
exabeam
UNDER THE HOOD OF NEXT GEN SIEM
Presented by: Tim Gibbs, Regional Sales Director
Randeep Gill, Security Engineer

Exabeam Gartner Magic Quadrant and Voice of the Customer Placements

2018 Gartner SIEM Magic Quadrant

Gartner peerinsights customers' choice 2018™

Exabeam won the *2018 Gartner Peer Insights Customer Choice award for Best SIEM*

Exabeam won the following recognition in the *2018 Gartner Voice of the Customer Report for SIEM*:

- Best overall rating
- Highest willingness to recommend (by customers)
- Best experience in evaluation and contacting
- Best integration and deployment
- Best services and support

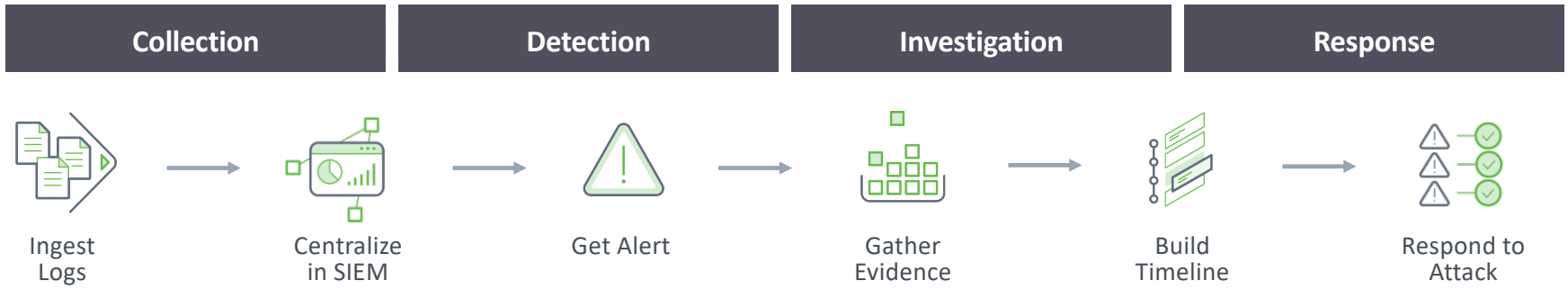
exabeam

Historical considerations for SIEM

- **Why do I need one?**
  - Compliance
  - Visibility
  - Improve threat detection
- **£££**
  - Volume-based pricing. How do I budget for this?
  - How will this be impacted in 1/3/5 years?
- **Log Sources**
  - What do I need to log? Security controls, routers, cloud apps?
  - How much data do I need to retain?
- **Rules**
  - What rules should I apply?
  - Who will create/tune these?
- **Who is going to run it?**
  - Who will go through all my events?
  - Should I build a SOC?
  - How many people do I need to manage it?

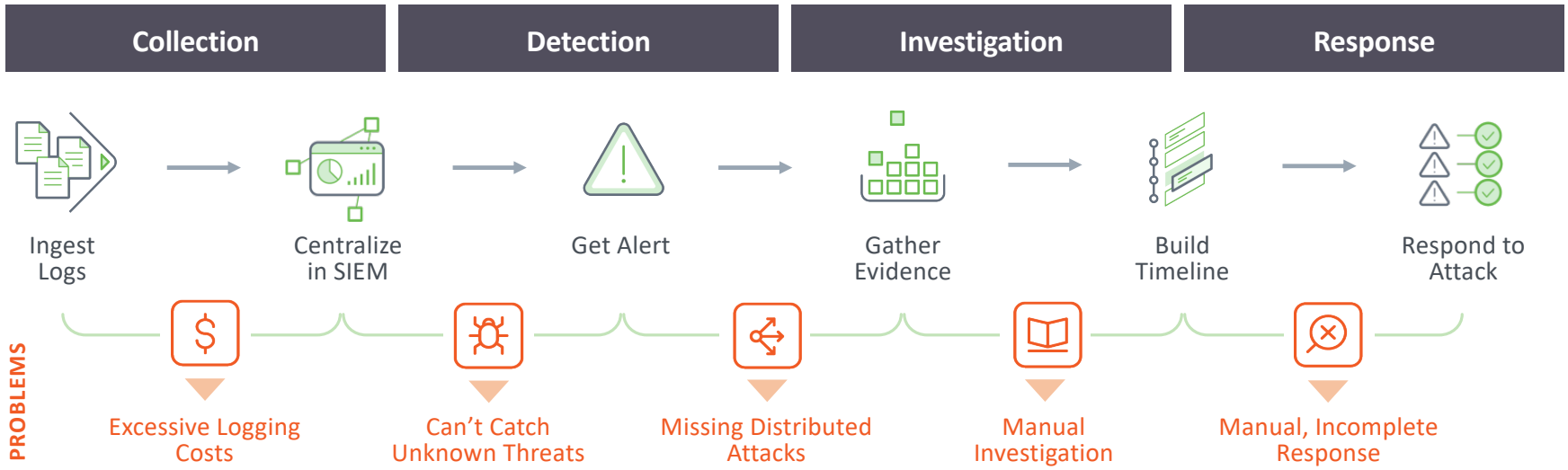
exabeam

Security Management Process with Legacy SIEM



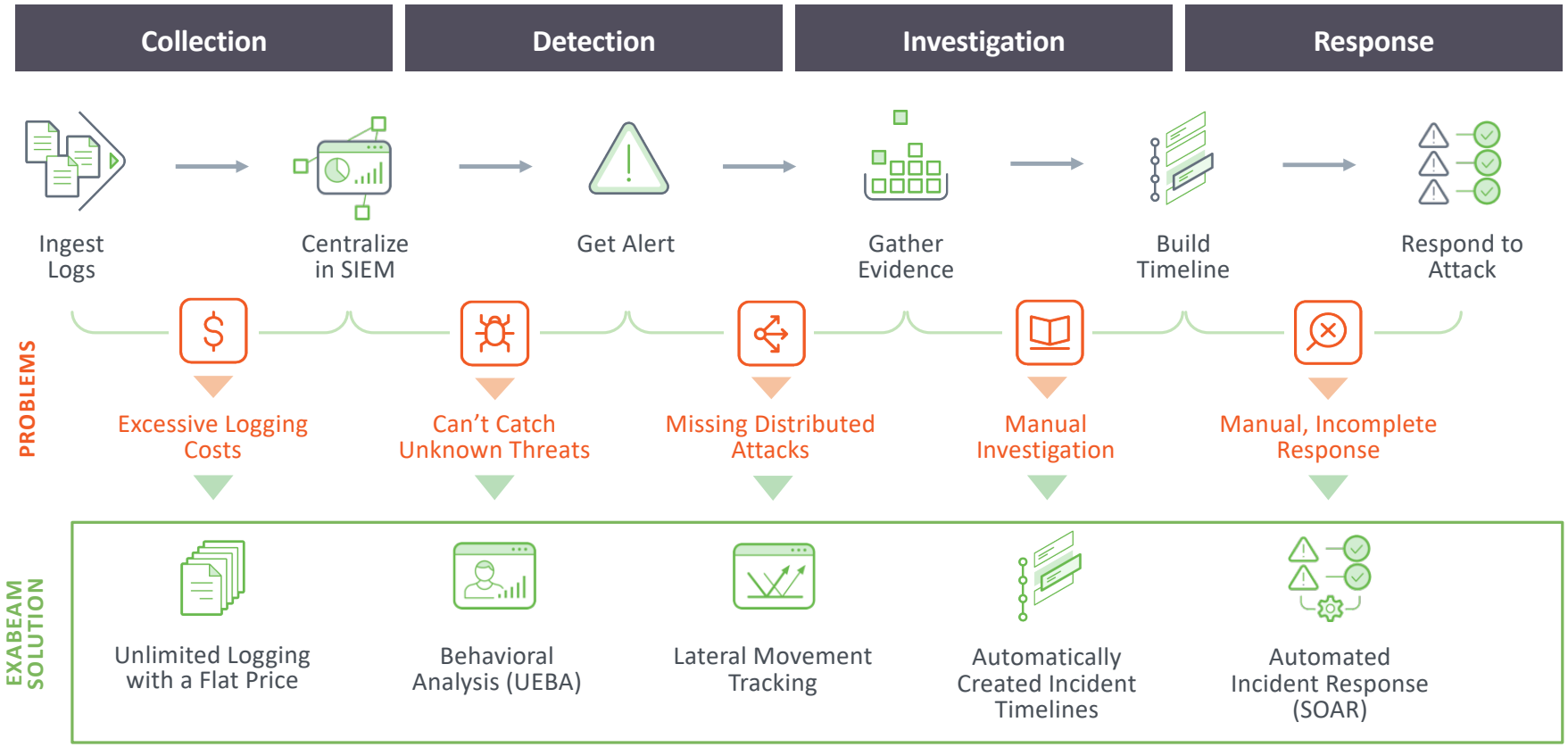
exabeam

Legacy SIEMs Cause Challenges at Each Step



exabeam

Solving Security Management Challenges



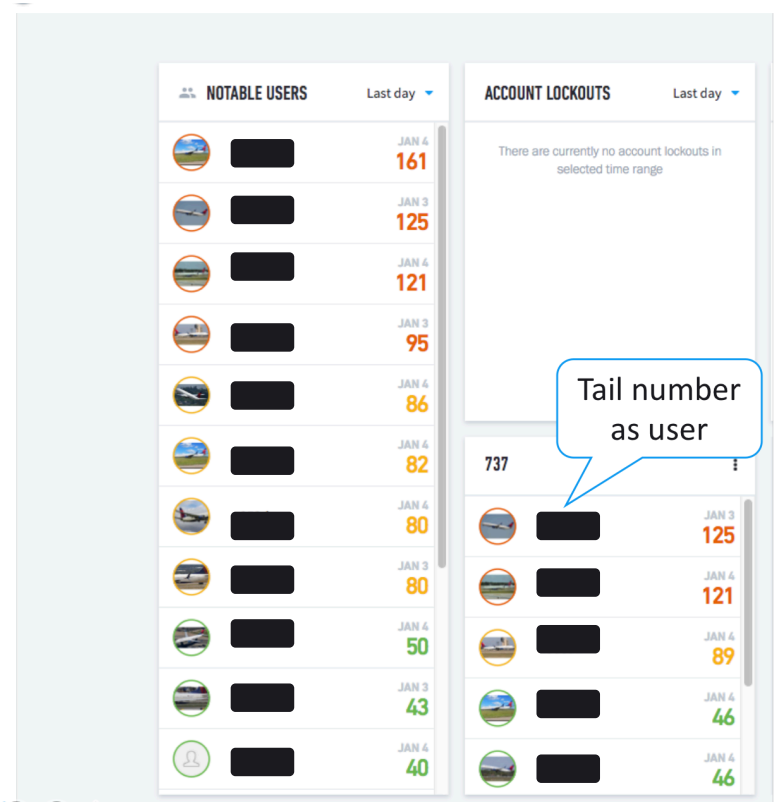
exabeam

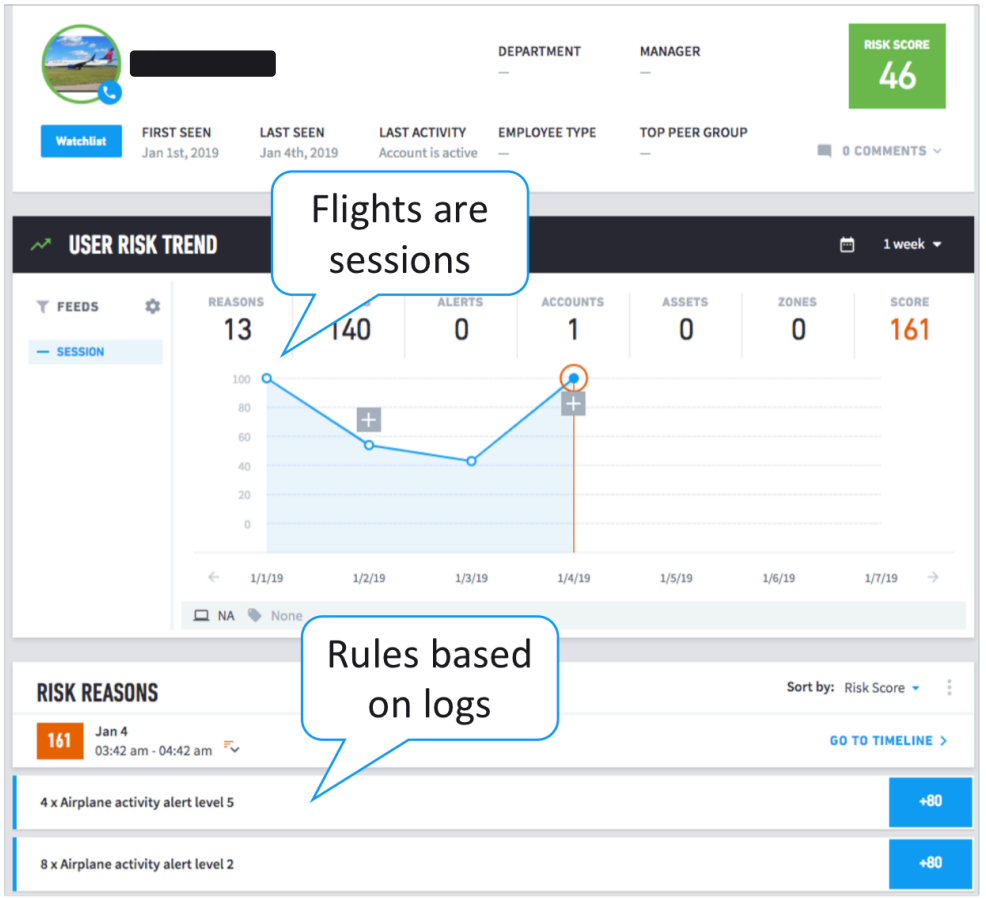

exabeam
HOW DOES LEGACY SIEM WORK TODAY?


exabeam
HOW DOES LEGACY SIEM WORK TODAY?


exabeam
USE CASES

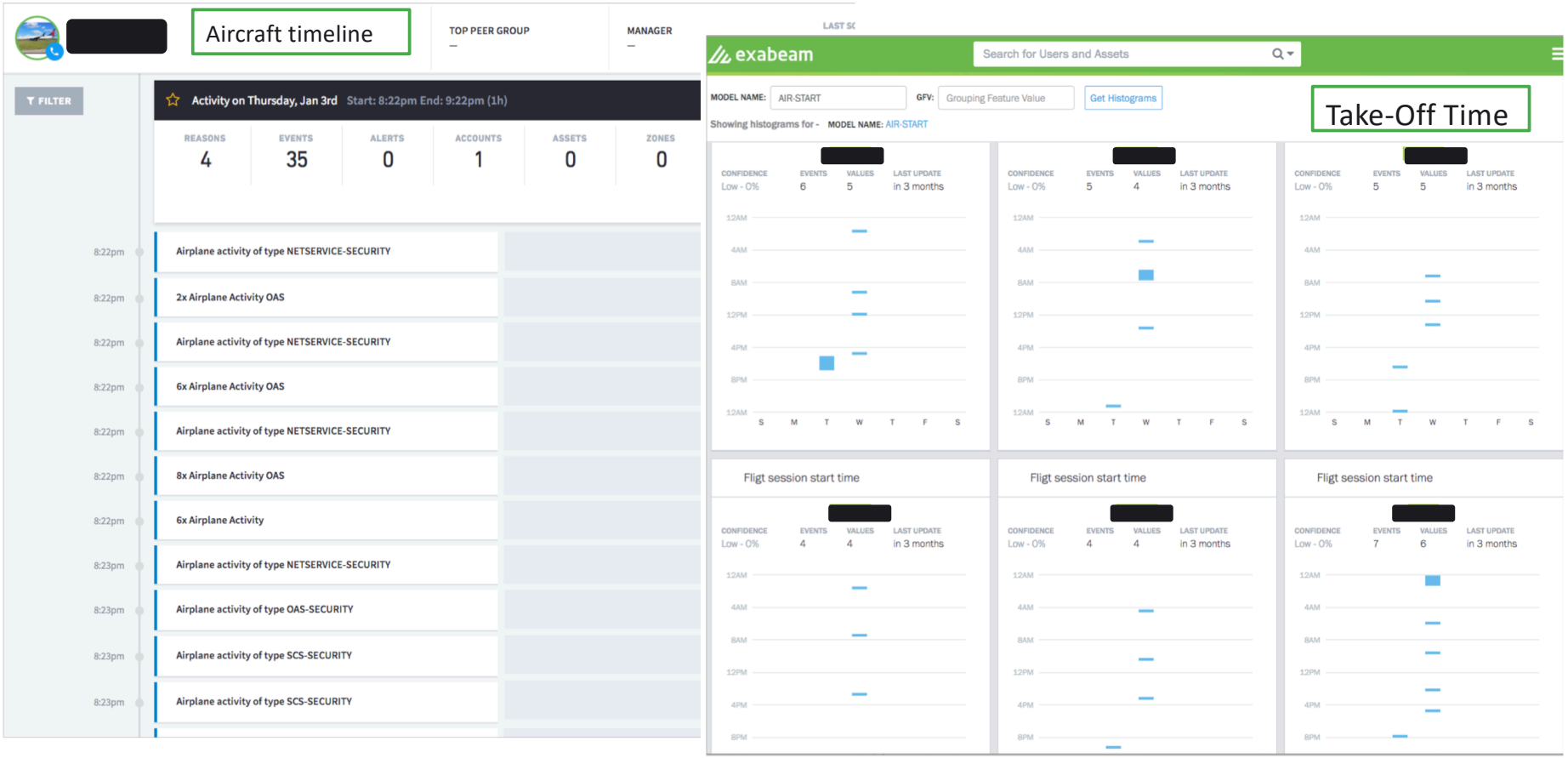
Use Case 1: Aircraft Behaviour





beam

Use Case 1: Aircraft Behaviour – timelines and models



exabeam

Use Case 2: Legal Application – iManage DMS

- Abnormal activity within iManage DMS i.e creating/modifying/exporting actions
- Abnormal number of objects (files) accessed
- Abnormal access from source machine
- Abnormal quantity of files exported
- Abnormal client access to DMS (word, excel, thinclient etc)
- Abnormal executive management activity within DMS (something which could be akin to compromised credentials)
- Abnormal time of day/night accessing DMS
- Abnormal source network zone where DMS is accessed from

exabeam

Use Case 2: Legal Application – iManage DMS

DMS Model #1 – Monitoring # of Document Exports

Use Case Requirements:
Model for each and every user in the environment how many documents they normally export, and alert if an abnormally large number of documents are being exported compared to their norms.

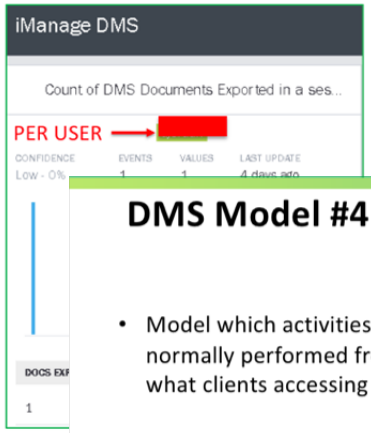
Objective:
Detecting DLP violations

Outcome:
This is a pre-existing Application Model that was customized in ~10 minutes to meet the requirements of a custom use case. An example of how Exabeam can assist with DLP use cases.

name	description	modelTemplate
DMS-UExp-Number	Models the number of DMS Documents Exported in a session	Count of DMS Documents Exported in a session

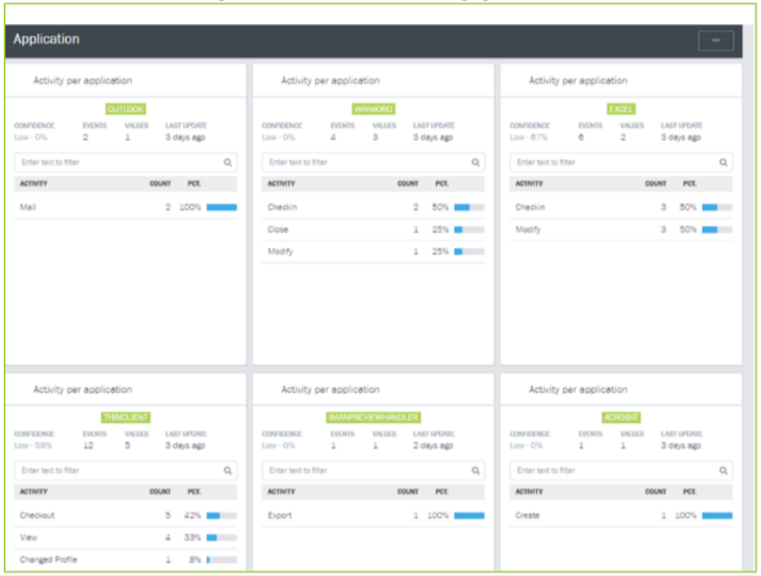
scopeType	scopeValue	featureName	featureType
USER	user	Docs Exported	quantity

histogramEventTypes
session-end:vpn-logout

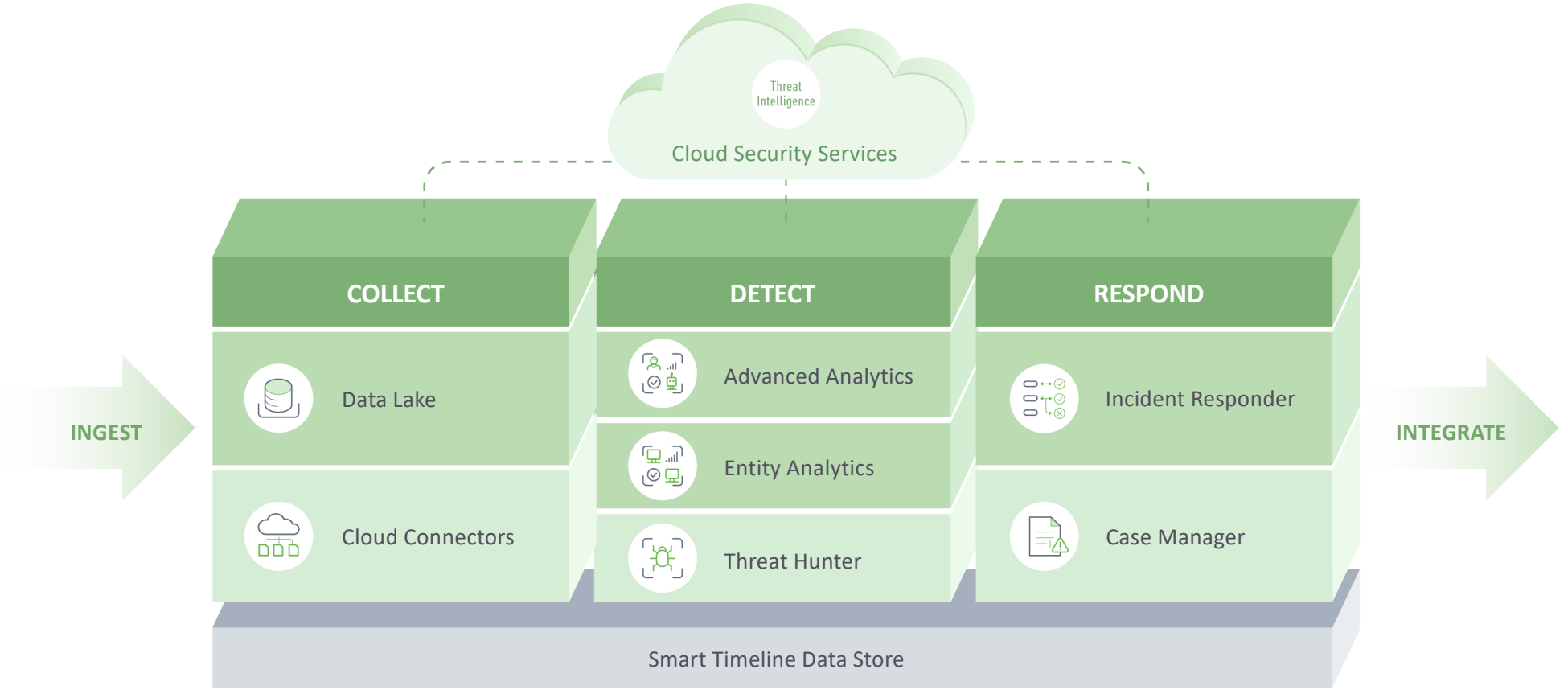


DMS Model #4 – Abnormal activity from Client Application

- Model which activities are normally performed from what clients accessing DMS
- Specific actions e.g. "**Mail**" will normally occur from client applications e.g. "**OUTLOOK**"
- Should Exabeam spot suspicious activities from abnormal clients, additional risk points will be generated



Exabeam Security Management Platform



exabeam

Next steps

Learn how Exabeam helps address:

- Insider Threat Detection
- SOC Automation
- Cloud Security
- IoT Monitoring
- Compliance

Dive deeper on Exabeam technology:

- Data Lake
- Advanced Analytics
- Entity Analytics
- Threat Hunter
- Incident Responder

exabeam