MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

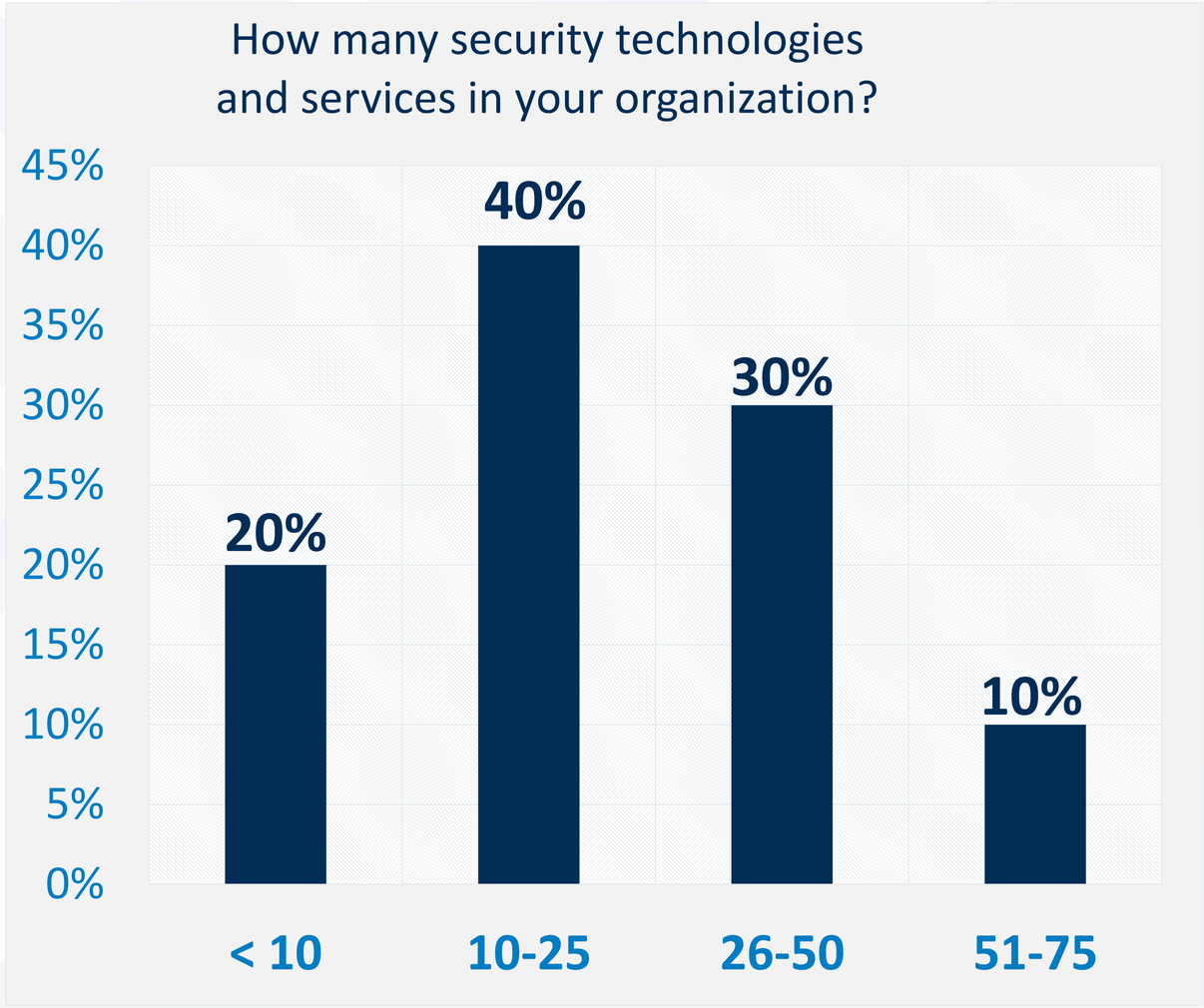
DETECT AND INVESTIGATE SUSPICIOUS BEHAVIOR WITH UEBA

Brandon Pace

Sales Engineer, LogRhythm

KEY MARKET TRENDS

- **Growing challenges from threat landscape and regulation**
- **Worsening shortage of qualified analysts**
- **Broadening set of disconnected security tools and data**
- **Significant interest in automation and orchestration (SAO)**
- **Artificial Intelligence gaining traction for security use cases**



InfoSec World
Conference & Expo 2018

USER *AND ENTITY* BEHAVIOR ANALYTICS?

“Wait a second, when did THAT happen?!”

UBA/UEBA

User Behavior Analytics (**UBA**):

- Detects insider threats, targeted attacks and financial fraud
- Observes human behavior patterns
- Applies algorithms/rules/statistical analysis to detect anomalies & threats

User and Entity Behavior Analytics (UEBA):

- Profiling & anomaly detection based on a range of analytics approaches
- Everything UBA offers, plus **supervised and unsupervised machine learning**
- Expands to evaluate the activity of users ***and other entities***
  (hosts, applications, network traffic and data repositories)

UEBA QUESTIONS AND USE CASES

Insider Threats and Data Exfiltration

Are you concerned with internal users intentionally or inadvertently sharing your intellectual property?

Compromised Accounts

What risks do you have if a user had a weak password or if it was found on a sticky note?

Account Takeover

Do you have assets (IP, customer data, records) that would motivate a security breach?

System Account Misuse

What damage could privilege account abuse create?


Behaviors
& Patterns


DISCOVER SOMETHING GREATER THAN YOURSELF

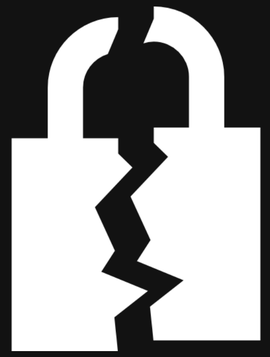

Accounting
DevOps
Human Resources
I.T. Security
ACLs
Access Credentials
Firewall Rules
Role-Based Access Control
URL Filtering

***25% of data breaches involve an insider threat**

****62% of users have access to data they shouldn't**

*****69% of organizations reported a recent insider data exfiltration attempt**

The Malicious Insider
The Compromised Insider
The Accidental Insider



**** Verizon Data Breach Investigations Report (2017)***

***** Ponemon Institute (2016)***

****** Accenture (2016)***

The Malicious Insider

McDonnell Douglass
F-15 Eagle
In Service: 1976-Present
Combat Record: 100 - 0

Boeing
F-15 2040C

Compromised Insider

- Vendor account compromised by a hacker
- Hacker ultimately made his way in
- Difficult to stop since compromised account resembled legit user
- When people have keys to the kingdom, monitoring vigilance is key

The Accidental Insider

- Spreadsheet of customers who had gift cards for Woolworths.
- Vouchers totaled over $1 million dollars across 8,000 people
- Emails sent to these gift card holders.
- Accidentally shared the full gift card spreadsheet plus instructions
- Scrambled to replace the gift cards and apologize for the leak

Attack Lifecycle

Modern threats take their time
and leverage the holistic attack surface

Early neutralization stops cyber incidents & data breaches

USER-BASED ANALYSIS TECHNIQUES

- **Common Event Searches**
  - Require host or application knowledge
  - Applicable to a given timeframe
- **Leverage (extensive) Infrastructural Knowledge**
  - To identify something out of the norm
- **Manual Searching through Alarms, Events, and Logs**
  - Upwards of **millions or billions** of messages per day

  Warning: *Alert Fatigue*
- **Analysts Must Focus on <u>Actionable Data</u>**
  - Can only investigate one thing at a time
  - Virtually impossible to scale effectively
  - Correlation of disparate (seemingly unrelated) events *even harder*

SPECTRUM OF ATTACKS REQUIRES ANALYTICS IN DEPTH

Brute-force

Spear-phishing

Zero-day

Rootkit

Session hijacking

Insider threat

Commodity malware

Custom malware

Spectrum of Attacks

Real-time threat detection via scenario-based analytics

Anomaly detection via deep behavioral profiling


Machine
Learning

A *subfield of CS*, Machine Learning is a type of Artificial Intelligence that enables computers to *learn sans* explicit programming.

Built on **algorithms** that detect patterns in data and adjust accordingly.

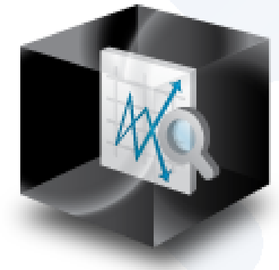
Supervised - apply past knowledge to new data

Unsupervised - draw inferences from datasets

TRADITIONAL DETECTION & RESPONSE SHORTCOMINGS

- **Not all incidents are started with malware, use specific "hacker tools," or leave readily available evidence for analysis**
- **Advanced threat actors leverage common administrative tools and attempt to blend into the spectrum of normal**
- **Operational Technology (IOT, SCADA, ICS, Medical Devices) can be sensitive and only *passively* accessible for security**
- **Indicator of Compromise (IOC) Threat Intelligence is too reactive (short TTL, slow public reveal); Attacker(s) can breach by the time you get IOC-based intel**

CORRELATION ENGINES



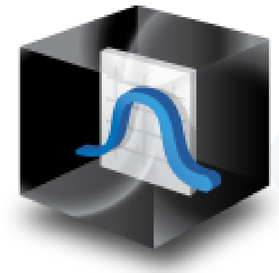
- Correlation engines identify threats in real time by performing multiple, *automated* analytical techniques on data

Scenario-based analytics expose threats other approaches miss

- Eliminates blind spots by analyzing all data types
- Identifies zero-day attacks by *not relying on previously established patterns*
- Minimizes false positives by corroborating disparate aspects of a single security incident detected by different analytical techniques

Reduces Time-to-Detect and Time-to-Respond

- Abnormal end-user behavior (Statistical and trend analysis over time)
- Insider detection (Employee data theft, internal espionage)
- Change in system behavior (Failed applications or SW components)
- Prioritize the most significant security risks



THE VALUE OF UEBA

- **UEBA cuts across everything without needing all those capabilities configured, set up, and perfectly tuned**
- **Focuses on user *behaviors*, regardless of your other protective *and* detective technology investments**
- **Bridges the gap in existing detection and response capabilities**
- **Easily integrates into your existing Security Ops Center workflow**

BEHAVIORS: A DIMENSION OF USER ANALYSIS

Each behavior is modeled and evaluated by a set of quantitative features derived from authentication data

Origin/Impacted Host Behavior	Authentication Classification Behavior	Origin Location Behavior	Authentication Time Behavior
Features: • Max • Mean • Standard Deviation • Total Count • Unique Count • New Count	**Features:** • Success Count • Fail Count • Percent Fail • Common Event Counts • Unique Common Event Count • New Common Event Count • Common Event Distribution Divergence	**Features:** • New Count • Distance Mean • Distance Standard Deviation • Distance Max • Unique Count	**Features:** • Auth Time (NormalDate Hour)

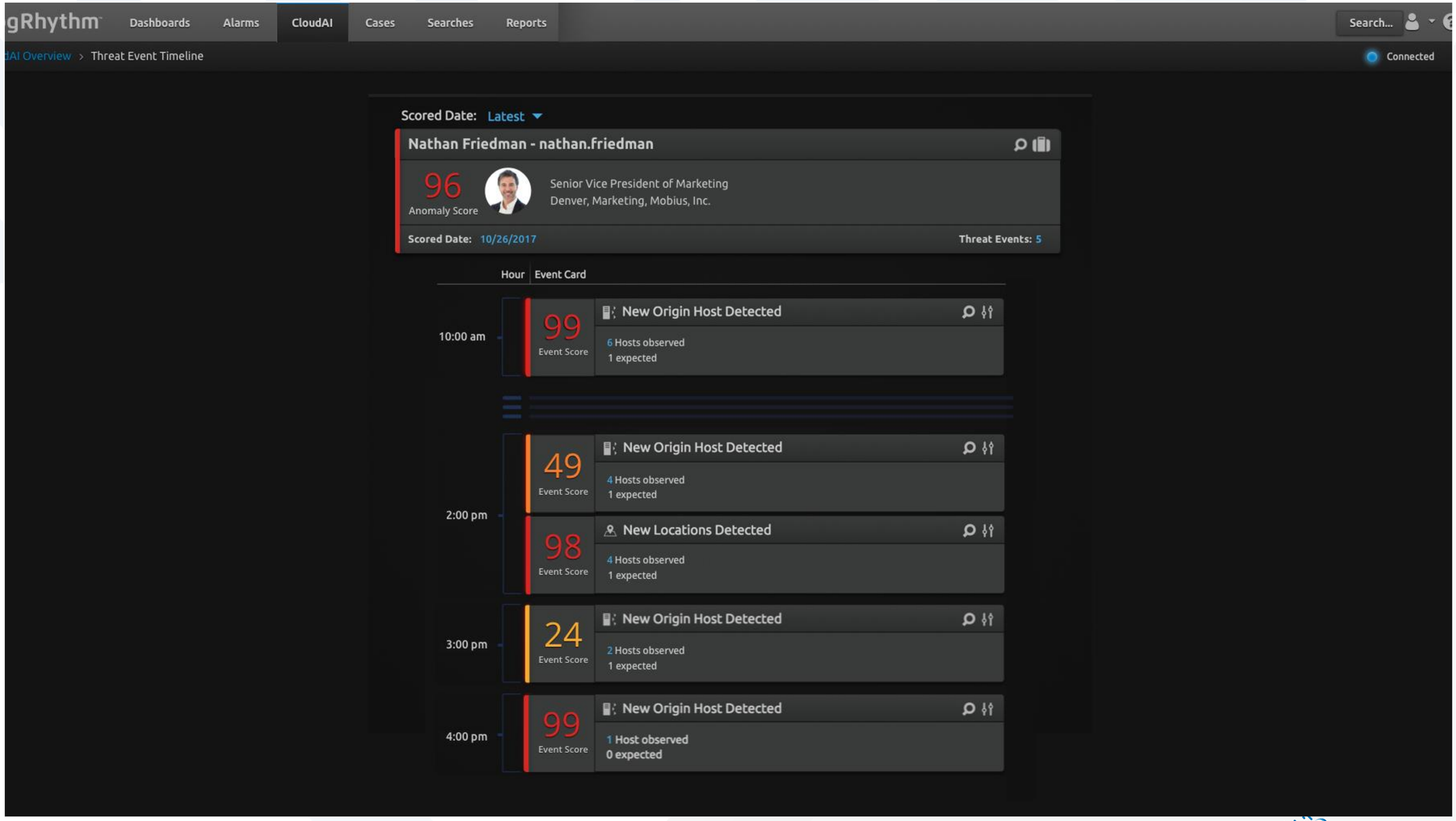
Attack Lifecycle to Progression Correlation

LOGRHYTHM UEBA (POWERED BY CLOUDAI)

Detects advanced threats via Machine Learning, Artificial Intelligence, and statistical analysis

- ✓ Model user behavior to reveal anomalous activity
- ✓ Uncover insider threats, compromised accounts, administrator abuse, and other user-based threats
- ✓ Detect previously unknown attacks/methods
- ✓ Accelerate qualification and investigation with powerful visualizations
- ✓ Achieve rapid time-to-value with cloud delivery, automated data processing, and tuneless analytics

LOGRHYTHM UEBA (POWERED BY CLOUDAI)



MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Brandon Pace

Sales Engineer, LogRhythm