Logpoint UEBA

Advanced attacks to your organization often rely on compromised accounts or insiders performing risky actions. Logpoint UEBA detects unknown threats by determining abnormal from normal behavior. Make events more insightful than ever, and cut detection and response time significantly.

LOGPOINT
DASHBOARD
SEARCH
REPORT
INCIDENT
SETTINGS
UEBA
THREAT INTELLIGENCE
DARKTRACE
NESSUS
SOC
LP_AD: USER ACCOUNT MANAGEMENT
GENERAL ACTIVITIES
LP_NW: NETWORK ACCESS
OVERALL RISK
EXPLORE
Analytics were run on February 29, 2020 on the data ingested between December 22, 2019 and February 20, 2020
114,831,487
Events Analyzed
2,590
Anomalies Found
3
Active Risky Entities
There are 3 entities with extremely high risk scores:
10
Users
5
Websites
4
Servers
3
Shares
Overall risk is high and increasing rapidly
On February 20, 2020 the threat of Potential Lateral Movement is contributing 36% to the overall risk:
EXTREME
Dec 29
Jan 05
Jan 12
Jan 19
Jan 26
Feb 02
Feb 09
Feb 16

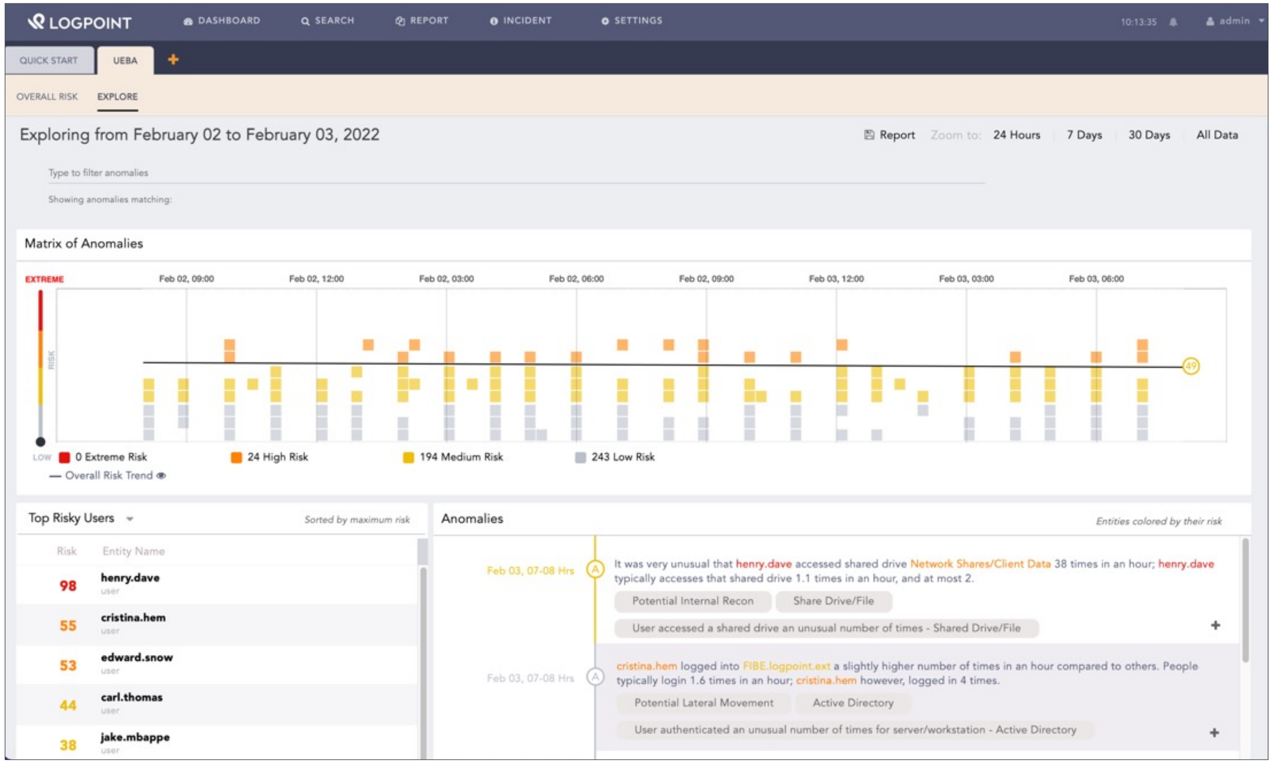
/logpoint

Detect unknown risks and threats early with UEBA

Logpoint user and entity behavior analytics (UEBA) helps your security team better respond to threats. UEBA tools analyze the behavior of users and entities, such as hosts, devices, files, and transactions, to find suspicious or malicious behaviors and patterns coming from inside or outside of your organization.

Using machine learning, Logpoint UEBA builds baselines for normal behavior for each user and entity in the network, without following predefined rules or signatures. By evaluating activity against these baselines, UEBA detects any unusual behavior and frees up time for security analysts to focus on finding real threats.

Combining UEBA and security information and event management (SIEM) helps your security team effectively monitor and react to abnormal activities. Mitigate risk, damage, and data loss by detecting advanced attacks early.



Exploring from February 02 to February 03, 2022

Matrix of Anomalies

🟥 0 Extreme Risk 🟧 24 High Risk 🟨 194 Medium Risk ▨ 243 Low Risk
— Overall Risk Trend

Top Risky Users
Sorted by maximum risk

Risk	Entity Name
98	henry.dave user
55	cristina.hem user
53	edward.snow user
44	carl.thomas user
38	jake.mbappe user

Anomalies

Feb 03, 07-08 Hrs — It was very unusual that henry.dave accessed shared drive Network Shares/Client Data 38 times in an hour; henry.dave typically accesses that shared drive 1.1 times in an hour, and at most 2.

Feb 03, 07-08 Hrs — cristina.hem logged into FIBE.logpoint.ext a slightly higher number of times in an hour compared to others. People typically login 1.6 times in an hour; cristina.hem however, logged in 4 times.

UEBA displaying a detailed overview of anomalies.

Why you should enrich your SIEM-SOAR with UEBA

UEBA is an additional cybersecurity tool available on top of Logpoint SIEM extending the capabilities of the Logpoint SIEM-SOAR solution

Immediately spot insider threats

Detect suspicious behavior quickly and effectively across your network. Without UEBA, analysts need to create complicated, predefined rules to define what is normal and permitted. Since every individual has different habits, it would become a long list, especially if you employ hundreds of staff worldwide. And worse yet, it will never be definitive.

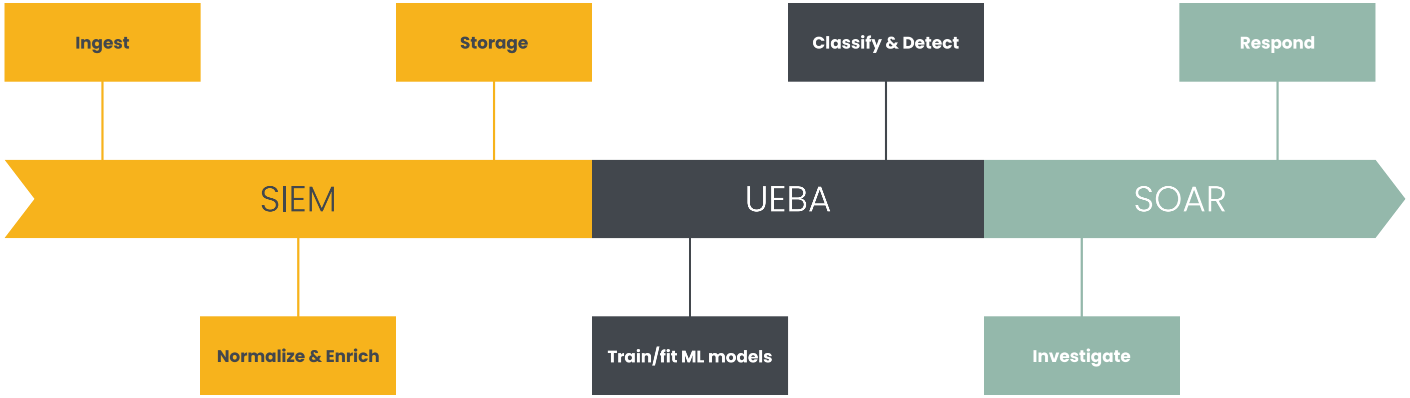
Data-centric threat detection

Our approach to threat detection is data-centric, focused on monitoring access to sensitive data, with an ultimate goal of ensuring data never gets to a point where it can be compromised. This specialty makes our UEBA solution suitable also for companies with emphasis on intellectual property.

Fast implementation and easy scalability

Logpoint's UEBA module is built on top of the most flexible and scalable SIEM solution on the market, making our UEBA have industry leading time-to-value for customers, allowing short time to deployment to create immediate insights. Our common taxonomy readily gives access to a wide array of machine learning models targeting investigation of abnormal behavior.

Logpoint products work together to create the best insights



UEBA can empower the capabilities of your SIEM-SOAR in many ways:

Combine data from UEBA with SIEM events to make the original events more insightful than ever

Free up your time to focus on genuine threats with UEBA eliminating false positives and cutting the detection and response time

Speed up your threat hunting capabilities with UEBA's visual dashboards and search templates

Utilize machine learning and advanced behavioral analytics to counter the shortage of experienced security analysts

Fully automate processes by having threat detection in UEBA and setting up automatic responses with the assistance of SOAR

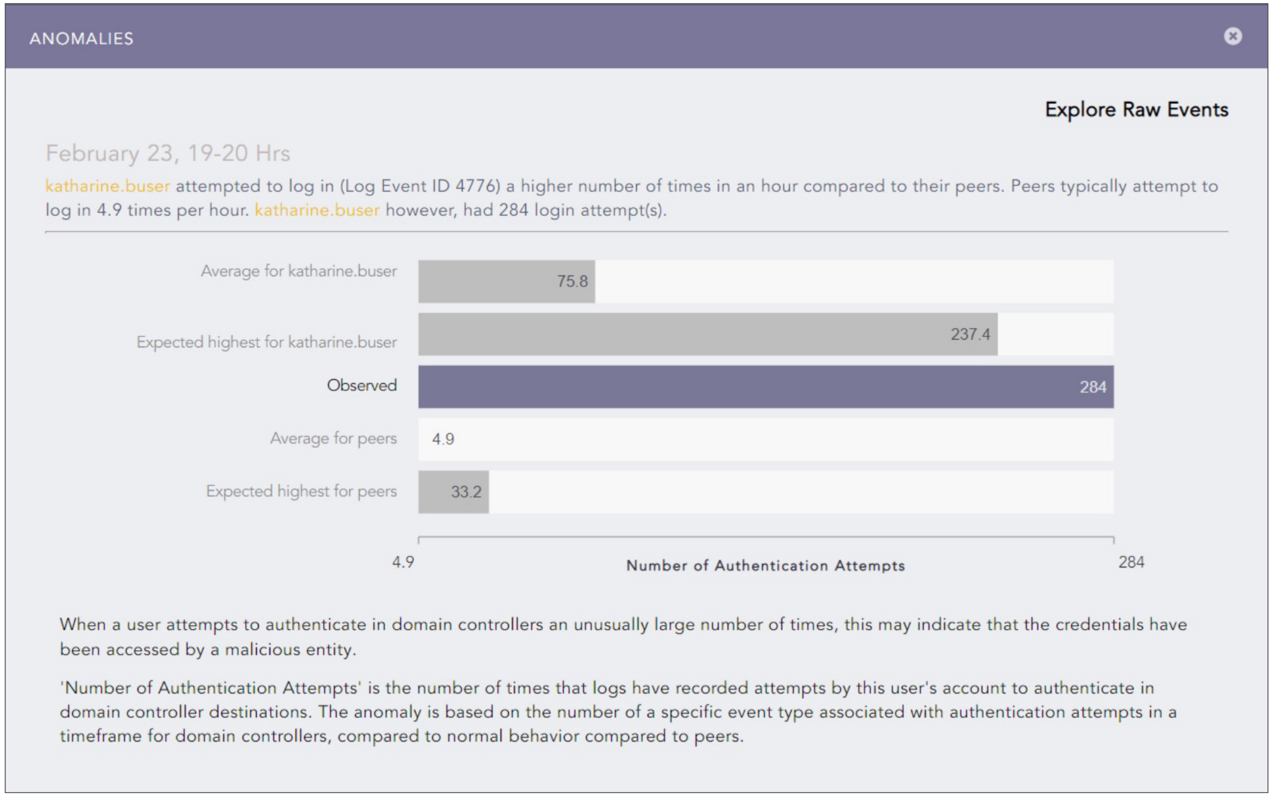
Common UEBA use cases

Logpoint UEBA, as an extension to your SIEM-SOAR, can catch complex threats coming from inside and outside of your organization. Here are three common use cases where the capabilities of UEBA stand out.

Detecting authentication abnormalities

The most popular type of intrusion is account compromise – it can take place in multiple parts of the ATT&CK kill chain for multiple reasons. This is one of the strongest aspects of Logpoint UEBA, as it is inherently a tool for tracking account activity and can be applied broadly and deeply to many different security use cases.

The most common of these cases is many concurrent logins, failed or successful. Not only will detecting this help in identifying malicious activity, but it also helps to detect misconfigured or undocumented service accounts in your environment. Said accounts also get automatically grouped together by a separate detector so that it is easier to have an overview.


ANOMALIES
Explore Raw Events

February 23, 19-20 Hrs

katharine.buser attempted to log in (Log Event ID 4776) a higher number of times in an hour compared to their peers. Peers typically attempt to log in 4.9 times per hour. katharine.buser however, had 284 login attempt(s).

Average for katharine.buser
75.8
Expected highest for katharine.buser
237.4
Observed
284
Average for peers
4.9
Expected highest for peers
33.2
4.9
Number of Authentication Attempts
284

When a user attempts to authenticate in domain controllers an unusually large number of times, this may indicate that the credentials have been accessed by a malicious entity.

'Number of Authentication Attempts' is the number of times that logs have recorded attempts by this user's account to authenticate in domain controller destinations. The anomaly is based on the number of a specific event type associated with authentication attempts in a timeframe for domain controllers, compared to normal behavior compared to peers.

Viewing login attempts

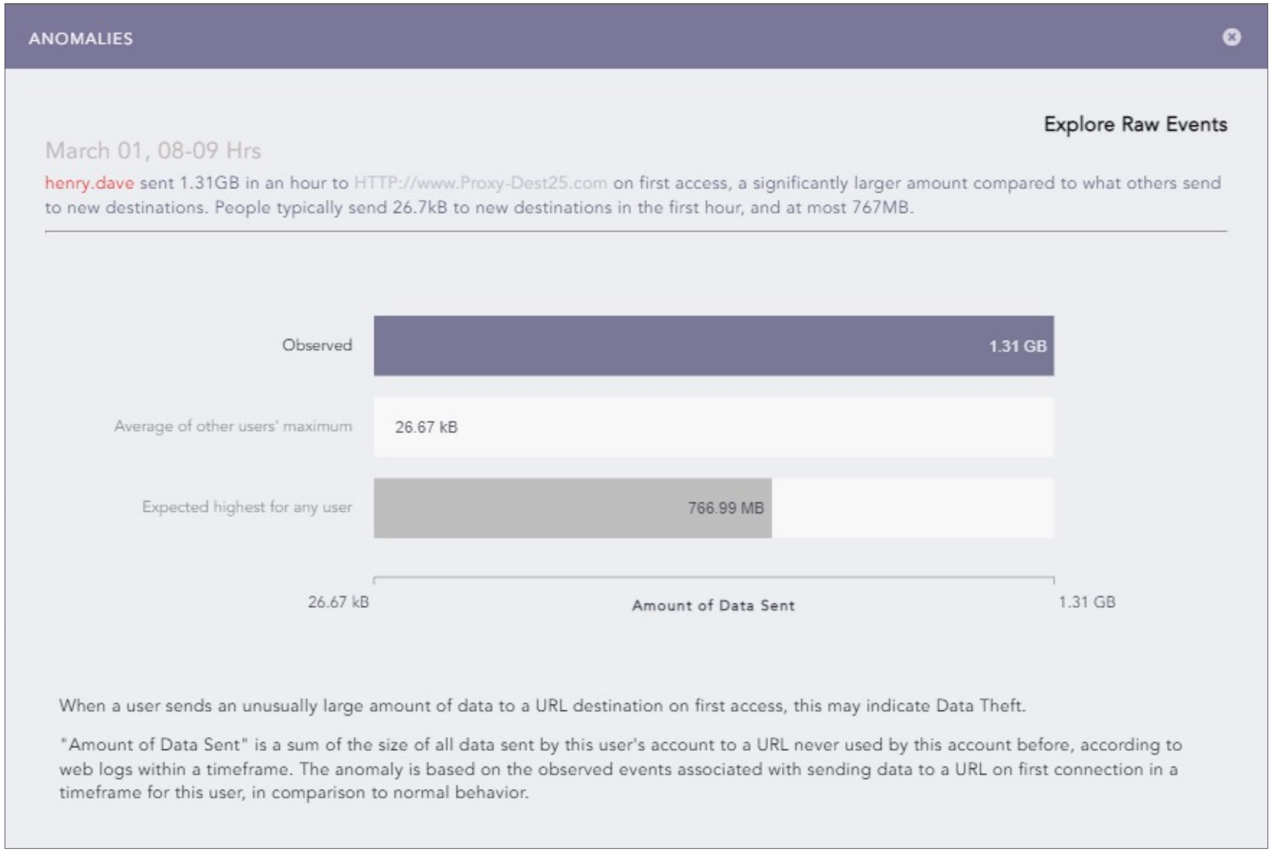
Besides manual analysis, login abnormalities is a good example of a use case to be set up as a trigger for SOAR playbook. When feeling unsure about taking action against an anomaly, you could set up a playbook that automatically runs checks against these suspicious accounts, so that when the analyst gets involved, they have a detailed, highly actionable picture.

Detecting suspicious data transfer activities

Another area where UEBA can offer significant assistance is by automatically analyzing the amount of data sent over the network by the accounts and devices in the environment. Because of its machine learning capabilities, UEBA can produce extremely precise judgments on the relative abnormality of occurrence in the environment. These automatic capabilities are a major improvement over any manually configured alerting.

The option of comparing a user to their peers also introduces a different level of precision into the equation, since, for example, comparing against the whole network in a global environment would not bae helpful nor informative to the analyst. Furthermore, the response can also be automated with the assistance of SOAR making it a completely automated set of steps.

An example of this is comparing the amount of data to an overall environmental baseline. The graphic also demonstrates the difference helping the analyst make a judgment about the level of abnormality.



ANOMALIES

Explore Raw Events

March 01, 08-09 Hrs

henry.dave sent 1.31GB in an hour to HTTP://www.Proxy-Dest25.com on first access, a significantly larger amount compared to what others send to new destinations. People typically send 26.7kB to new destinations in the first hour, and at most 767MB.

When a user sends an unusually large amount of data to a URL destination on first access, this may indicate Data Theft.

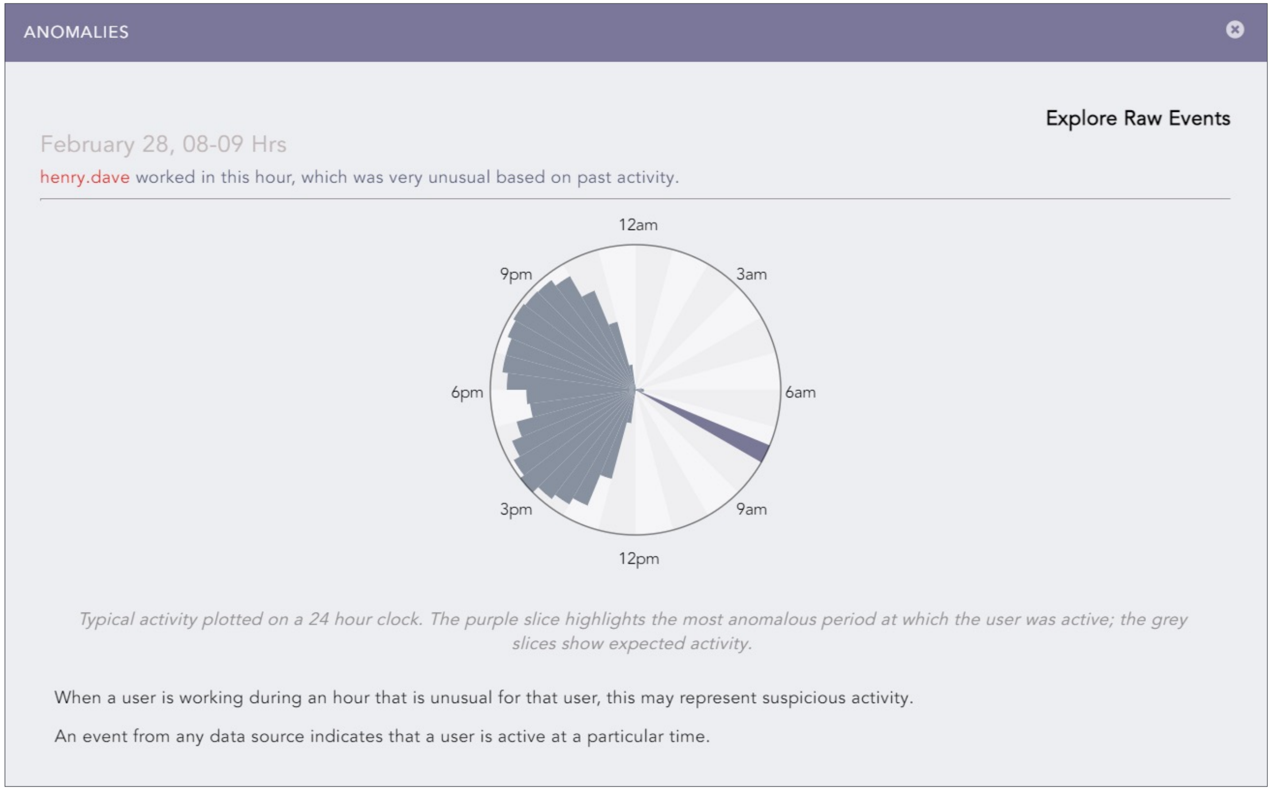
"Amount of Data Sent" is a sum of the size of all data sent by this user's account to a URL never used by this account before, according to web logs within a timeframe. The anomaly is based on the observed events associated with sending data to a URL on first connection in a timeframe for this user, in comparison to normal behavior.

Observing the amount of data sent

Detecting activity-based inconsistencies

Our UEBA solution has a highly granular way of measuring account activity, filtering out the events that are not directly associated with the actual account being used. This is also an area where peer grouping makes this even more insightful. Logpoint UEBA and the peer grouping capabilities focus on actual patterns instead of any pre-defined limits, and it does not require one to input time constraints as one would do with alerting.

A good example of how this works in practice is the 'unusual time worked' insider threat, which gets triggered when a particular account is active during hours considered abnormal when compared to their usual behavior. In the graphic, the user has been active during nighttime, which is unusual for them. In this type of anomaly, peer grouping also provides useful insights by displaying the most common working times in the company and automatically adjusts typical working hours if needed in a global environment.



February 28, 08-09 Hrs

henry.dave worked in this hour, which was very unusual based on past activity.

Typical activity plotted on a 24 hour clock. The purple slice highlights the most anomalous period at which the user was active; the grey slices show expected activity.

When a user is working during an hour that is unusual for that user, this may represent suspicious activity.

An event from any data source indicates that a user is active at a particular time.

Displaying unusual time worked

About Logpoint

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

Learn more about the benefits of our UEBA solution

To learn more about the benefits of our UEBA product and different download options, contact us: https://www.logpoint.com/en/contact/

Trusted by more than 1,000 enterprises

KONICA MINOLTA
CAPTIVATE
BOEING
GOSECURE
RÉMY COINTREAU

Awards and honors

Gartner peer insights customers' choice 2021
Gartner Peer Insights

Gartner
Gartner Magic Quadrant

Software Reviews GOLD MEDAL 2021 SECURITY INCIDENT AND EVENT MANAGEMENT

/logpoint