UserXDR

As threat actors increase their sophistication and frequency of attacks, the threat landscape becomes increasingly complex and unpredictable. From motivated insiders to well-armed nation-states, potential threats to an organization are diverse in nature and increasingly difficult to detect.

Focusing on user-based threats is a critical method for combating an expanding attack surface. With an increasing number of attacks involving insider accounts, either through negligence or malicious intent, many security teams recognize a significant challenge targeting these more nuanced threats with manual procedures. Organizations feel increasingly vulnerable due to excessive privilege access and the rising number of devices with access to sensitive data.

Full Spectrum Threat Coverage

LogRhythm UserXDR is a User and Entity Behavior Analytics (UEBA) solution that enables your security team to quickly and effectively detect and respond to known and unknown threats. Providing evidence-based starting points for investigation, the solution employs a combination of scenario-based analytics (e.g., statistical analysis, rate analysis, trend analysis, advanced correlation), and supervised and unsupervised machine learning (ML) techniques. Complementing the automated risk analysis achieved through ML, scenario-based analytics allow security teams to strengthen their security posture through scenario customization. A graphical builder and extensive library of scenarios enable analysts to quickly create organization-specific alarms without complex data science knowledge.

Through this variety of analytical techniques, UserXDR leverages diverse environmental data to uniquely expose user-based threats, such as insider threat, account compromise, and account privilege abuse. To ensure accurate and collective analysis of all associated user activity, UserXDR utilizes TrueIdentity, a feature that maps disparate accounts and unique identifiers to build a singular user identity for comprehensive monitoring. With TrueIdentity, anomalous and potentially malicious activity can be successfully attributed to the appropriate identity, supporting quicker threat detection and response.

Top User-Based Threats

Insider Threat: A security threat that originates from within an organization, inadvertantly or through malicious intent

Account Compromise: An account that is accessed by an unauthorized entity for malicious purposes

Privilege Abuse: The creation and deletion of privileged accounts, elevation of permissions, and suspicious use of privileged accounts by a malicious entity

Benefits

Uncover insider threats, compromised accounts, privilege abuse and other user-based threats

Detect known and unknown threats with a variety of analytical techniques

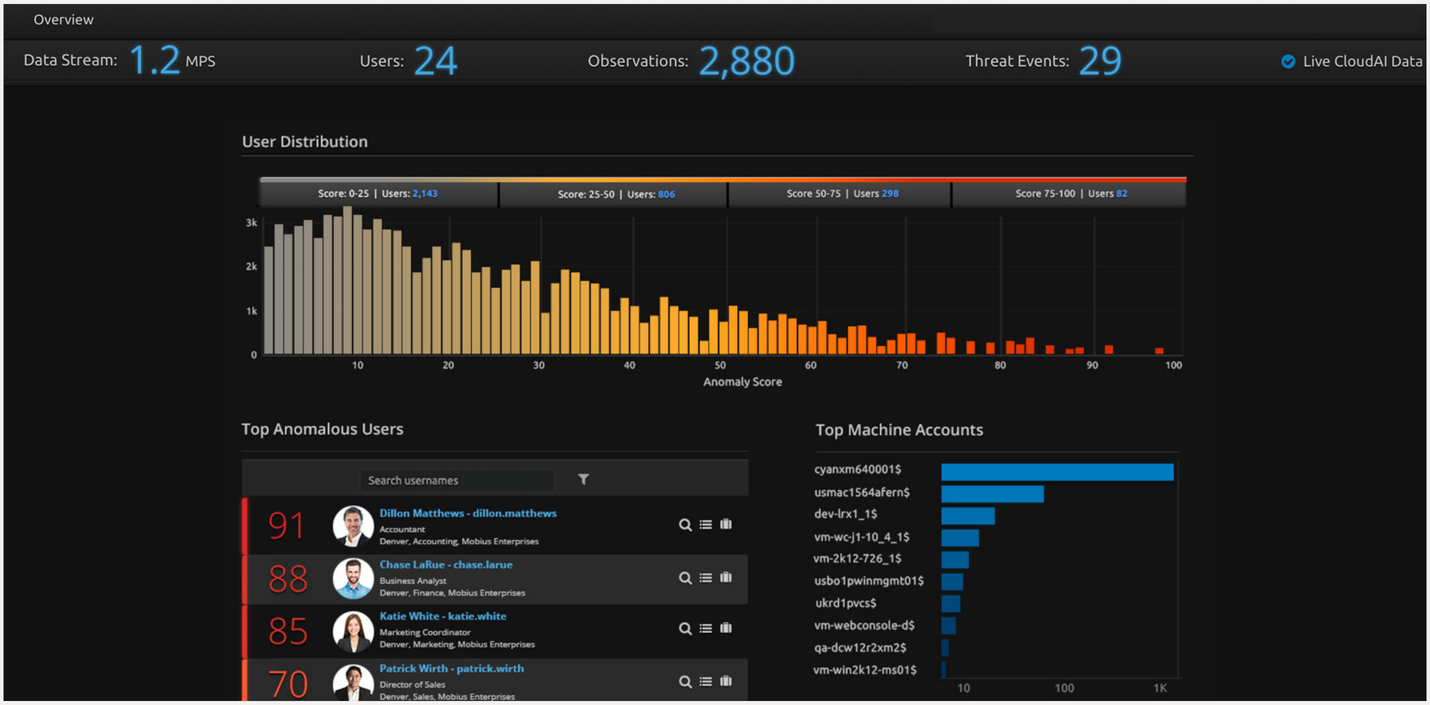
Reduce noise and false positives by corroborating machine learning and scenario analytics for risk-based prioritization

Realize rapid time to value through automated user baselining and peer-group analysis

Streamline incident response with orchestrated playbooks and task automation

By applying risk context and corroborating evidence to a user behavior, UserXDR enables organizations to more accurately identify security relevant activity, reducing time spent investigating false positives.

Peer group analysis provides additional validation by comparing user activity against the baseline of other individuals in a similar role, further verifying the extent of the abnormal behavior. Accounting for the changing threat landscape, UserXDR continues to evolve through updated content from LogRhythm Labs' threat research and global feedback, ensuring emerging threat tactics and techniques are continuously recognized



Overview

Data Stream: 1.2 MPS | Users: 24 | Observations: 2,880 | Threat Events: 29 | Live CloudAI Data

Top Anomalous Users

Search usernames

91 Dillon Matthews - dillon.matthews
Accountant
Denver, Accounting, Mobius Enterprises

88 Chase LaRue - chase.larue
Business Analyst
Denver, Finance, Mobius Enterprises

85 Katie White - katie.white
Marketing Coordinator
Denver, Marketing, Mobius Enterprises

70 Patrick Wirth - patrick.wirth
Director of Sales
Denver, Sales, Mobius Enterprises

The customizable UEBA dashboard provides a holistic view of the entire user base while focusing on users and activity that present the highest risk.

Accelerated Time to Value

Faster setup and configuration results in decreased risk, a critical objective of any security team. With UserXDR, automated user baselining and risk analysis removes the need for time-intensive configuration and tuning while also tailoring the solution to each user's unique behavior. By improving the signal-to-noise ratio, security teams focus their time on investigating more meaningful activity instead of drowning in false alarms.

Achieving rapid time to value relies on accurate analysis, with data analysis only being as effective as the underlying data. LogRhythm's patented Machine Data Intelligence (MDI) Fabric—a framework for data normalization and enrichment—provides unique, rich metadata thathelps security teams quickly troubleshoot issues and ensure accurate analysis. By leveraging classification, contextualization, and time normalization, our MDI Fabric empowers security teams to realize use cases quickly and effectively.

Streamlined Security Operations

Adding UserXDR to the LogRhythm NextGen SIEM delivers the additional benefit of embedded Security, Orchestration, Automation, and Response (SOAR) capabilities that optimize analyst workflows for faster threat qualification and mitigation. The SOAR feature set enables analysts to automate a wide variety of investigative and response efforts. Integrated analyst playbooks, centralized evidence collection, and automated tasks decrease your mean time to detect (MTTD) and mean time to respond (MTTR).

Automated data processing, tuneless analytics, and robust visualizations provide pervasive visibility into user behavior, reducing MTTD and MTTR and freeing up security resources to address the most critical threats.

Request a demo today.

logrhythm.com/demo

www.logrhythm.com

LogRhythm®