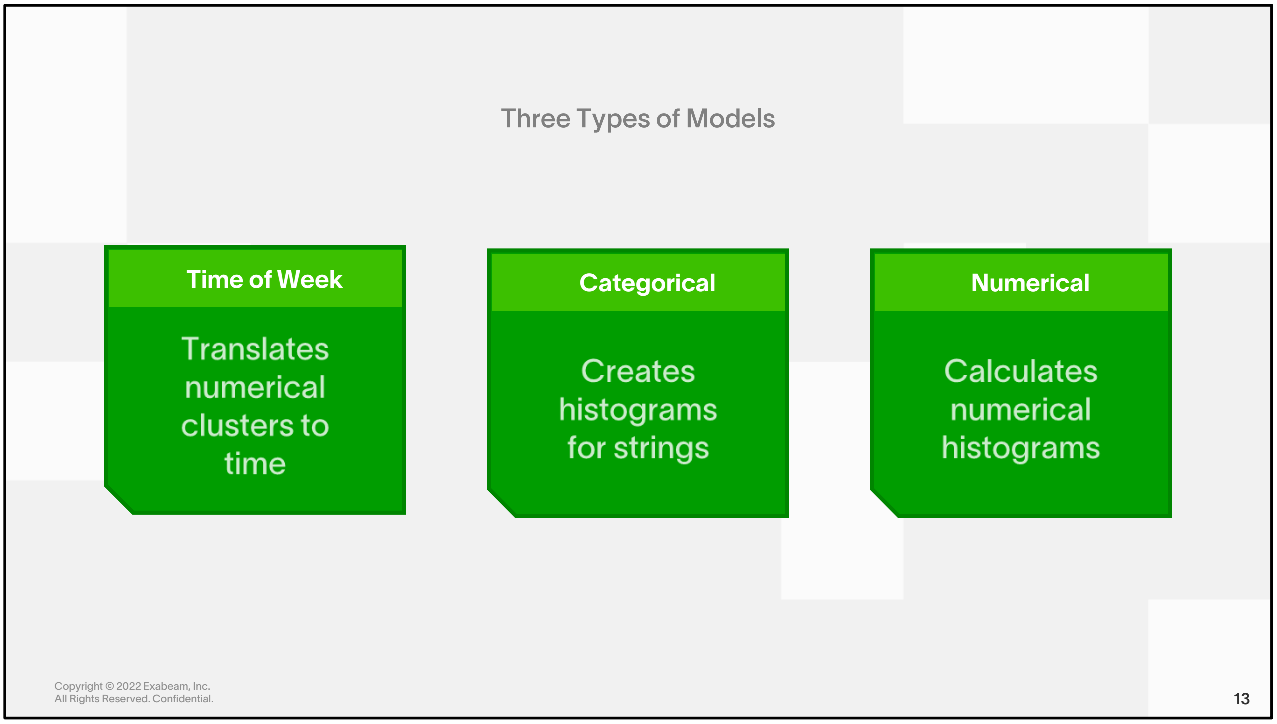
VPN Activity

Logon Activity

Database Activity

Security Event

Student Notes
Models determine what captured event data to observe. Machine learning is trained to determine the unique “normal” of the logged data at multiple levels, including, users, assets, groups, and organization wide.



Three Types of Models

Time of Week

Translates numerical clusters to time

Categorical

Creates histograms for strings

Numerical

Calculates numerical histograms

Student Notes
We will look at the three types of models that are used by Advanced Analytics to create histograms of data.

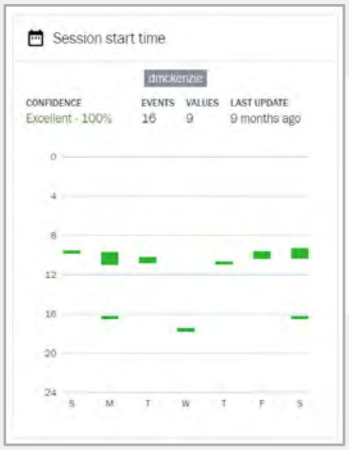
Definitions of Model Types:
Categorical is the most common. It models a string with significance: number, host name, username, etc. Where numbers fall into specific categories which cannot be quantified. When you model which host a user logs into, it is a categorical model.
Numerical Clustered involves numbers that have meaning – it builds clusters around a user's common activities so you can easily see when the user deviates from this norm. For example, you can model how many hosts a user normally accesses in a session.
Numerical Time-of-Week models when users log into their machines in a 24-hour period. It models time as a cycle so that the beginning and end of the period are close together, rather than far apart. For example, if a user logs into a machine Sunday at 11:00 pm, it is closely modeled to Monday at 12:00am.

Reference
https://docs.exabeam.com/en/advanced-analytics/i56/advanced-analytics-administration-guide/125371-configure-advanced-analytics.html#UUID-aa5d6f0f-544d-2681-b8b9-2649f4011948

Three Types of Models

Time of Week

Translates numerical clusters to time



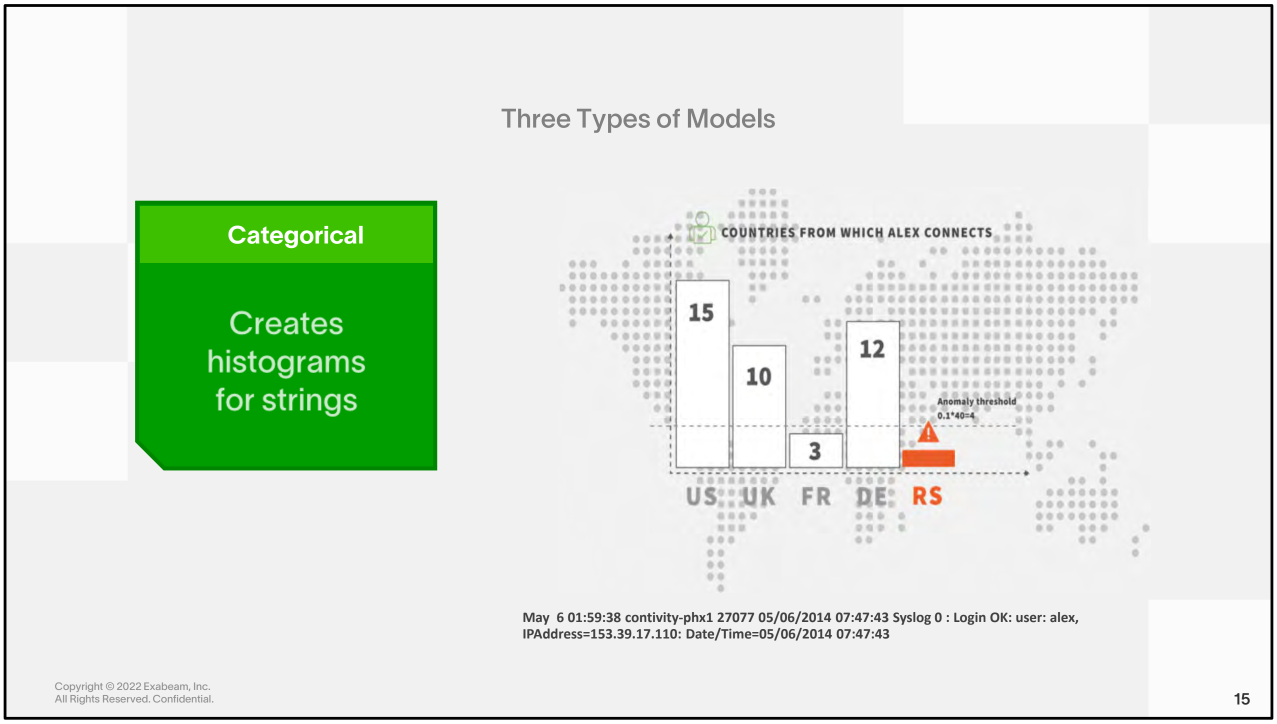
Session start time

dmckenzie

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
Excellent - 100%	16	9	9 months ago

Student Notes

Numerical Time-of-Week models when users log into their machines in a 24-hour period. It models time as a cycle so that the beginning and end of the period are close together, rather than far apart. For example, if a user logs into a machine Sunday at 11:00 pm, it is closely modeled to Monday at 12:00am.



Three Types of Models

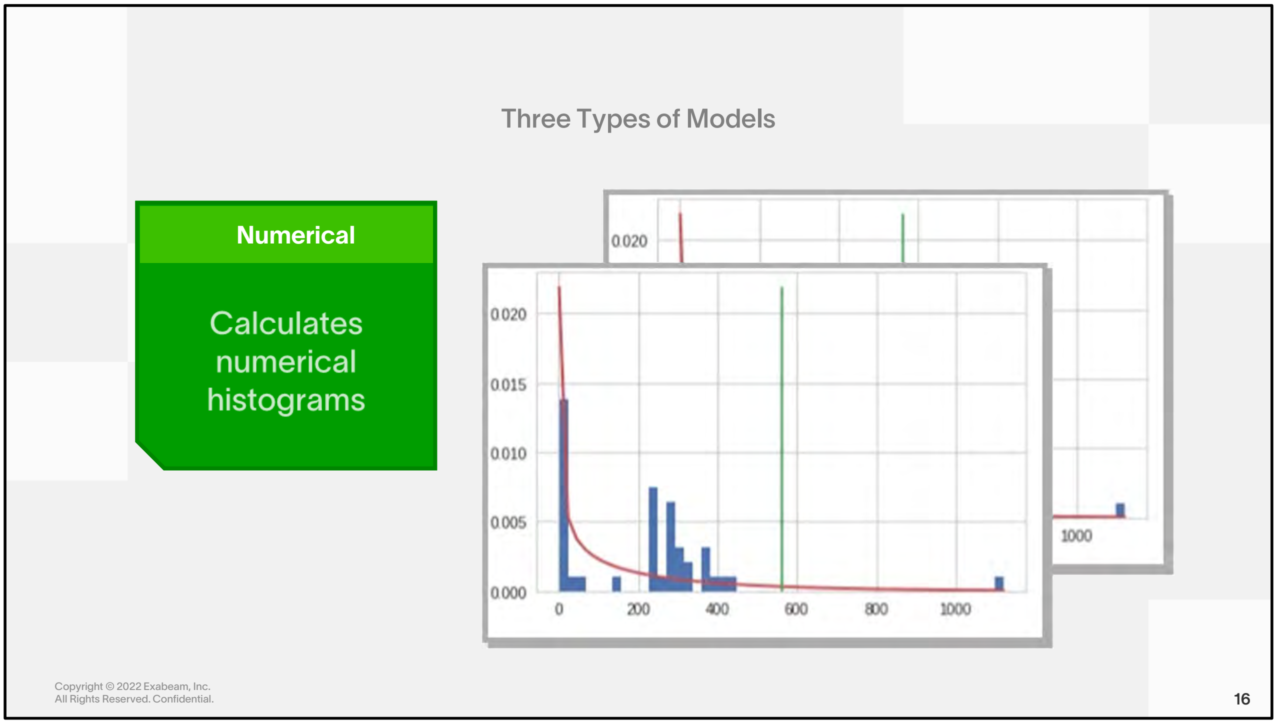
Categorical

Creates histograms for strings

May 6 01:59:38 contivity-phx1 27077 05/06/2014 07:47:43 Syslog 0 : Login OK: user: alex, IPAddress=153.39.17.110: Date/Time=05/06/2014 07:47:43

Student Notes

Categorical is the most common. It models a string with significance: number, host name, username, etc. Where numbers fall into specific categories which cannot be quantified. When you model which host a user logs into, it is a categorical model.



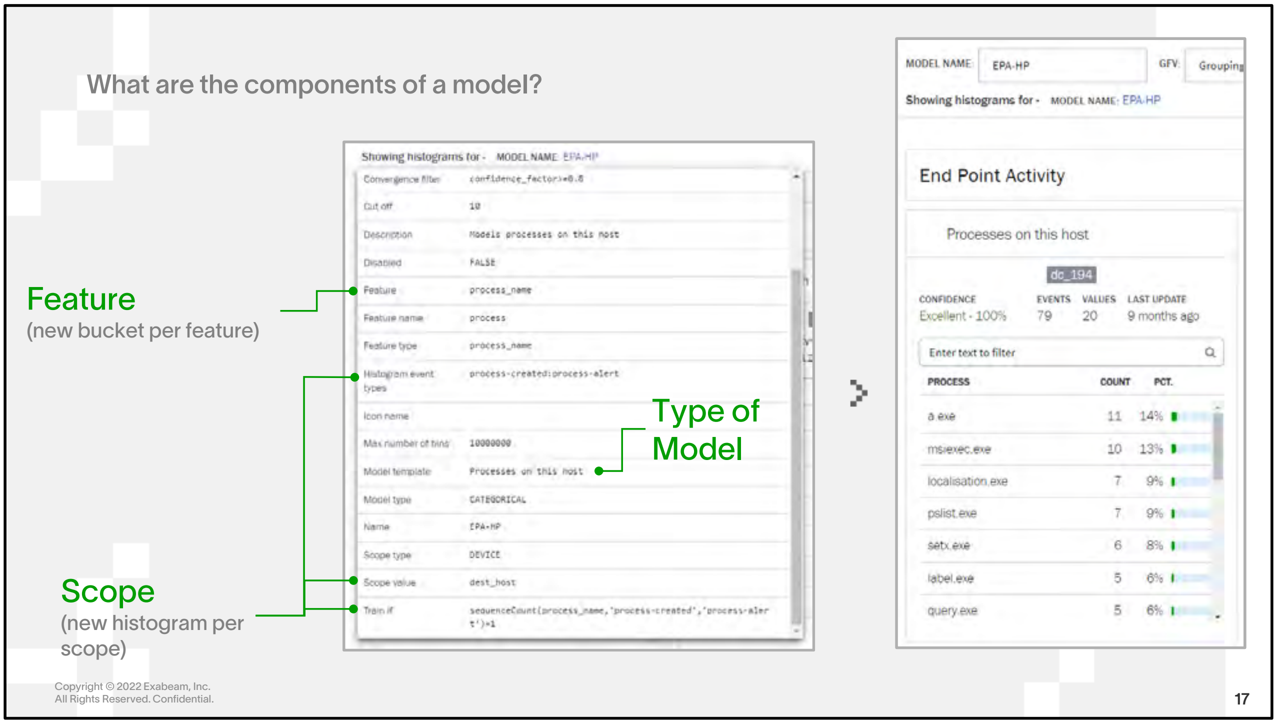
Three Types of Models

Numerical

Calculates numerical histograms

Student Notes

Numerical Clustered involves numbers that have meaning – it builds clusters around a user's common activities so you can easily see when the user deviates from this norm. For example, you can model how many hosts a user normally accesses in a session.



What are the components of a model?

Feature
(new bucket per feature)

Type of Model

Scope
(new histogram per scope)

Showing histograms for - MODEL NAME: EPA-HP

Convergence filter	confidence_factor>=0.8
Cut off	10
Description	Models processes on this host
Disabled	FALSE
Feature	process_name
Feature name	process
Feature type	process_name
Histogram event types	process-created:process-alert
Icon name	
Max number of bins	10000000
Model template	Processes on this host
Model type	CATEGORICAL
Name	EPA-HP
Scope type	DEVICE
Scope value	dest_host
Train if	sequenceCount(process_name,'process-created','process-alert')=1

MODEL NAME: EPA-HP GFV: Grouping

Showing histograms for - MODEL NAME: EPA-HP

End Point Activity

Processes on this host

dc_194

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
Excellent - 100%	79	20	9 months ago

Enter text to filter

PROCESS	COUNT	PCT.
a.exe	11	14%
msiexec.exe	10	13%
localisation.exe	7	9%
pslist.exe	7	9%
setx.exe	6	8%
label.exe	5	6%
query.exe	5	6%

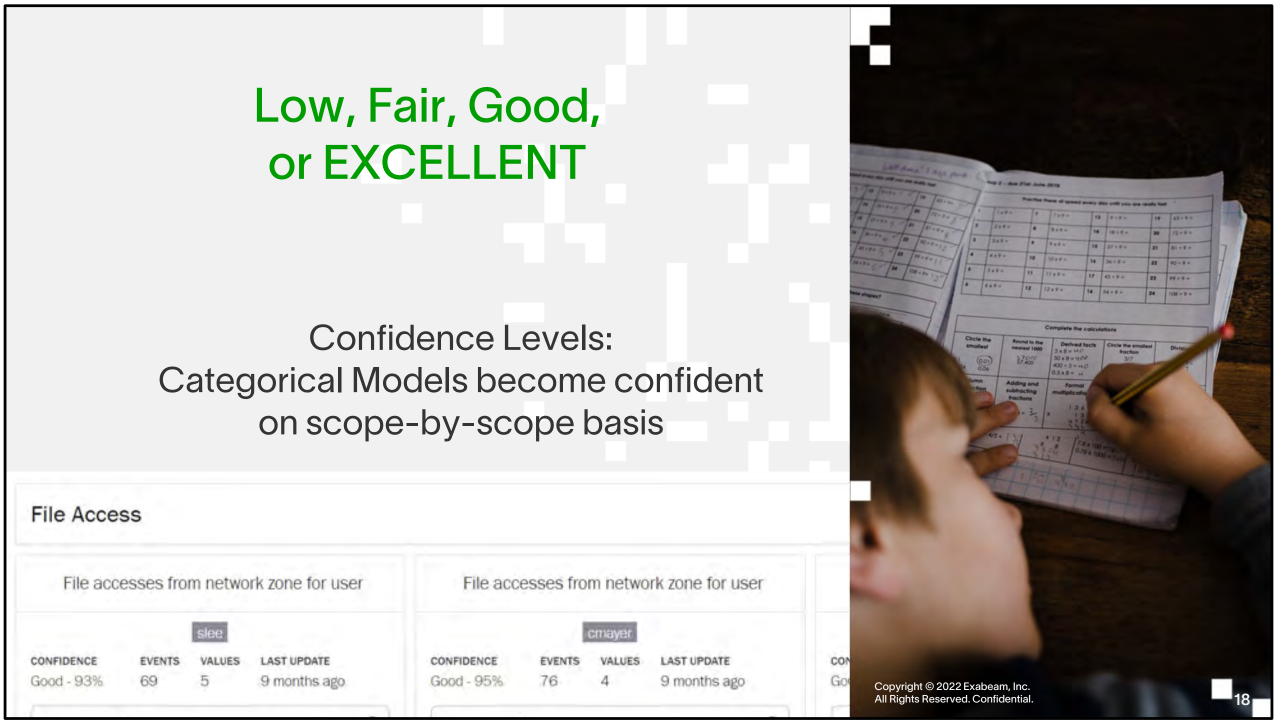
Student Notes

Since anomaly-based rules depend on models, it is helpful to have a basic understanding of how Exabeam's models work.

Our anomaly detection relies on statistical profiling of network entity behavior. Our statistical profiling is not only about user-level data. In fact, Exabeam profiles all network entities, including hosts and machines, and this extends to applications or processes, as data permits. The statistical profiling is histogram frequency based. To perform the histogram-based profiling, which requires discrete input, we incorporate a variety of methods to transform and to condition the data. Probability distributions are modeled using histograms, which are graphical representations of data. There are three different model types – categorical, numerical clustered, and numerical time-of-week.

Reference

https://docs.exabeam.com/en/advanced-analytics/i56/advanced-analytics-administration-guide/125371-configure-advanced-analytics.html#UUID-aa5d6f0f-544d-2681-b8b9-2649f4011948



Low, Fair, Good, or EXCELLENT

Confidence Levels:
Categorical Models become confident on scope-by-scope basis

File Access

File accesses from network zone for user

slee

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
Good - 93%	69	5	9 months ago

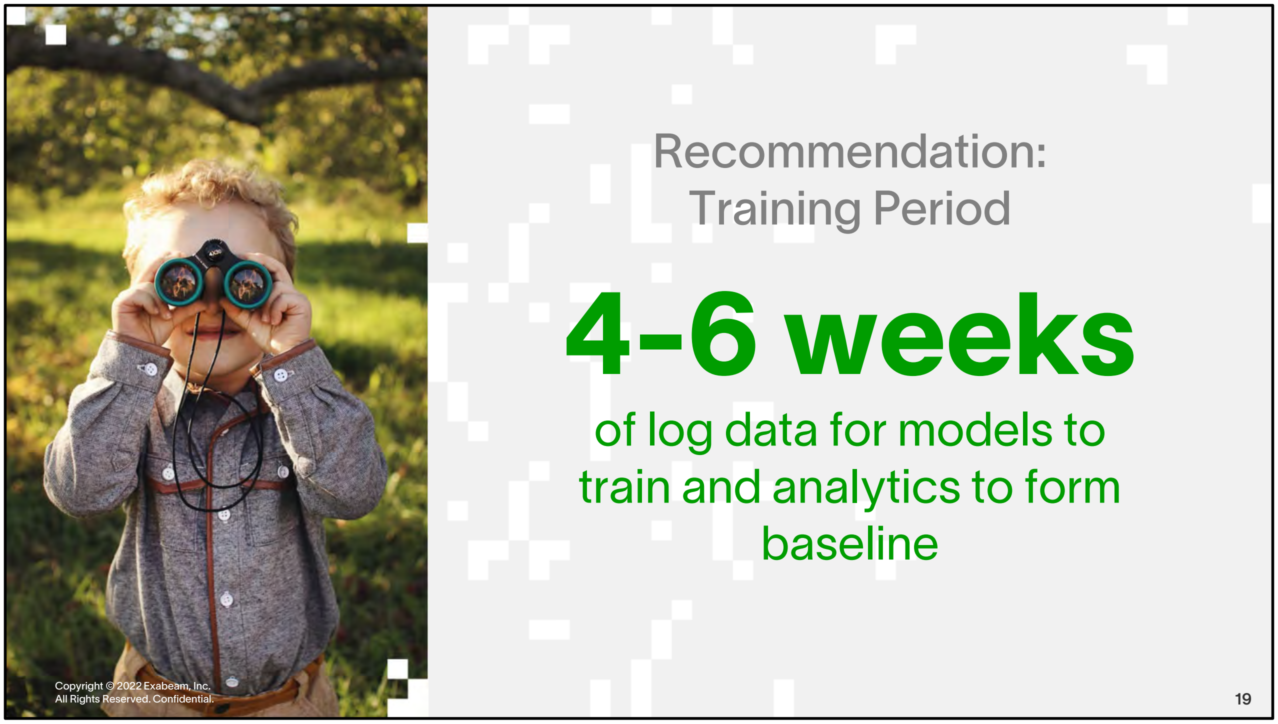
File accesses from network zone for user

cmayer

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
Good - 95%	76	4	9 months ago

Student Notes
Levels of convergence for a model based upon trained data is expressed per-scope as a confidence level.
Low = <80%
Fair = 80%-89%
Good = 90%-99%
Excellent = 100%

Remember: LOW confidence only means "We don't have enough Data" for it to be sure!! So, when does the confidence increase... when we have more data!



Recommendation: Training Period

4-6 weeks

of log data for models to train and analytics to form baseline

Student Notes
Predictive analysis requires data to be useful. There has to be a baseline in order to compare it with. The more data the more accurate a model can usually be.

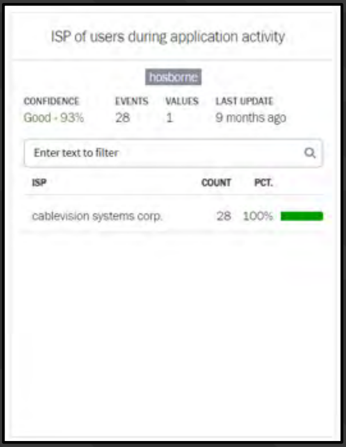
MODEL AGING
Over time, models built in your deployment naturally become outdated. For example, if an employee moves to a different department or accepts a promotion and they do not adhere to the same routines, access points, or other historical regularities.

We automatically clean up and rebuild all models on a regular basis (default is every 16 weeks) to ensure your models are as accurate and up-to-date as possible. This process also enhances system performance by cleaning out unused or underutilized models.

{Photo by Jen Theodore on Unsplash}

What are Histograms?

Table



ISP of users during application activity

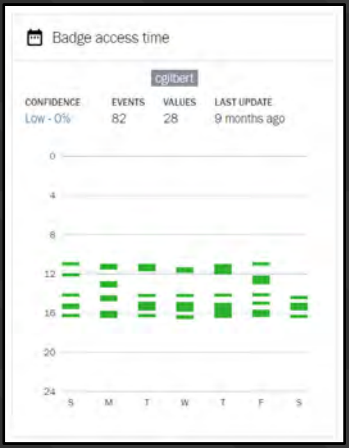
hosborne

CONFIDENCE Good - 93%
EVENTS 28
VALUES 1
LAST UPDATE 9 months ago

Enter text to filter

ISP	COUNT	PCT.
cablevision systems corp.	28	100%

Time of Week



Badge access time

cgilbert

CONFIDENCE Low - 0%
EVENTS 82
VALUES 28
LAST UPDATE 9 months ago

Student Notes

Histogram definition: A histogram is a visualization of statistical information that uses rectangles to show the frequency of data items in successive numerical intervals of equal size.

Types of Histograms

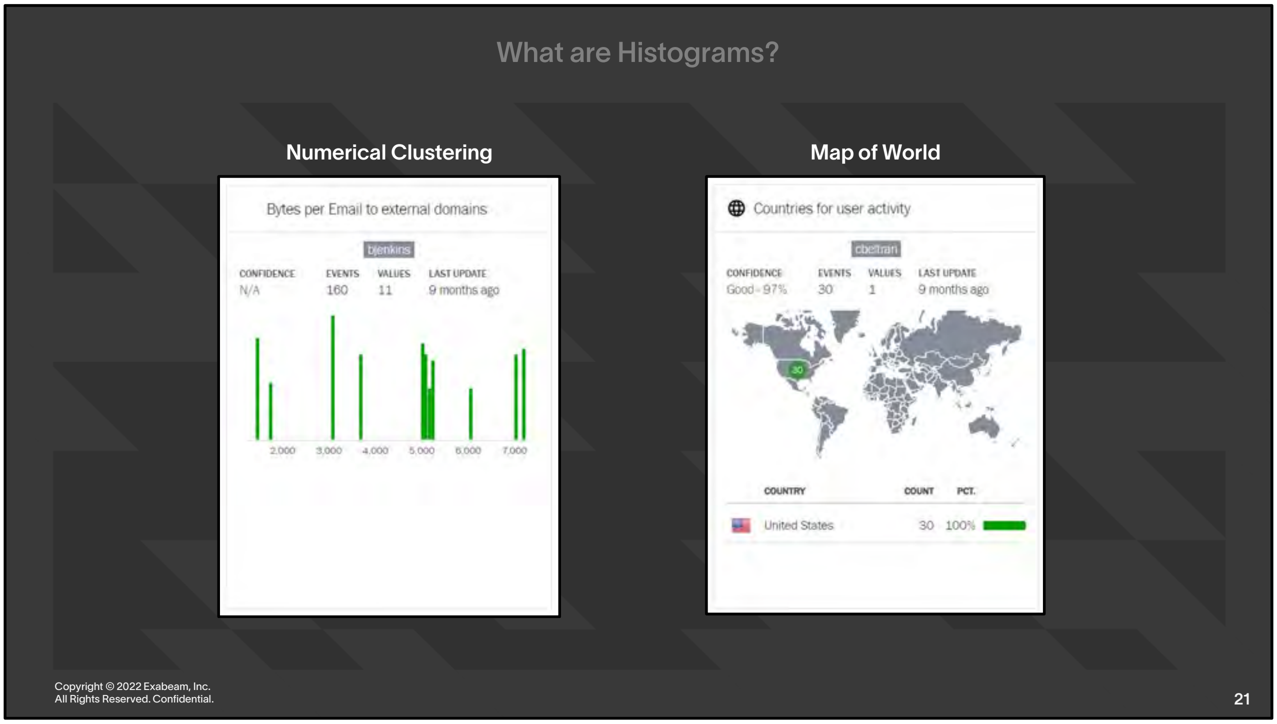
Each histogram has one of several possible templates or presentations. This section describes each histogram type. The presentation types are as follows:

- Table Histogram: presents a list of values and the number of times they were observed.
- Time of Week: shows blocks of time during the day on one axis, plotted against the days of the week.
- Cluster Histogram: uses a bar to represent ranges of values that constitute a cluster of events.
- Map (of the world): which, for example, can show countries from which a VPN session was started.

Histograms can be viewed from Data Insights.

Source

https://docs.exabeam.com



What are Histograms?

Numerical Clustering

Bytes per Email to external domains

bjenkins

CONFIDENCE N/A | EVENTS 160 | VALUES 11 | LAST UPDATE 9 months ago

Map of World

Countries for user activity

cbeltran

CONFIDENCE Good - 97% | EVENTS 30 | VALUES 1 | LAST UPDATE 9 months ago

COUNTRY	COUNT	PCT.
United States	30	100%

Student Notes

Types of Histograms Each histogram has one of several possible templates or presentations. This section describes each histogram type. The presentation types are as follows:

- Table Histogram: presents a list of values and the number of times they were observed.
- Time of Week: shows blocks of time during the day on one axis, plotted against the days of the week.
- Cluster Histogram: uses a bar to represent ranges of values that constitute a cluster of events.
- Map (of the world): which, for example, can show countries from which a VPN session was started.

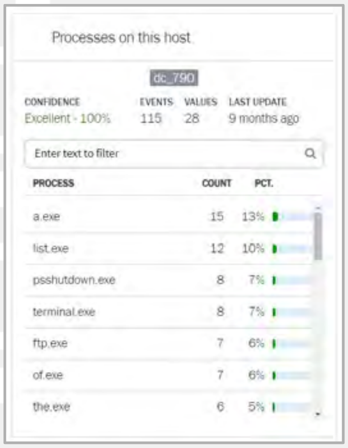
Histograms can be viewed from Data Insights.

Source

https://docs.exabeam.com

Demo

A Look at Models and Histograms

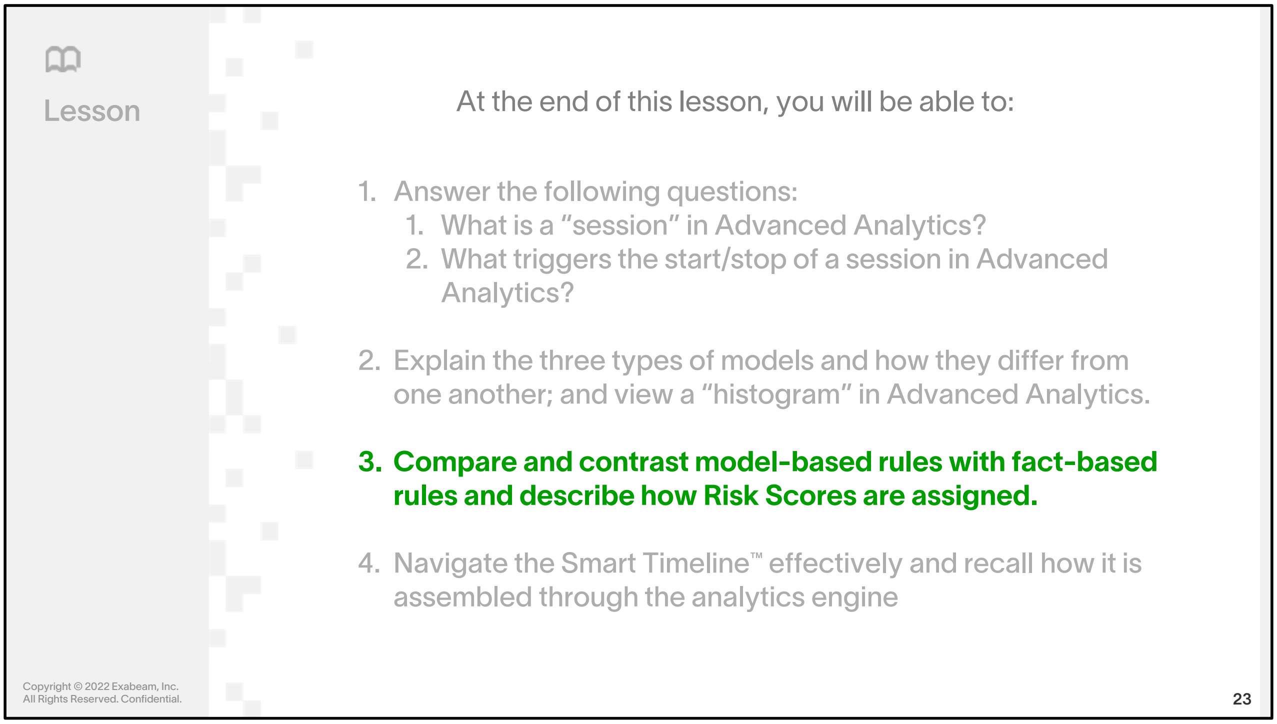


Processes on this host

dc_790

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
Excellent - 100%	115	28	9 months ago

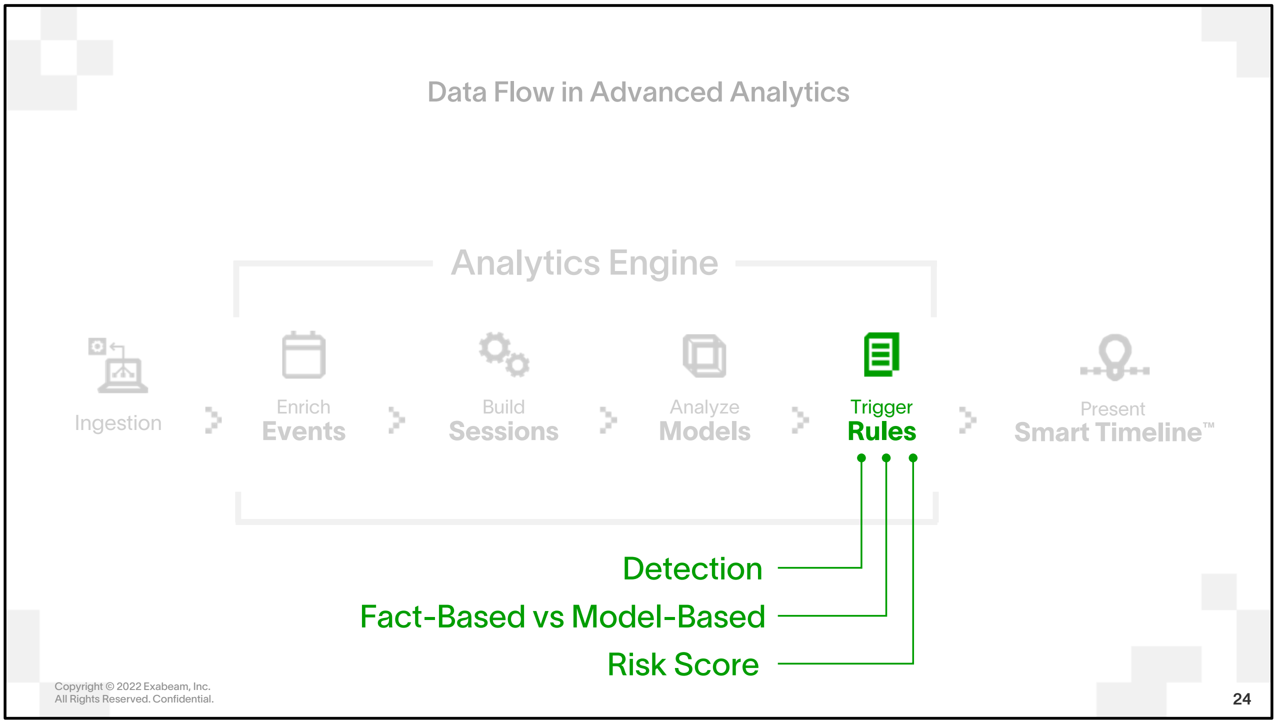
PROCESS	COUNT	PCT.
a.exe	15	13%
list.exe	12	10%
psshutdown.exe	8	7%
terminal.exe	8	7%
ftp.exe	7	6%
of.exe	7	6%
the.exe	6	5%



Lesson

At the end of this lesson, you will be able to:

1. Answer the following questions:
    1. What is a “session” in Advanced Analytics?
    2. What triggers the start/stop of a session in Advanced Analytics?
2. Explain the three types of models and how they differ from one another; and view a “histogram” in Advanced Analytics.
3. **Compare and contrast model-based rules with fact-based rules and describe how Risk Scores are assigned.**
4. Navigate the Smart Timeline™ effectively and recall how it is assembled through the analytics engine



Data Flow in Advanced Analytics

Analytics Engine

Ingestion > Enrich **Events** > Build **Sessions** > Analyze **Models** > Trigger **Rules** > Present **Smart Timeline™**

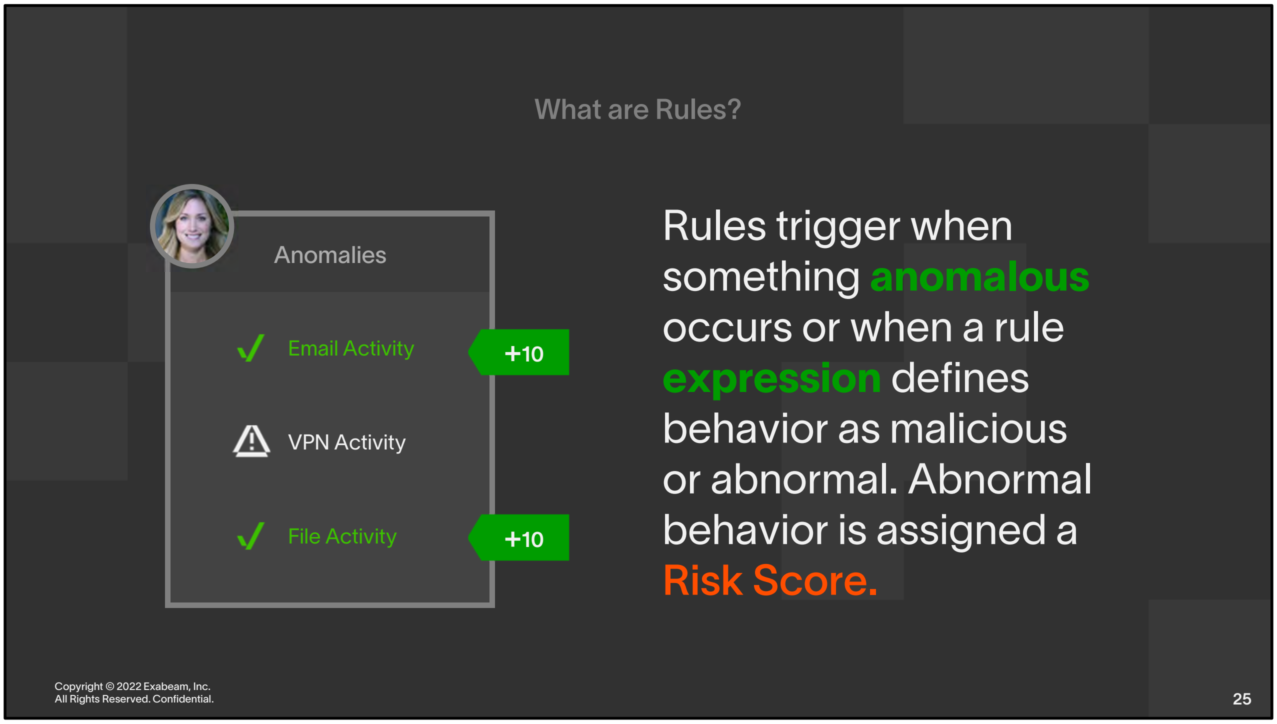
Detection

Fact-Based vs Model-Based

Risk Score

Student Notes

Most times Models will raise anomalies and then evaluate rules and assign risk. However, with ***fact-based*** rules this is not the case as will be detailed in the next few slides.



What are Rules?

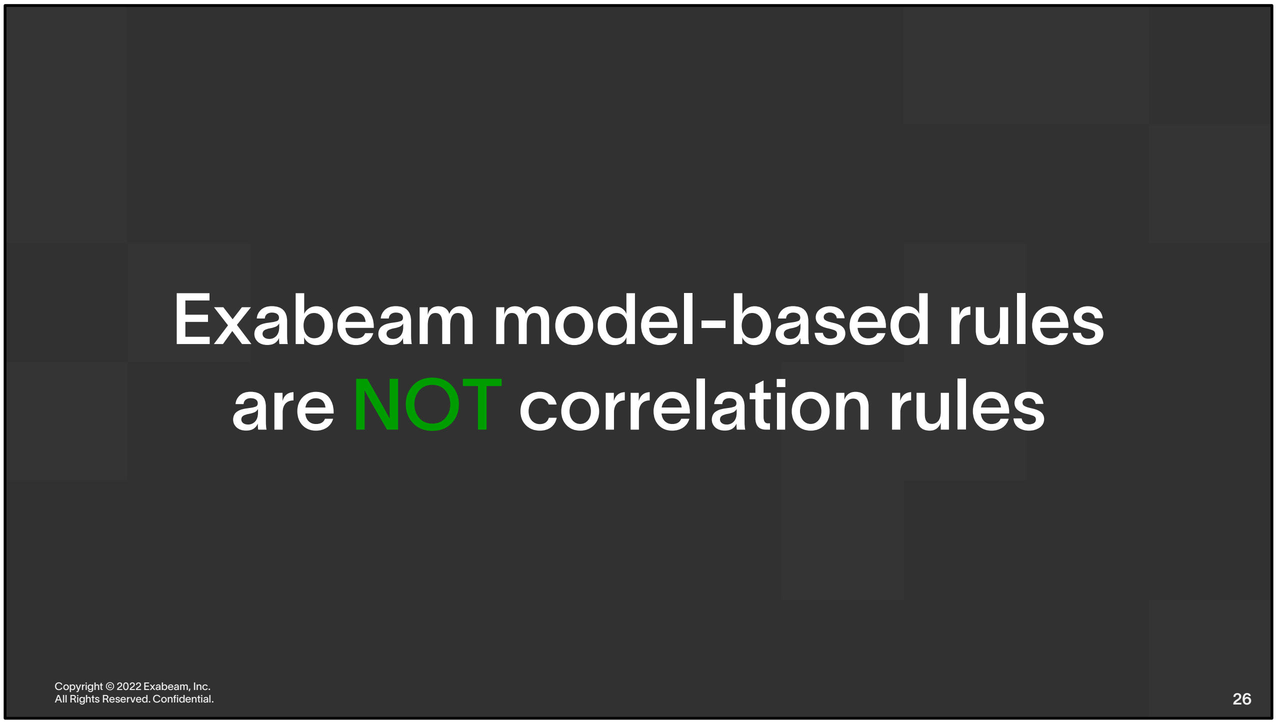
Anomalies

✓ Email Activity +10

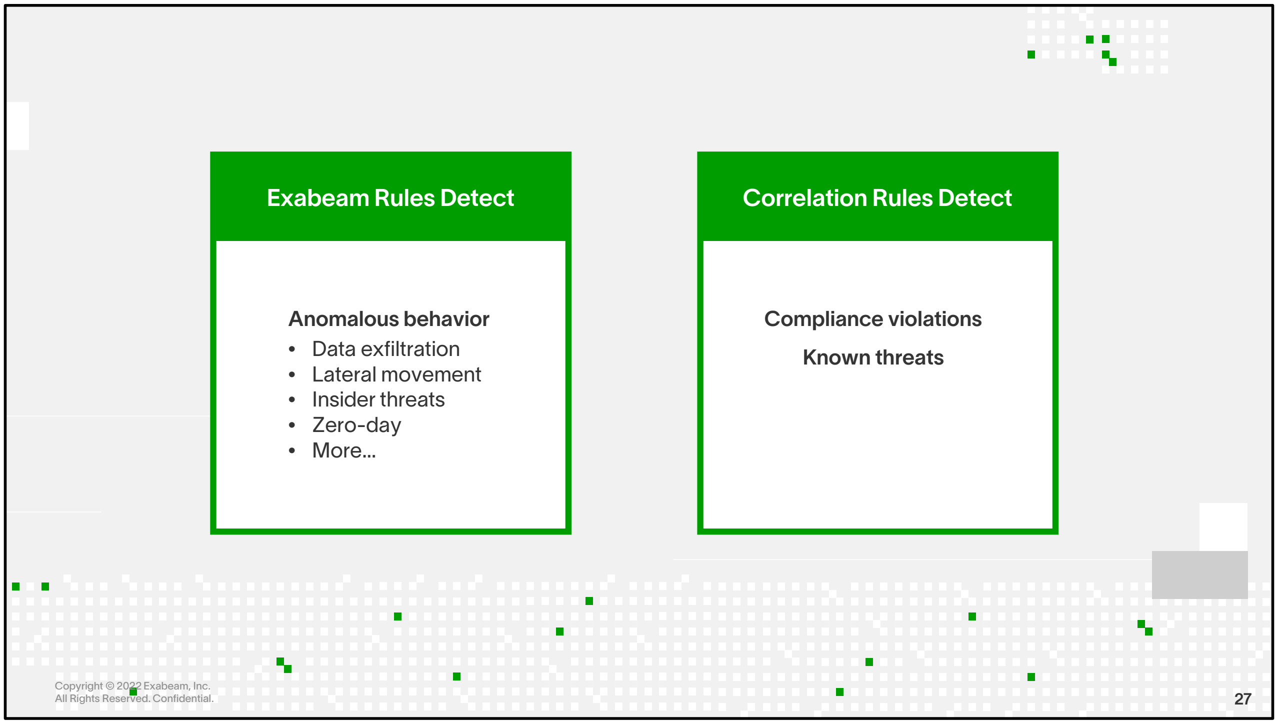
⚠ VPN Activity

✓ File Activity +10

Rules trigger when something **anomalous** occurs or when a rule **expression** defines behavior as malicious or abnormal. Abnormal behavior is assigned a Risk Score.



Exabeam model-based rules are NOT correlation rules



Exabeam Rules Detect

Anomalous behavior

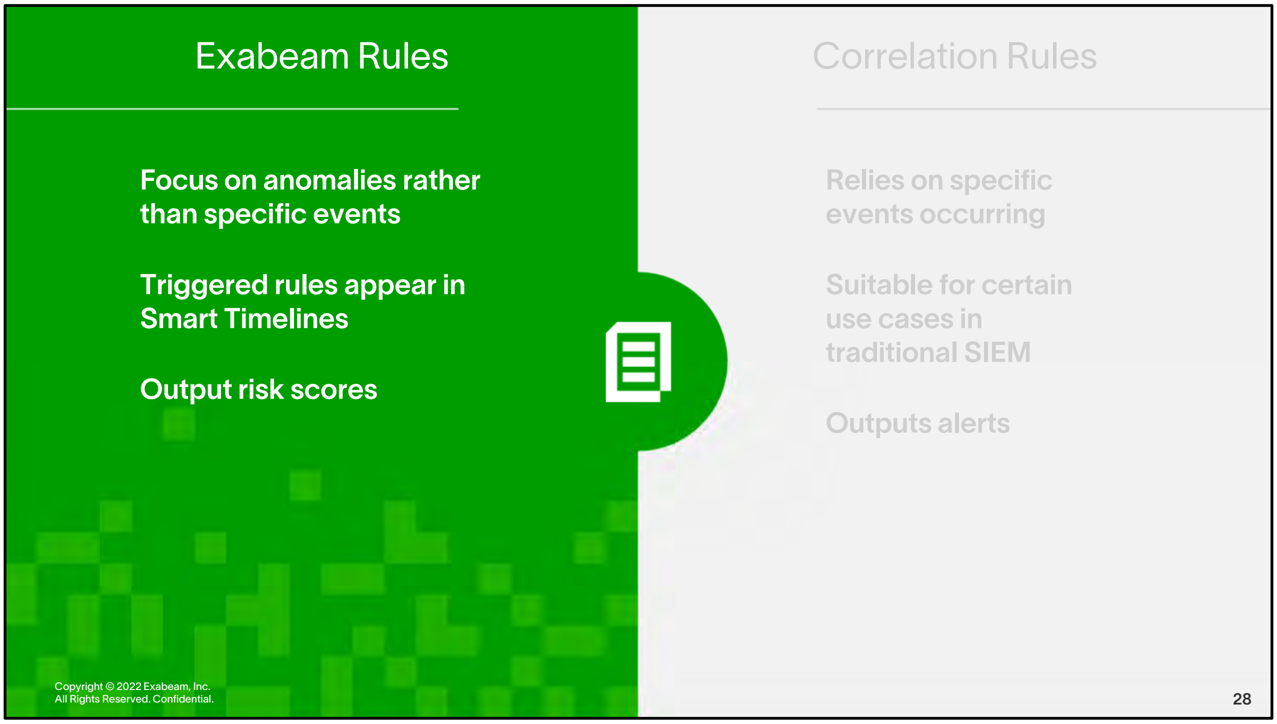
- Data exfiltration
- Lateral movement
- Insider threats
- Zero-day
- More…

Correlation Rules Detect

Compliance violations

Known threats

More Information
https://www.exabeam.com/wp-content/uploads/2018/10/Rules-vs.-Models-in-your-SIEM-WP.pdf



Exabeam Rules

Focus on anomalies rather than specific events

Triggered rules appear in Smart Timelines

Output risk scores

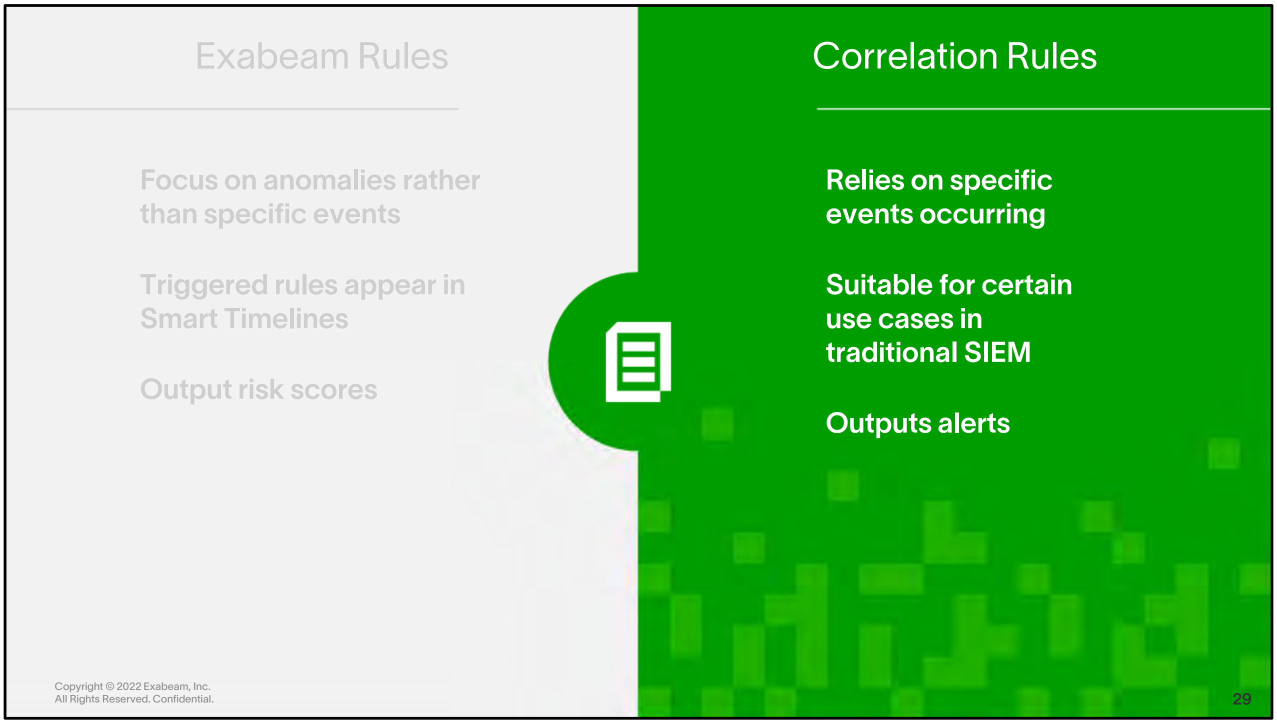
Correlation Rules

Relies on specific events occurring

Suitable for certain use cases in traditional SIEM

Outputs alerts

More Information
https://www.exabeam.com/wp-content/uploads/2018/10/Rules-vs.-Models-in-your-SIEM-WP.pdf



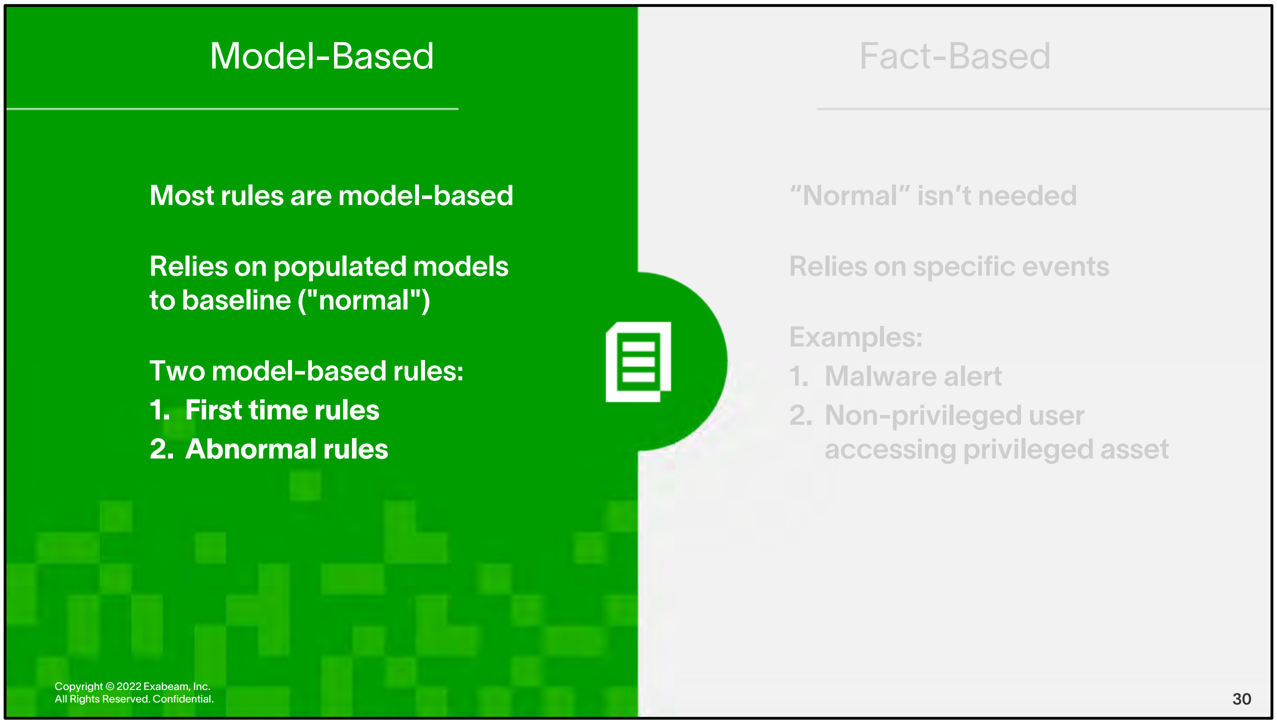
Exabeam Rules

- Focus on anomalies rather than specific events
- Triggered rules appear in Smart Timelines
- Output risk scores

Correlation Rules

- Relies on specific events occurring
- Suitable for certain use cases in traditional SIEM
- Outputs alerts

More Information
https://www.exabeam.com/wp-content/uploads/2018/10/Rules-vs.-Models-in-your-SIEM-WP.pdf



Model-Based

Most rules are model-based

Relies on populated models to baseline ("normal")

Two model-based rules:

1. First time rules
2. Abnormal rules

Fact-Based

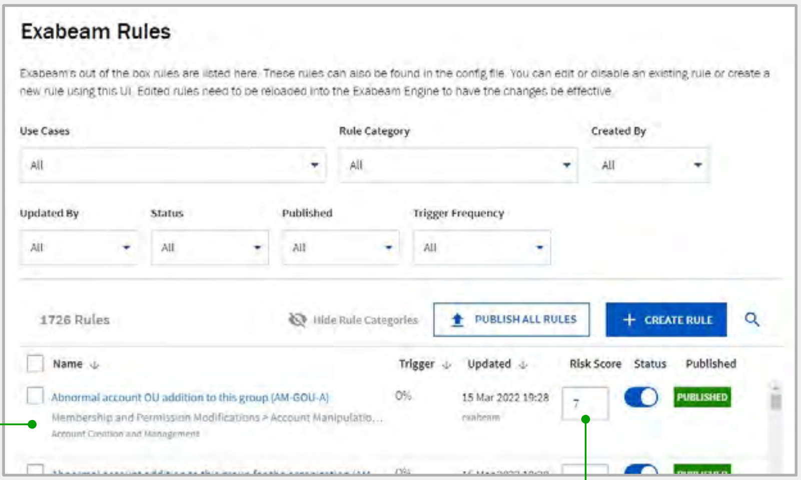
“Normal” isn’t needed

Relies on specific events

Examples:

1. Malware alert
2. Non-privileged user accessing privileged asset

Additional Details on Model-Based Rules



Exabeam Rules

Exabeam's out of the box rules are listed here. These rules can also be found in the config file. You can edit or disable an existing rule or create a new rule using this UI. Edited rules need to be reloaded into the Exabeam Engine to have the changes be effective.

Use Cases: All
Rule Category: All
Created By: All
Updated By: All
Status: All
Published: All
Trigger Frequency: All

1726 Rules

□	Name ↓	Trigger ↓	Updated ↓	Risk Score	Status	Published
□	Abnormal account OU addition to this group (AM-GOU-A) Membership and Permission Modifications > Account Manipulatio... Account Creation and Management	0%	15 Mar 2022 19:28 exabeam	7	●	PUBLISHED

Rules are scoped to:

- User
- Group
- Asset
- Organization

Can be tuned and customized by admins or engineers

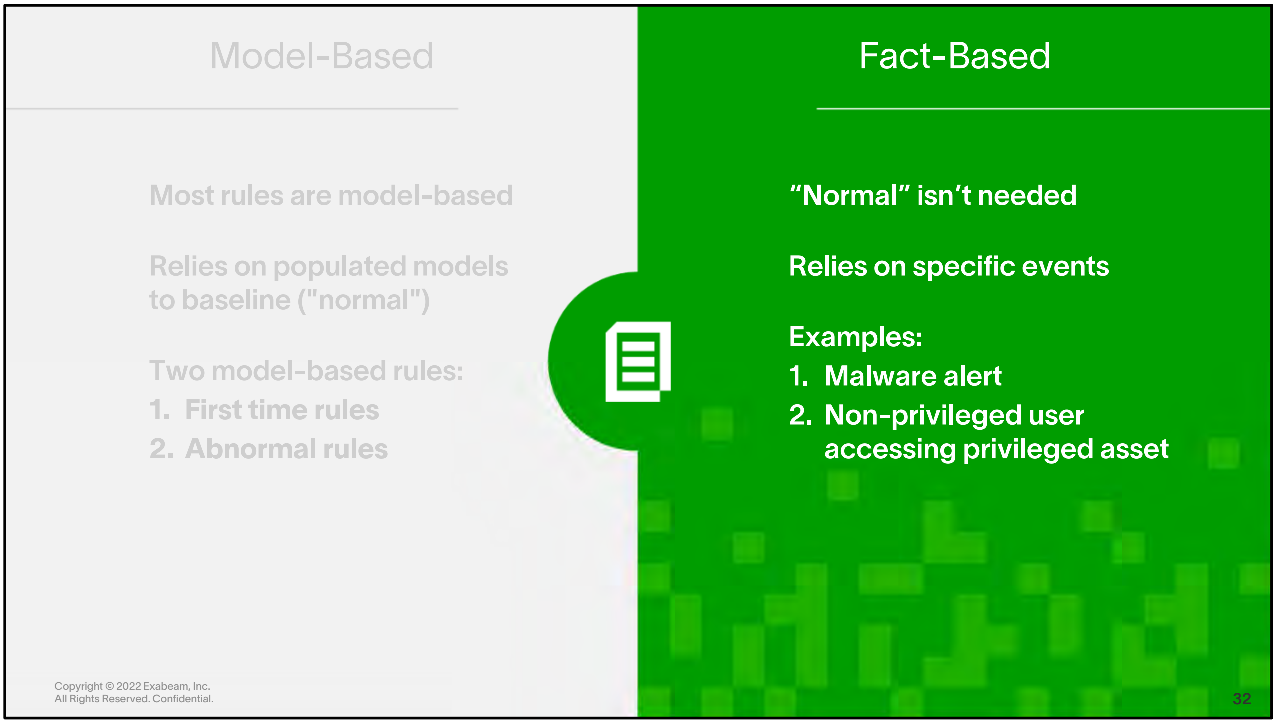
Student Notes

The Exabeam Rules interface in Advanced Analytics has been redesigned to simplify searching, creating, and modifying rules. Rules are organized by use case and use case scenario—for example, "Abnormal VPN Access" is a scenario in the "Compromised Credentials" use case. Modules 7, 8, and 9 covers use cases and use case categories in depth.

By default, only Tier 3 analysts and Administrators have permission to view and manage rules.

References

View rules in Advanced Analytics: https://docs.exabeam.com/en/cloud-delivered-advanced-analytics/all/administration-guide/127389-configure-advanced-analytics.html#UUID-def1b652-3338-e767-c2ce-0e1fee32e401
Filter rules: https://docs.exabeam.com/en/cloud-delivered-advanced-analytics/all/administration-guide/127389-configure-advanced-analytics.html#UUID-ebce552b-a965-df67-ab52-a8aaded8c96e
TDIR Use Case Packages: https://docs.exabeam.com/en/use-cases/all/get-started-with-tdir-use-case-packages/159617-threat-detection,-investigation,-and-response--tdir--use-case-packages.html#UUID-d069dccf-1743-50f9-8a05-58fa2b624a34
https://community.exabeam.com/s/article/Landing-Page-for-Tuning-Rules-in-Advanced-Analytics



Model-Based

Most rules are model-based

Relies on populated models to baseline ("normal")

Two model-based rules:

1. First time rules
2. Abnormal rules

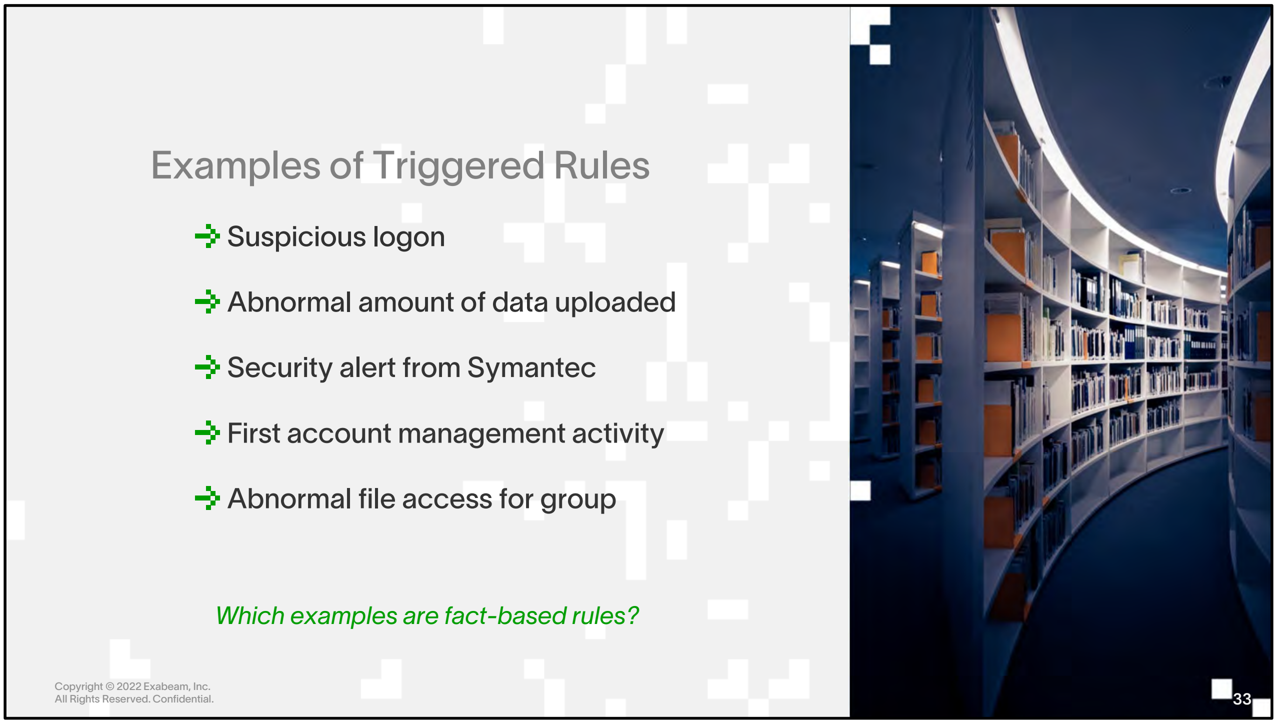
Fact-Based

"Normal" isn't needed

Relies on specific events

Examples:

1. Malware alert
2. Non-privileged user accessing privileged asset

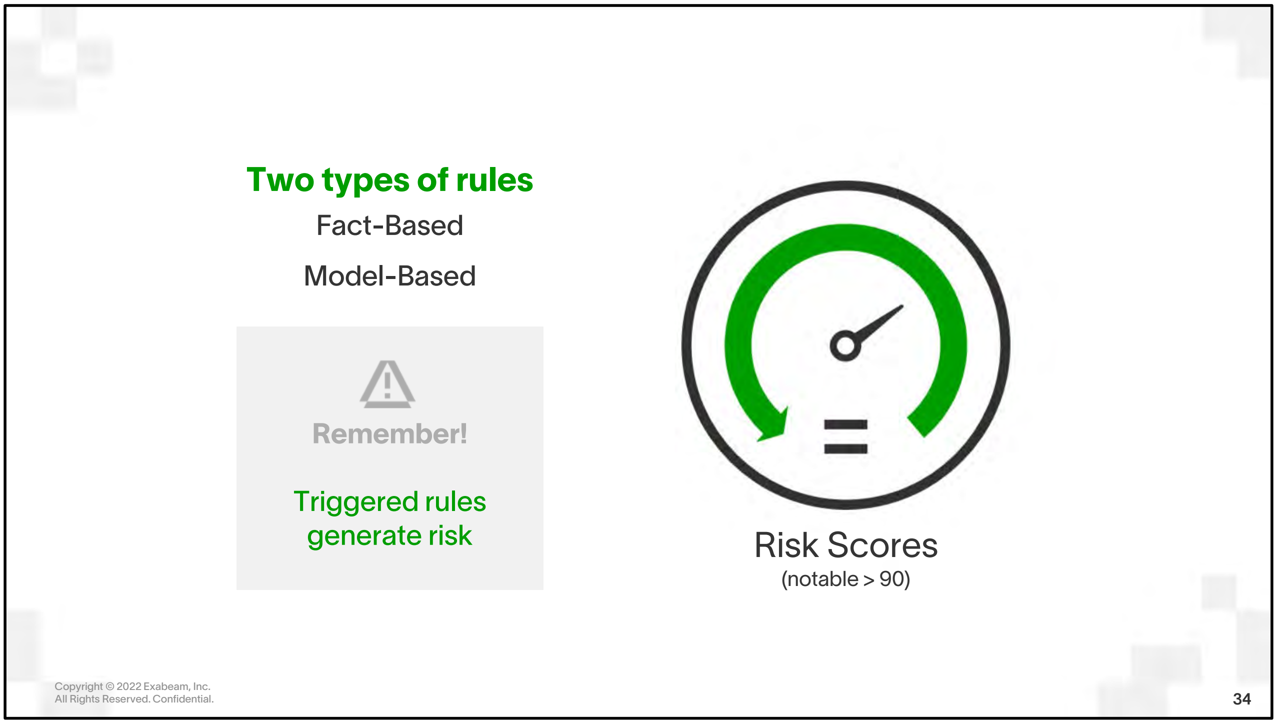


Examples of Triggered Rules

- Suspicious logon
- Abnormal amount of data uploaded
- Security alert from Symantec
- First account management activity
- Abnormal file access for group

Which examples are fact-based rules?

{Photo by Martin Adams on Unsplash}



Two types of rules

Fact-Based

Model-Based

⚠ Remember!

Triggered rules generate risk

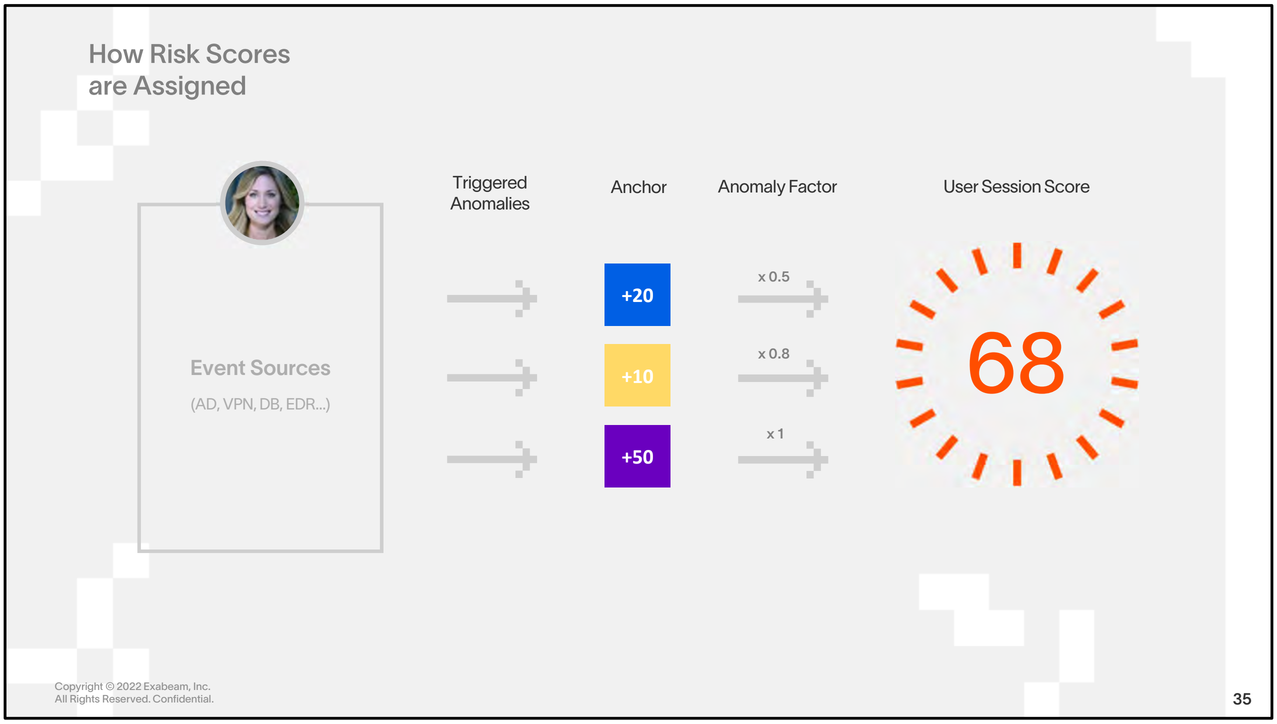
Risk Scores

(notable > 90)

Student Notes

- A majority of AA's rules will be model-based. In fact, when we review rule conditions, there will be two tables for rules and models. These are required to define "normal".
- There are 4 categories for rules:
  - All Rules,
  - Exabeam (out of box) Rules,
  - Custom Rules,
  - Disabled Rules

  Model-based rules are sometimes called "exabeam rules"



How Risk Scores are Assigned

Event Sources

(AD, VPN, DB, EDR...)

Triggered Anomalies

Anchor

Anomaly Factor

User Session Score

+20

+10

+50

x 0.5

x 0.8

x 1

68

Copyright © 2022 Exabeam, Inc.
All Rights Reserved. Confidential.

35

Student Notes

Risk Scores are adjusted based on machine-learning determined factors. These adjustments are called “Anomaly Factors” and can be imagined as the chain attached to an anchor; wherever the Anchor Score goes, the Anomaly Factor follows. It is determined and set automatically by Exabeam.

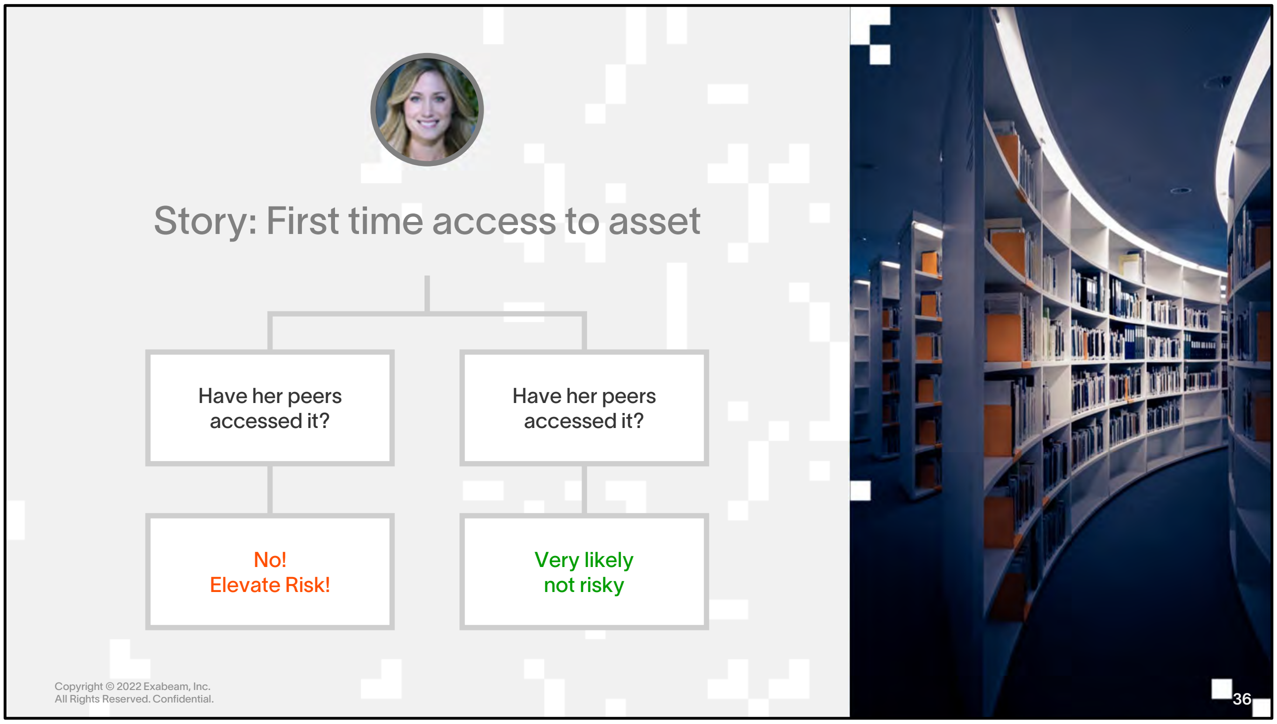
Anomaly Factors are mostly controlled by Exabeam’s Machine Learning. It is a way to reduce the number of rules that are “noisier” than others – and retain the integrity of truly anomalous behavior. For example, if you have a rule occurring at a very high rate among many users, that may indicate that less attention should be given to the rule.

Source

https://community.exabeam.com/s/article/Understanding-AA-Risk-Score

More Information

https://www.exabeam.com/ueba/user-entity-behavior-analytics-scoring-system-explained/



Story: First time access to asset

Have her peers accessed it?

No!
Elevate Risk!

Have her peers accessed it?

Very likely
not risky

Copyright © 2022 Exabeam, Inc.
All Rights Reserved. Confidential.

36

More Information

https://www.exabeam.com/information-security/first-time-access-asset-risky-not-machine-learning-question/

https://www.exabeam.com/ueba/who-do-i-belong-to-dynamic-peer-analysis-for-ueba-explained/

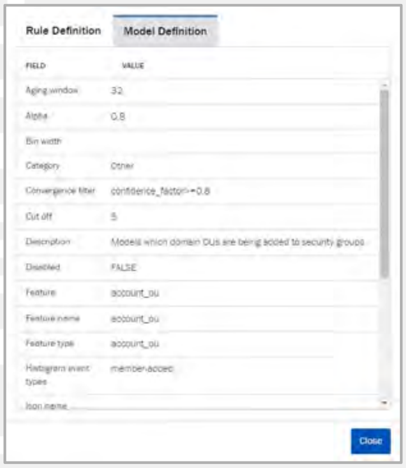
References

https://www.exabeam.com/ueba/who-do-i-belong-to-dynamic-peer-analysis-for-ueba-explained/
https://docs.exabeam.com/en/advanced-analytics/cloud-delivered/advanced-analytics-user-guide/153664-get-to-know-a-user-profile.html
https://docs.exabeam.com/en/advanced-analytics/i56/advanced-analytics-administration-guide/125371-configure-advanced-analytics.html#UUID-471e24ff-903c-5af6-6901-21f028485ad9
https://community.exabeam.com/s/article/Dynamic-Multi-Peer-Groups

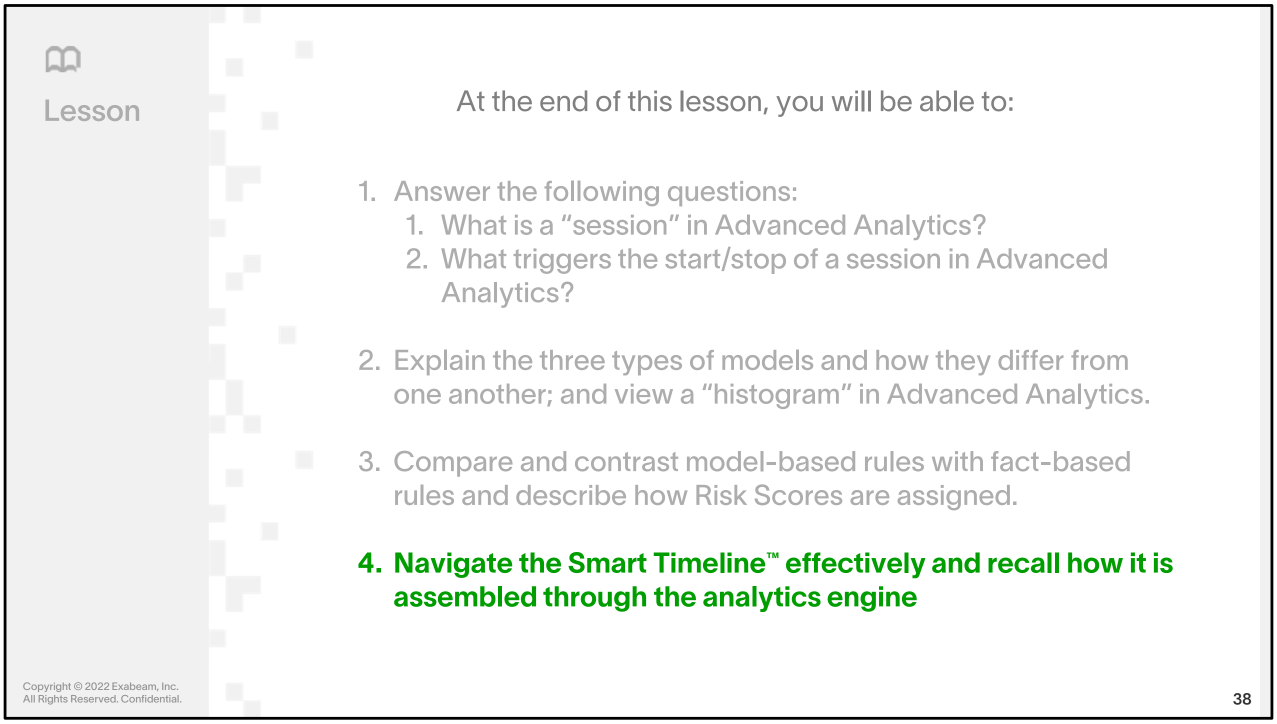
{Photo by Martin Adams on Unsplash}

Demo

A Look at Rules and Rule Types



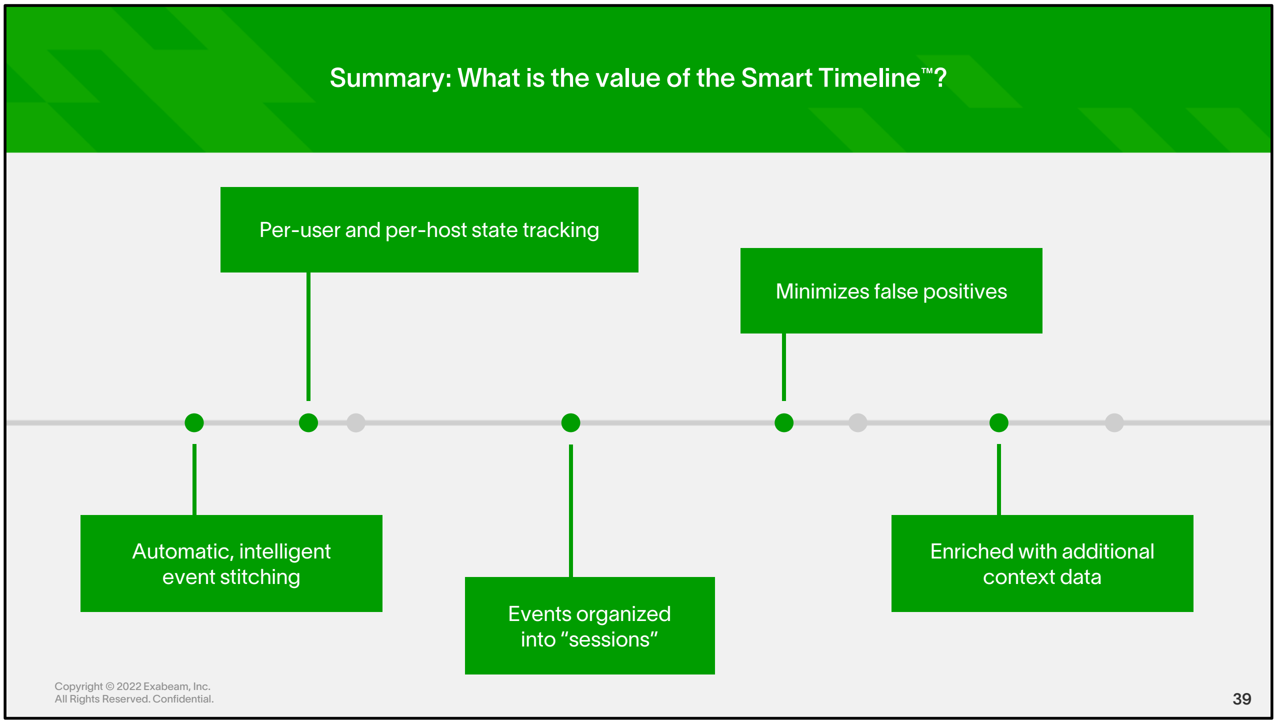
FIELD	VALUE
Aging window	32
Alpha	0.8
Bin width	
Category	Other
Convergence filter	confidence_factor>=0.8
Cut off	5
Description	Models which domain OUs are being added to security groups
Disabled	FALSE
Feature	account_ou
Feature name	account_ou
Feature type	account_ou
Histogram event types	member-added
Icon name	



Lesson

At the end of this lesson, you will be able to:

1. Answer the following questions:
   1. What is a "session" in Advanced Analytics?
   2. What triggers the start/stop of a session in Advanced Analytics?
2. Explain the three types of models and how they differ from one another; and view a "histogram" in Advanced Analytics.
3. Compare and contrast model-based rules with fact-based rules and describe how Risk Scores are assigned.
4. **Navigate the Smart Timeline™ effectively and recall how it is assembled through the analytics engine**



Summary: What is the value of the Smart Timeline™?

Per-user and per-host state tracking

Minimizes false positives

Automatic, intelligent event stitching

Events organized into "sessions"

Enriched with additional context data

Student Notes

Here is a useful quote that describes the need for Stateful User Tracking:

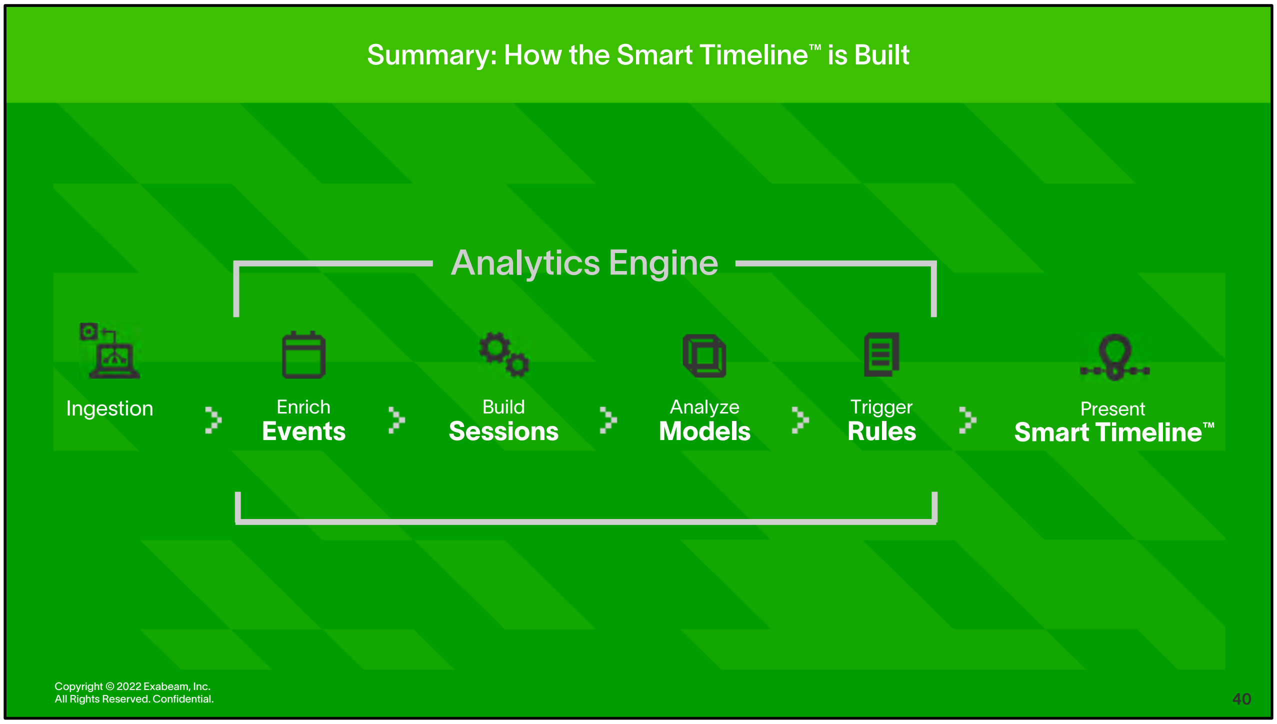
"**Security log data is stateless**…a platform must be able to piece events together to track the state of data, and ultimately, a user's behavior." -Derek Lin, Exabeam Chief Data Scientist

Source

https://www.exabeam.com/ueba/data-science-and-stateful-user-tracking-the-two-key-uba-enablers/

More information

https://www.exabeam.com/ueba/data-science-and-stateful-user-tracking-the-two-key-uba-enablers/



Summary: How the Smart Timeline™ is Built

Analytics Engine

Ingestion

Enrich **Events**

Build **Sessions**

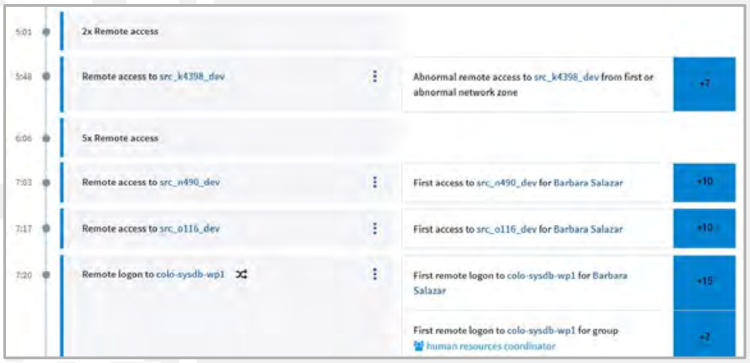
Analyze **Models**

Trigger **Rules**

Present **Smart Timeline™**

Demo

A Look at the Smart Timeline



5:01	2x Remote access		
5:48	Remote access to src_k4398_dev	Abnormal remote access to src_k4398_dev from first or abnormal network zone	+7
6:06	5x Remote access		
7:03	Remote access to src_n490_dev	First access to src_n490_dev for Barbara Salazar	+10
7:17	Remote access to src_o116_dev	First access to src_o116_dev for Barbara Salazar	+10
7:20	Remote logon to colo-sysdb-wp1	First remote logon to colo-sysdb-wp1 for Barbara Salazar	+15
		First remote logon to colo-sysdb-wp1 for group human resources coordinator	+7

Risk Scores in the Smart Timeline™

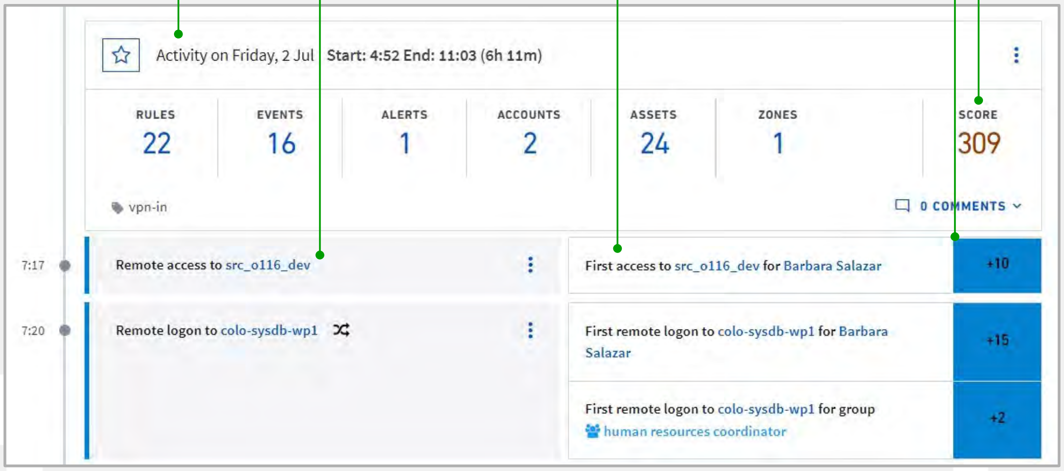
Session Risk Score

Modeled Events

Session Info

Triggered Rules

Assigned Risk



Activity on Friday, 2 Jul | Start: 4:52 End: 11:03 (6h 11m)

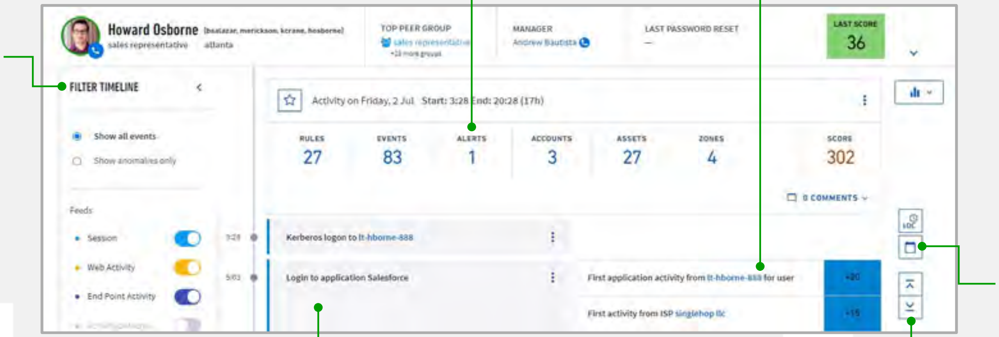
RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES	SCORE
22	16	1	2	24	1	309

vpn-in

0 COMMENTS

Time	Event	Triggered rule	Risk
7:17	Remote access to src_o116_dev	First access to src_o116_dev for Barbara Salazar	+10
7:20	Remote logon to colo-sysdb-wp1	First remote logon to colo-sysdb-wp1 for Barbara Salazar	+15
		First remote logon to colo-sysdb-wp1 for group human resources coordinator	+2

Navigating User and Asset Timelines



Howard Osborne (bsalazar, merickson, kcrane, hosborne)
sales representative atlanta

TOP PEER GROUP: sales representative +11 more groups

MANAGER: Andrew Bautista

LAST PASSWORD RESET: —

LAST SCORE: 36

FILTER TIMELINE

● Show all events
○ Show anomalies only

Feeds
- Session
- Web Activity
- End Point Activity

Activity on Friday, 2 Jul Start: 3:28 End: 20:28 (17h)

RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES	SCORE
27	83	1	3	27	4	302

0 COMMENTS

3:28 Kerberos logon to lt-hborne-888

5:03 Login to application Salesforce

First application activity from lt-hborne-888 for user +20

First activity from ISP singlehop llc +15

Session Header with Findable Statistics

Rules Have Details

Filter Timeline

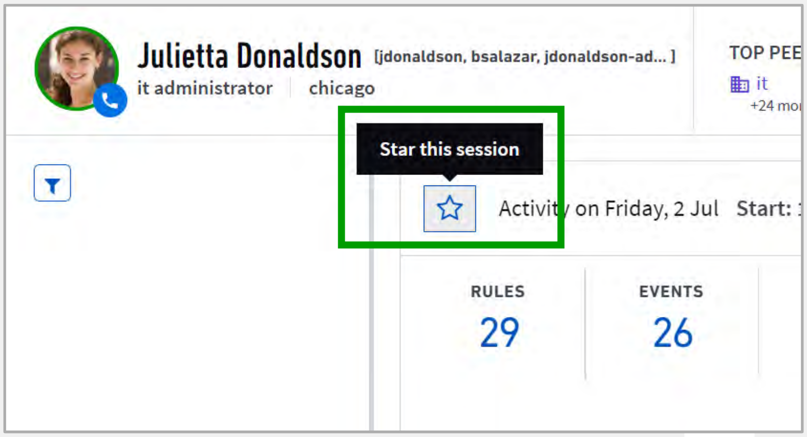
Date Picker

Events Have Details

Session Back/Forward

Student Notes
Filters let you choose to show or hide events of different activity types
The Session Header stays pinned to the top as you scroll down for both Users and Assets
Clicking a statistic in the Session Header in the timeline shows you the details of that statistic and triggers a find within the session
Clicking a Modeled Event on the left will display the details of that event
Clicking a Triggered Rule on the right will display the details, definition, and histograms associated with that rule
There is a Date Picker and a Back Session / Forward Session tool in the bottom right

Add a Comment, then Bookmark Sessions with a Star

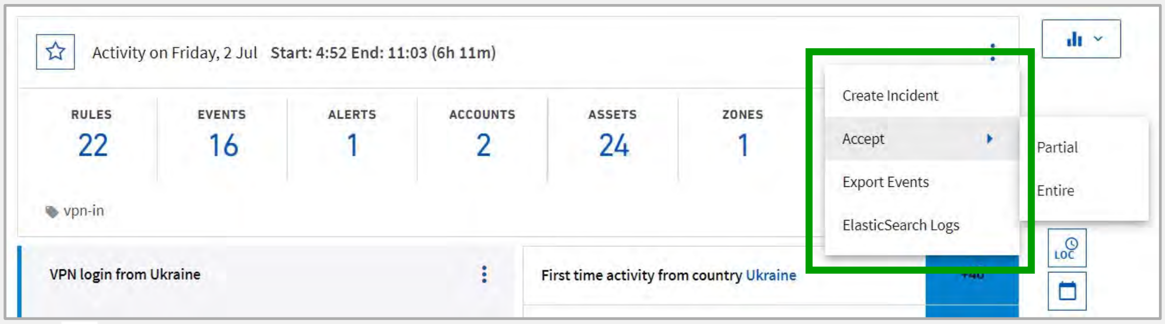

Julietta Donaldson [jdonaldson, bsalazar, jdonaldson-ad...]
it administrator
chicago
TOP PEE
it
+24 mo
Star this session
Activity on Friday, 2 Jul
Start:
RULES
29
EVENTS
26

Student Notes

Analysts can star a session as part of their workflow. Starring a session is like bookmarking because it becomes available from the main dashboard.

It is useful when pivoting to threat hunter for further investigation to root yourself in the original investigation and also to keep track of sessions that are related to the inv

Accepting Sessions (Can’t Be Undone!)



Activity on Friday, 2 Jul Start: 4:52 End: 11:03 (6h 11m)

RULES	EVENTS	ALERTS	ACCOUNTS	ASSETS	ZONES
22	16	1	2	24	1

vpn-in

VPN login from Ukraine

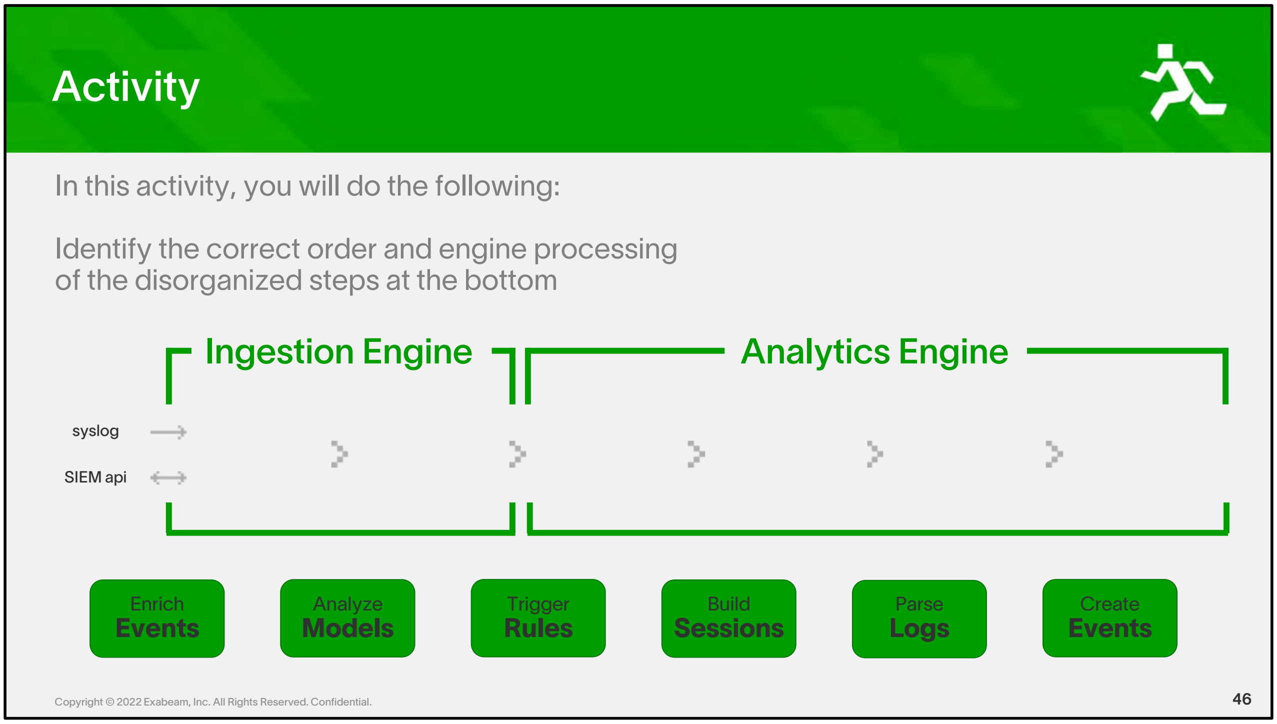
First time activity from country Ukraine

Student Notes

Accepting a session adds the behavior manual to the model to define it as “acceptable”

This is an action that requires special privileges to perform and may require custom roles

Accepting a session can NOT be revoked afterward



Activity

In this activity, you will do the following:

Identify the correct order and engine processing of the disorganized steps at the bottom

Ingestion Engine

Analytics Engine

syslog

SIEM api

Enrich **Events**

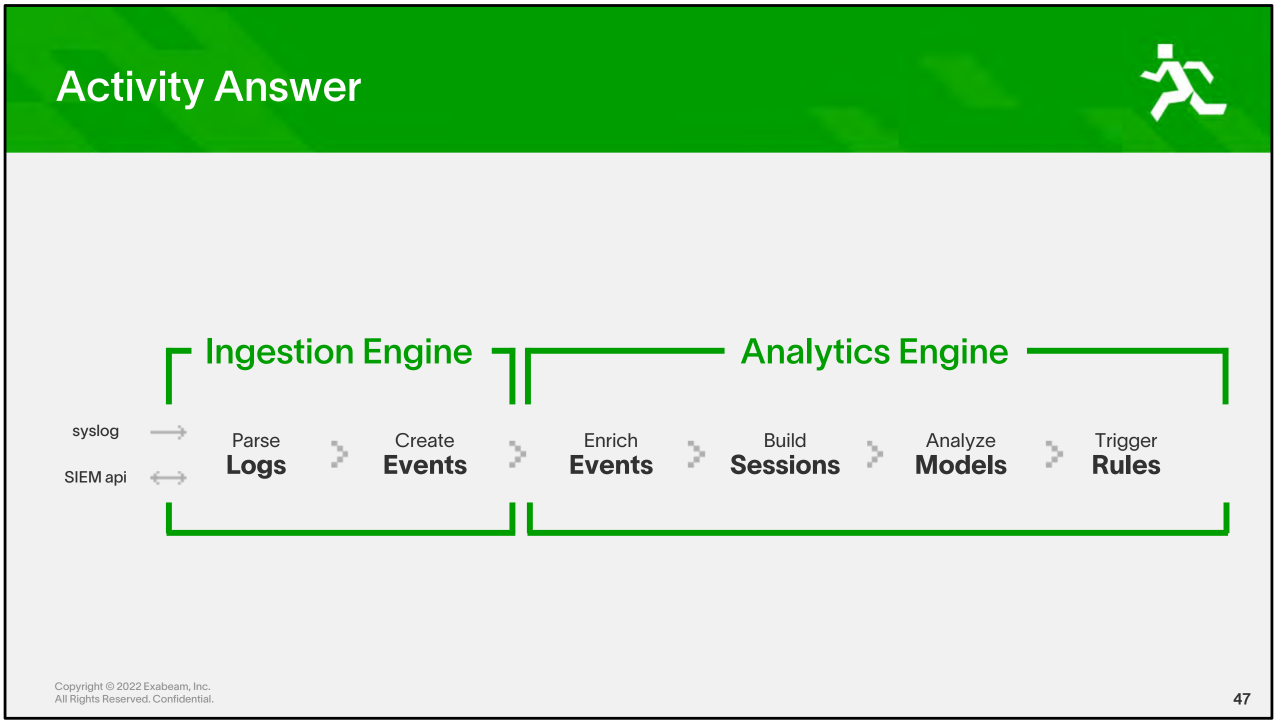
Analyze **Models**

Trigger **Rules**

Build **Sessions**

Parse **Logs**

Create **Events**



Activity Answer

Ingestion Engine

Analytics Engine

syslog

SIEM api

Parse **Logs**

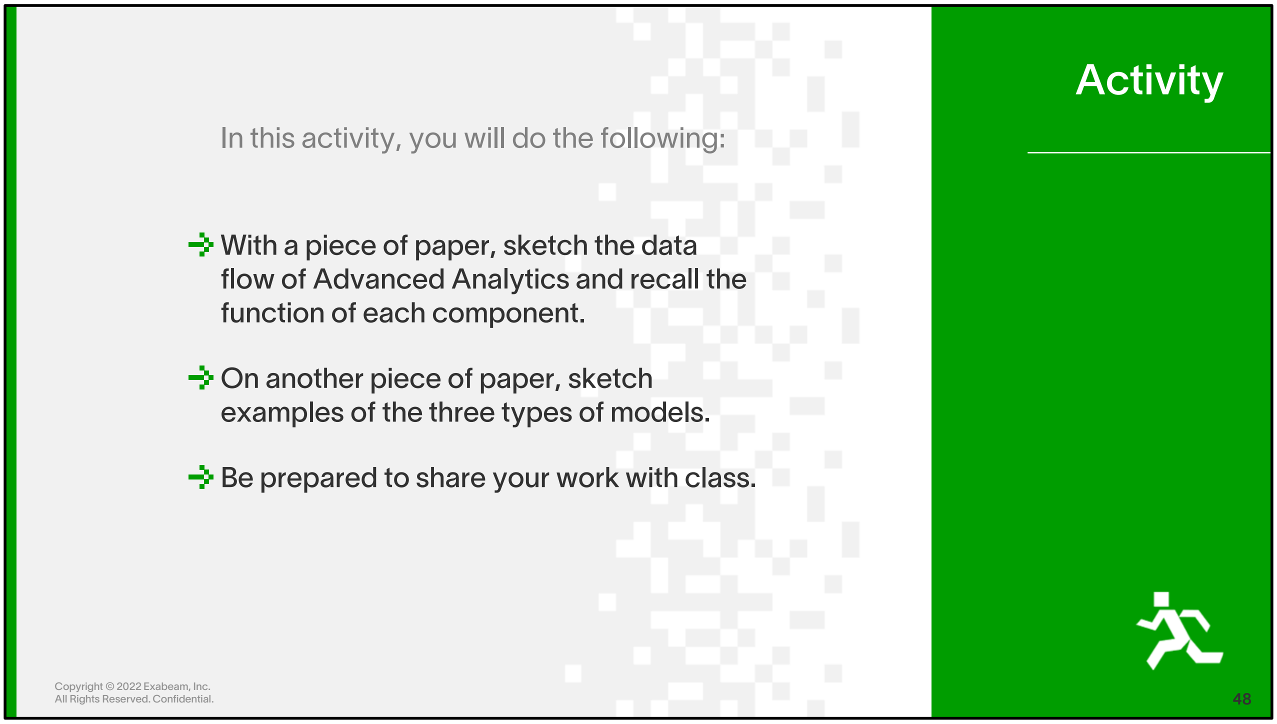
Create **Events**

Enrich **Events**

Build **Sessions**

Analyze **Models**

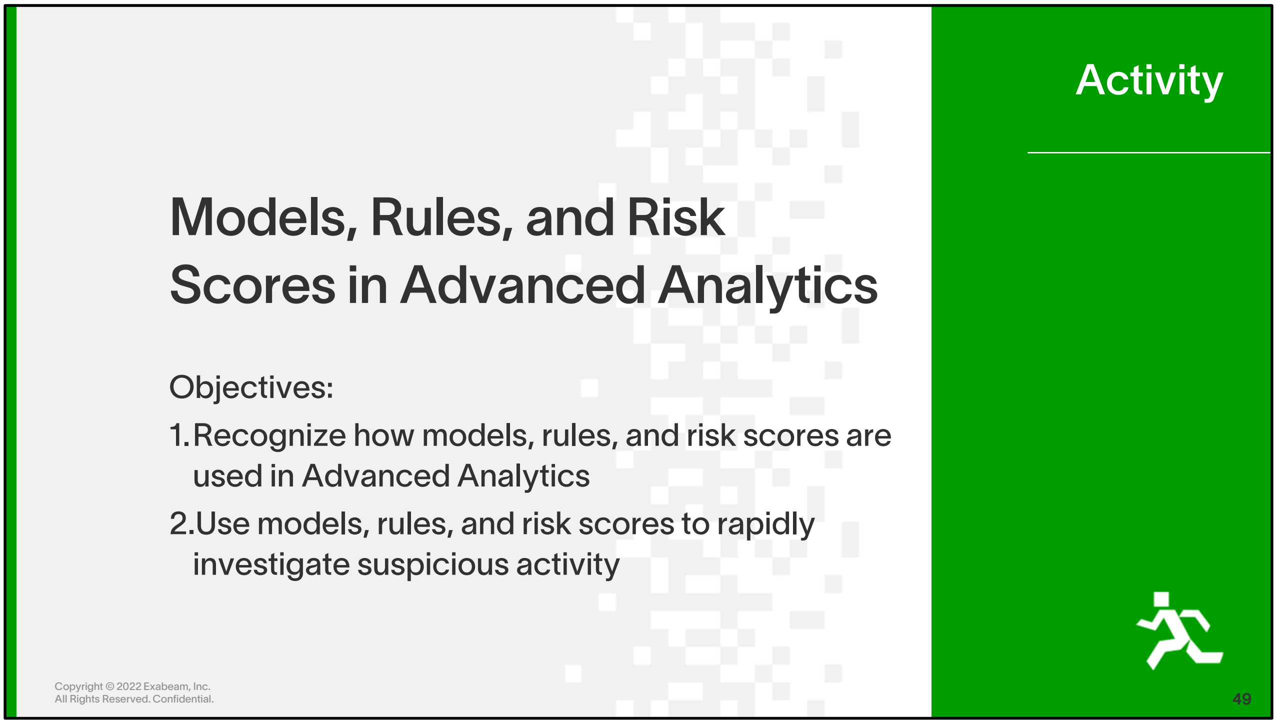
Trigger **Rules**



Activity

In this activity, you will do the following:

- With a piece of paper, sketch the data flow of Advanced Analytics and recall the function of each component.
- On another piece of paper, sketch examples of the three types of models.
- Be prepared to share your work with class.

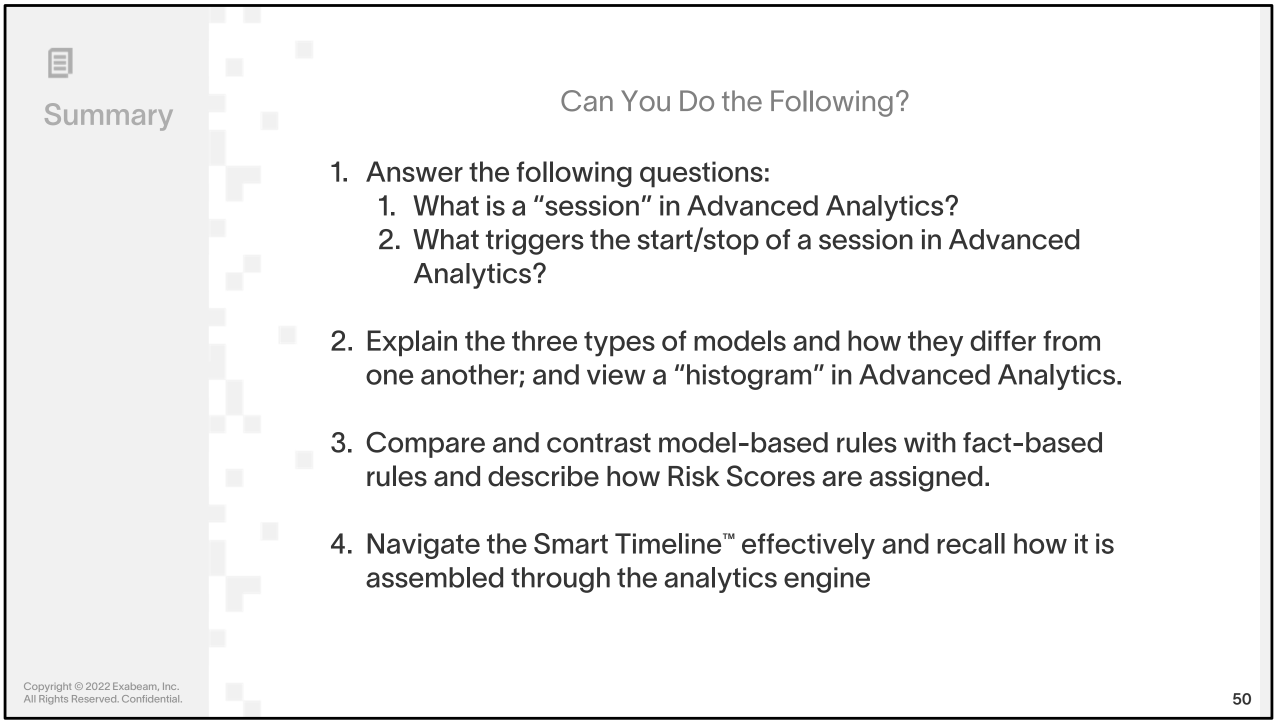


Activity

Models, Rules, and Risk Scores in Advanced Analytics

Objectives:

1. Recognize how models, rules, and risk scores are used in Advanced Analytics
2. Use models, rules, and risk scores to rapidly investigate suspicious activity



Summary

Can You Do the Following?

1. Answer the following questions:
   1. What is a “session” in Advanced Analytics?
   2. What triggers the start/stop of a session in Advanced Analytics?

2. Explain the three types of models and how they differ from one another; and view a “histogram” in Advanced Analytics.

3. Compare and contrast model-based rules with fact-based rules and describe how Risk Scores are assigned.

4. Navigate the Smart Timeline™ effectively and recall how it is assembled through the analytics engine