PRESIDIO | LogRhythm

LogRhythm UEBA: Advanced Analytics UEBA

Use machine learning to detect insider threats, compromised accounts, and more

With the dramatic increase in the number of cyberattacks and their advancement in complexity and sophistication, it's crucial to expand detection capabilities with advanced analytics such as machine learning (ML). As reinforced by the MITRE D3FEND Framework™, anytime threat detection related to user behavior requires you to search for statistical outliners that aren't obvious, or to make a comparison against a user's baseline, you need to use advanced analytics. LogRhythm UEBA is LogRhythm's advanced user entity behavior analytics (UEBA) solution.

Benefits

- **Detect:** Identify outliers and unusual user activity
- **Achieve:** Attain rapid time to value with ML algorithms
- **Integrate:** Easily integrate with the LogRhythm SIEM
- **Stay in the know:** Keep up with the threat landscape with continuously improved models

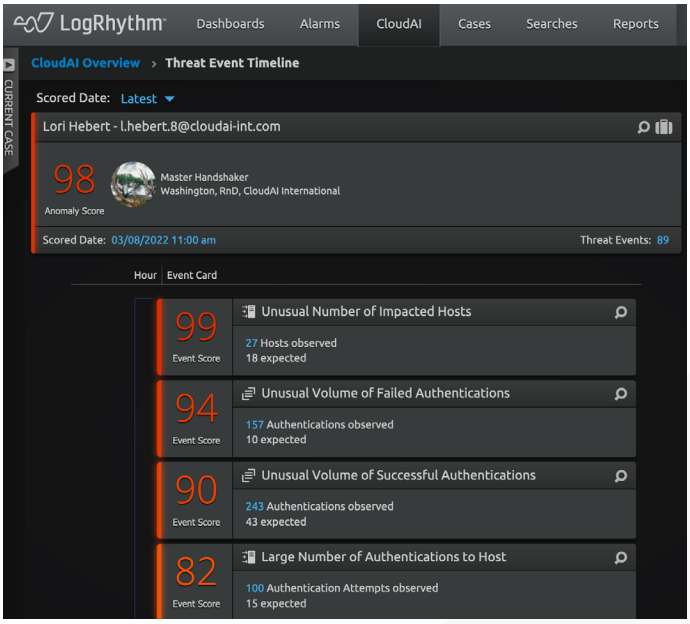

Figure 1: The Threat Event Timeline provides information about the anomalies observed.

LogRhythm UEBA, a cloud-native add-on to the LogRhythm SIEM Platform, uses ML to detect anomalies related to potential user attacks such as insider threats, compromised accounts, administrator abuse, and misuse. Together, LogRhythm UEBA and the field-proven threat models of the LogRhythm SIEM AI Engine deliver holistic analysis and deep visibility into user activity and outliers that would otherwise go undetected.

LogRhythm UEBA detects changes in user behavior that signal potential threats. Analysts can use the individual anomaly scores and a summary user score to prioritize anomalies for investigation and response.

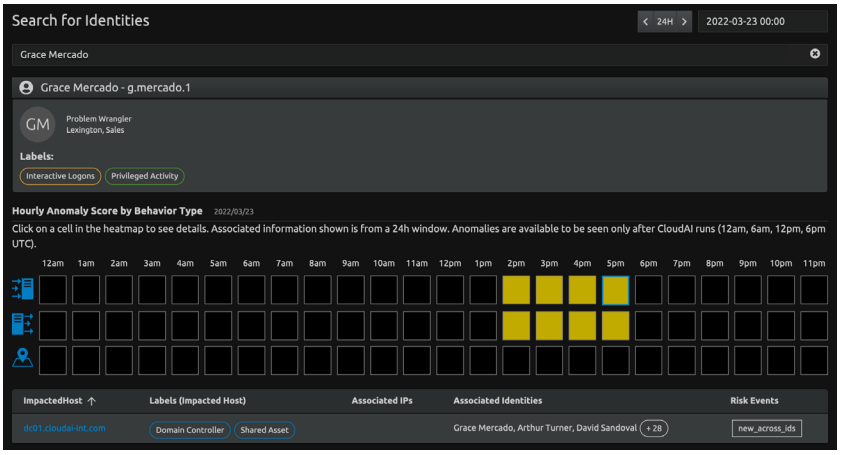

Figure 2: The LogRhythm UEBA heat map provides details about the anomalies including behavior-based labels.

SIEM integration

Formerly known as CloudAI, LogRhythm UEBA functions as an advanced UEBA log source in the SIEM. As with any other log in the SIEM, you can build customizable dashboards, run and save searches, and leverage AI Engine rules setting alarms and, SmartResponse™ automated actions when desired. LogRhythm makes integration simple. LogRhythm UEBA seamlessly integrates with the LogRhythm SIEM, allowing analysts to easily incorporate advanced UEBA analytics into their workflow.

```
2022-03-23T19:00:46-06:00 EventType=6 EventID=4 Version=1.0
EventTime=2022-03-23T20:00:00+00:00 Identity="2287" IdentityName="Danielle
Watkins" IdentityLabels=["Interactive Logons","Privileged Activity"] OriginLocation=
(United States, Michigan, Dearborn) Description="The user authenticated from an
unusual number of new geographical locations. This occurs when a user authenticates
from a new geographical location and may correspond to a user traveling or
authenticating from a server in a new datacenter."
CountermeasureMitreD3fendID="D3-UGLPA" EventTypeName="new"
EventName="OriginLocation" Severity="critical" DetectorScore=99.0 Expected=0.0
Observed=1.0
```

Figure 3: An example of a LogRhythm UEBA anomaly log processed in the SIEM.

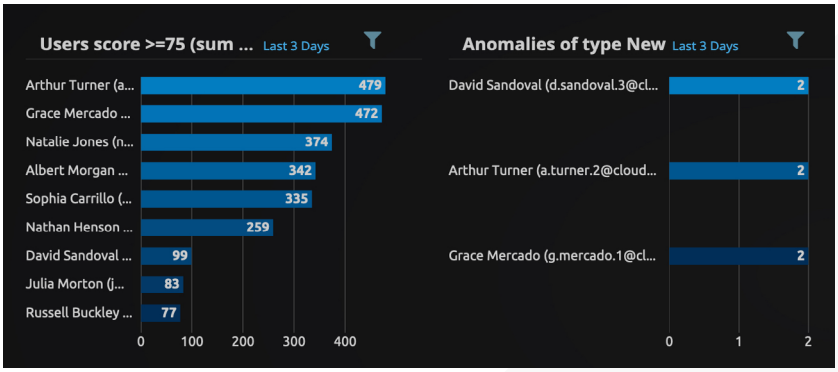

Figure 4: The LogRhythm SIEM dashboard features LogRhythm UEBA events.

LogRhythm UEBA in action

LogRhythm UEBA uses machine learning to detect outliers. AI Engine, an integrated component of the LogRhythm SIEM Platform, works with LogRhythm UEBA to offer UEBA holistic analytics. LogRhythm UEBAexpands detection coverage on top of existing out-of-the-box AI Engine UEBA rules by detecting outliers without the need of explicit defined logic. With LogRhythm UEBA, security analysts have additional layers of detection. LogRhythm UEBA is also SOC-2 compliant.

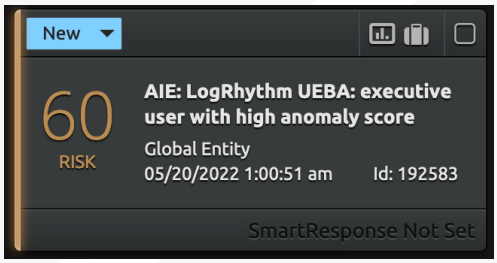

Figure 5: An alarm triggers when a LogRhythm UEBA event occurs.

Detect anomalies with machine learning

LogRhythm UEBA evolves with your SIEM environment. It uses several different machine learning models for continuous, automated tuning without manual intervention, so your security quickly grows smarter. LogRhythm UEBA observes authentication behaviors and identifies anomalies by developing a baseline of normal behavior for identities, then raises observations when an identity deviates from that baseline or from all identity baselines. LogRhythm UEBA uses a variety of models to detect anomalies that can be classified into two main categories:

- **Individual Anomalies:** These models analyze when an identity is anomalous in relation to its own baseline.
- **Group Anomalies:** These models analyze when an identity is anomalous in relation to its peers or anomalous in relation to all monitored identities.

In addition, LogRhythm UEBA uses different methods of evaluation for each category that includes numerical analysis as well as metadata content analysis.

Leave data preparation to LogRhythm

LogRhythm's experience in security analytics provides vital expertise in the preparation and analysis of metadata by LogRhythm's Machine Data Intelligence (MDI) Fabric. The MDI framework provides data enrichment and normalization with unique, rich metadata and contextual information that are automatically fed from the LogRhythm SIEM Platform into LogRhythm UEBA. This built-in support allows your organization to forgo the professional services engagements required by other UEBA vendors.

LogRhythm's expertise in log parsing and metadata extraction enables high fidelity in the models. Our focus on clean data enables LogRhythm UEBA to surface potential threats more effectively.

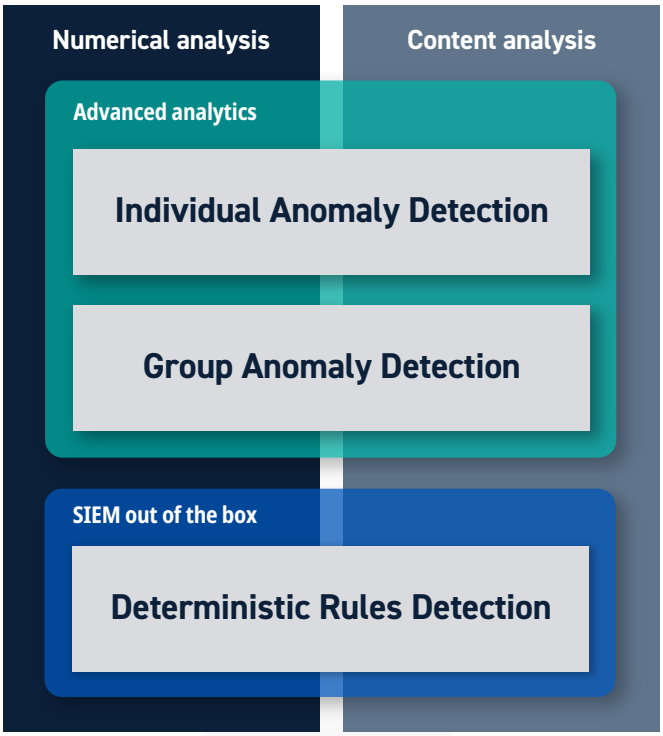

Figure 6: This is LogRhythm's holistic UEBA analytics approach.

Get smarter, faster with LogRhythm UEBA

LogRhythm UEBA is our advanced UEBA analytics solution that adds extra layers of detection to your organization against potential threats. The solution seamlessly integrates with the LogRhythm SIEM and self-evolves through machine learning.It can provide value in just weeks, enabling continuous tuning without manual intervention.

Ready to defend.

LogRhythm helps busy and lean security operations teams save the day—day after day. There's a lot riding on the shoulders of security professionals. LogRhythm helps lighten this load. As allies in the fight, LogRhythm combines a comprehensive and flexible SIEM platform, technology partnerships, and advisory services to help SOC teams close the gaps.

Learn more. Contact our sales team today: sales@logrhythm.com

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 330 // +65 6222 8110 // +61 2 8019 7185

www.logrhythm.com