Defend your organization from insider threats using LogPoint UEBA 2.0

With LogPoint UEBA, you can easily detect both suspicious user behavior as well as other entities such as cloud, mobile or on-premise applications, endpoints, networks and external threats - out of the box. Unlike any other UEBA solution, the LogPoint UEBA module will work instantly across all data sources in your network. There is no need for time-consuming and expensive integrations, and our UEBA module will provide unparalleled time-to-value for your business, along with vastly cutting investigation time by your security team.

October, 2018

LOGPOINT

About UEBA

Advanced attacks and pervasive threats to your organization often rely on compromised credentials or coercing users into performing actions that damage enterprise security. To identify these types of attacks, you need a powerful solution that allows analysts to quickly determine normal versus abnormal activity on your network. Unfortunately, the cybersecurity tools and the attack detection mechanism are becoming obsolete, as attackers are able to bypass the perimeter defense used by many companies.

These types of security incidents are costly. The average cost of a data breach is close to $4 million or even higher in sensitive industries such as healthcare or finance. On top of the costs associated to the data breach, organizations often also have to face different legal fees and the cost related to restoring the company's reputation.

UEBA, short for User and Entity Behavior Analytics is a security process focusing on monitoring both suspicious user behavior as well as other entities such as cloud, mobile or on-premise applications, endpoints, networks and external threats. Utilizing Machine Learning, UEBA builds baselines for every entity in the network and actions are then evaluated against these baselines. This allows analysts to answer the question "What is normal?" and "What is abnormal?" instead of creating complicated predefined rules to define "What is allowed?", enabling analysts to achieve situational awareness before, during and after responding to breaches.

LogPoint's new UEBA module has industry leading time to value for customers, allowing same-day, zero-professional service deployments and immediate insights. This is possible since the UEBA engine benefits from being built on top of the most flexible and scalable SIEM solution on the market. This white paper focuses on highlighting how UEBA 2.0 extends your SIEM's Threat Hunting capabilities.

Insider threats or user based threats are threats originating from users inside your organization such as current or past employees or outside contractors. Although not all users trigger the attack vectors knowingly, they are still one of the main failing point in a security team's fight against cyber attacks. When it comes to user based threats, we distinguish threats caused by users knowingly triggering the attack vectors and threats caused by users unknowingly triggering the attack vectors. In the first case, the attack can be initiated by the user itself, or by an outside attacker. In the latter case, we can talk about phishing attacks or spear phishing attacks depending on whether the event is generic or specific.

Did you know?

53% of organizations confirmed they have fallen victim to an insider attack in the previous 12 months. And 27% of organizations say insider attacks have become more frequent.

Suspicious user behavior? Not on our watch. Detected in the cloud, on-premise and inside of business applications - out of the box.

Cybersecurity Insiders: 2018 Insider Threat Report

When it comes to defending your organization against insider threats, there are two important defense mechanisms to consider: Rule based approach and Model based approach.

The first is a traditional approach where logs are evaluated against a set of pre-defined rules based on historical data. As any change in the attack type requires re-writing the rules, one might easily see why a rule based approach is becoming obsolete, especially when dealing with large volumes of data.

A model based approach is on the other hand a probabilistic approach where threat models are created for various threat categories. A new event is considered risky if it deviates from the standard baseline. The strength of the model based approach against the rule based approach is that the models are automatically adjusted in case of any change of behavior.

The Power of SIEM and UEBA

The rules- and thresholds-based approach of most SIEM vendors and other existing security tools produces too many false positives and a flood of alerts. When a SIEM solution, enhanced with top-notch security analytics, supports analysts in threat hunting, time spent on eliminating false positives is drastically decreased, empowering your team to focus on threats which really matter. Having SIEM as a data source supported by security analytics not only provides a more valuable than ever pool of log data, but it also enables your SOC team to work smarter, not harder by cutting the detection and response time in half. UEBA 2.0 easily connects to LogPoint through a plugin.

As a result, there is no need to do any mapping or customization which lowers time to value dramatically. The deployment architecture is easily scalable for increasing the number of entities and data volume. Our common taxonomy readily gives access to over 400 machine learning models for all devices. Detected anomalies are used as enrichment sources. Since logs and raw logs can easily be investigated based on the detected anomalies, investigation and forensics can take place immediately.

By leveraging ML and big-data analytics capabilities, built on LogPoint's unique One Taxonomy, UEBA 2.0 builds baselines for every entity in the network and actions are then evaluated against these baselines. By this, it becomes less critical to define the right rules, thus your analysts save time. With UEBA 2.0, suspicious user behavior can be detected in the cloud, on-premise and inside business applications - out of the box.

But the ultimate difference will unfold once you start viewing the information in LogPoint by leveraging the UEBA analytics through alerts and risk scores. Outputs from the UEBA module can be correlated with original and non-UEBA SIEM events, making the original events more insightful than ever. With LogPoint, you can statically or dynamically enrich the original log data using the information from the Machine Learning technology and thus, discover suspicious user behavior in the SIEM.

Wide coverage of use cases

LogPoint Common taxonomy readily gives access to over 400 machine learning models for all devices. Even better, if historical logs are available, baselining can start immediately.

The high-risk activities along with contextual information are then presented to the analyst for further investigation using the LogPoint alerts to enable faster and more informed decisions. Incidents can be visualised using dashboards and search templates for validation. The advanced analytics allows your cybersecurity team to work smarter by accelerating detection and response to threats without increasing the workload of your security analysts

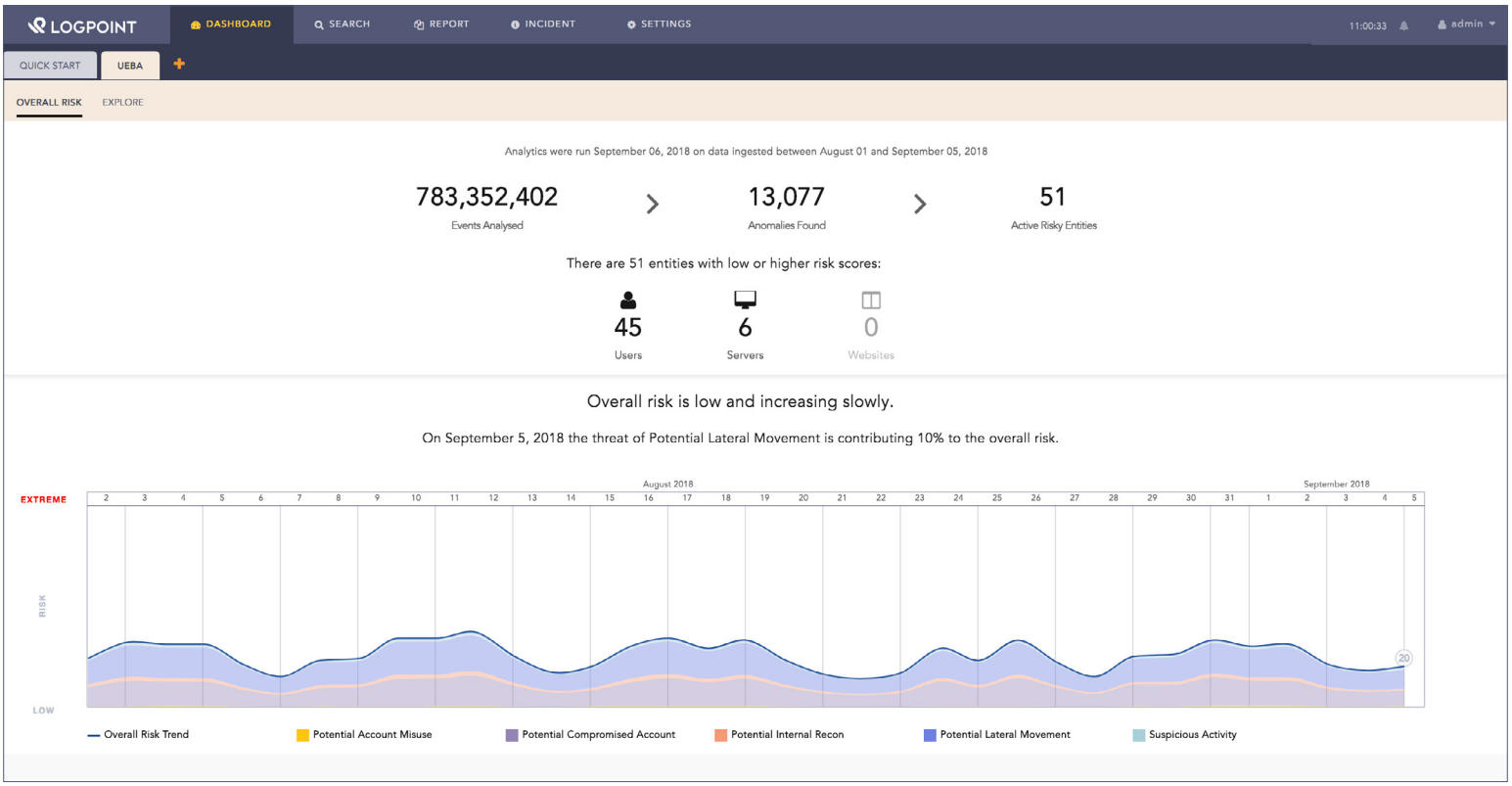
Sounds good, but is my data safe?

UEBA is delivered as a service which means that the identification of anomalies takes place in LogPoint operated and hosted servers.

For your added security, data is encrypted before it leaves your network. The encryption key stays within your network and no clear-text data is ever visible to LogPoint staff.

Any key value pair leaving the network is encrypted and all processing takes place on encrypted values. The system may observe an abnormal access pattern but it will not be able to identify the true identity behind the user.

The observation is sent back to your LogPoint server and decrypted - ultimately revealing the identity to your analysts and no one else.



The Overview page: This gives you on overview of the level of risk your organisation is exposed to. This is a good place to get a general overview of your current risky entities and to start an investigation if any of your users or entities are showing an increased risk score.

Nip insider threats in the bud with UEBA 2.0 – Key user and entity based threat use cases

Account Compromise:
Stop unauthorized account usage by anyone other than the account holder. This way you will never have to worry about your executives getting spearfished by outsiders attempting to infiltrate your organization.

Account misuse:
Monitor how your employees behave in your system and detect any unauthorized account usage by an account holder.

Internal reconnaissance:
Gather evidence on your network resource to be alerted if any of them are behaving differently than expected.

Infected host:
Stop attackers from gaining information about targeted computers or networks that can be used as a preliminary step toward a further attack seeking to exploit the target system.

Lateral Movement:
Restrict unauthorized movement within your environment. With UEBA 2.0 common lateral movement methods can be easily detected.

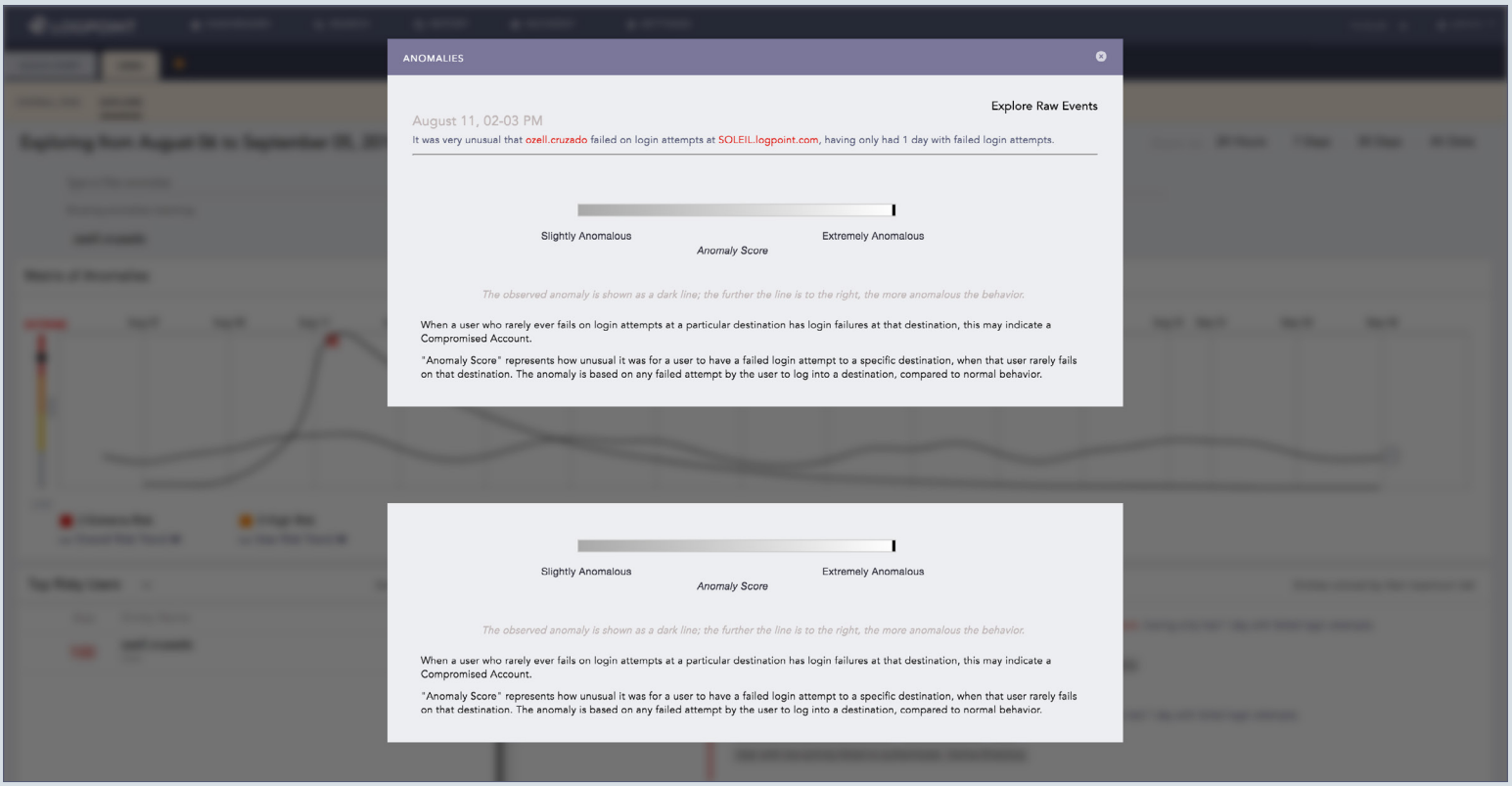
Insider fraud:
Prevent professional attackers, insiders, or customers from illegally acquiring assets such as money for personal use or profit.

Data staging/ Data exfiltration:
Get real-time alerts about unauthorized data transfers within your network. Whether the transfer is manual or carried out by someone with physical access to a computer or is automated.

Faster implementation

Get up and running faster on a SIEM implementation with UEBA. Without the need to tune and tweak static detection rules, it is faster to setup a LogPoint SIEM instance.

LOGPOINT



Context on unusual user behavior: By further investigation, the UEBA module provides your analyst with detailed context on why the user's behavior is highly unusual based on their individual baseline and peer behavior.

Scenario:

The following example showcases how UEBA 2.0 empowers you to detect insider threats in your organization

After finding out that his contract would be terminated, an infuriated admin in your organization decides to not go down without revenge. To seek revenge on your organization, he decides to create a new user account and logs into one of your cloud storage applications.

Anomaly 1
Account Misuse

Since the application in question is only used by a limited number of users, the system administrator's activity is flagged as suspicious.

Anomaly 2
Authentication / Compromised Account

Having a newly created user attempting to log in to the application with only zero days of prior login attempts indicates that something is not alright.

Anomaly 3
Common / Rare Activity

Having the newly created user working in an unusual hour on a day deviating from normal business behaviour is already an idicator of compromise, considering the fact that the user has zero days of prior activity the UEBA module, once again increases the user's risk score.

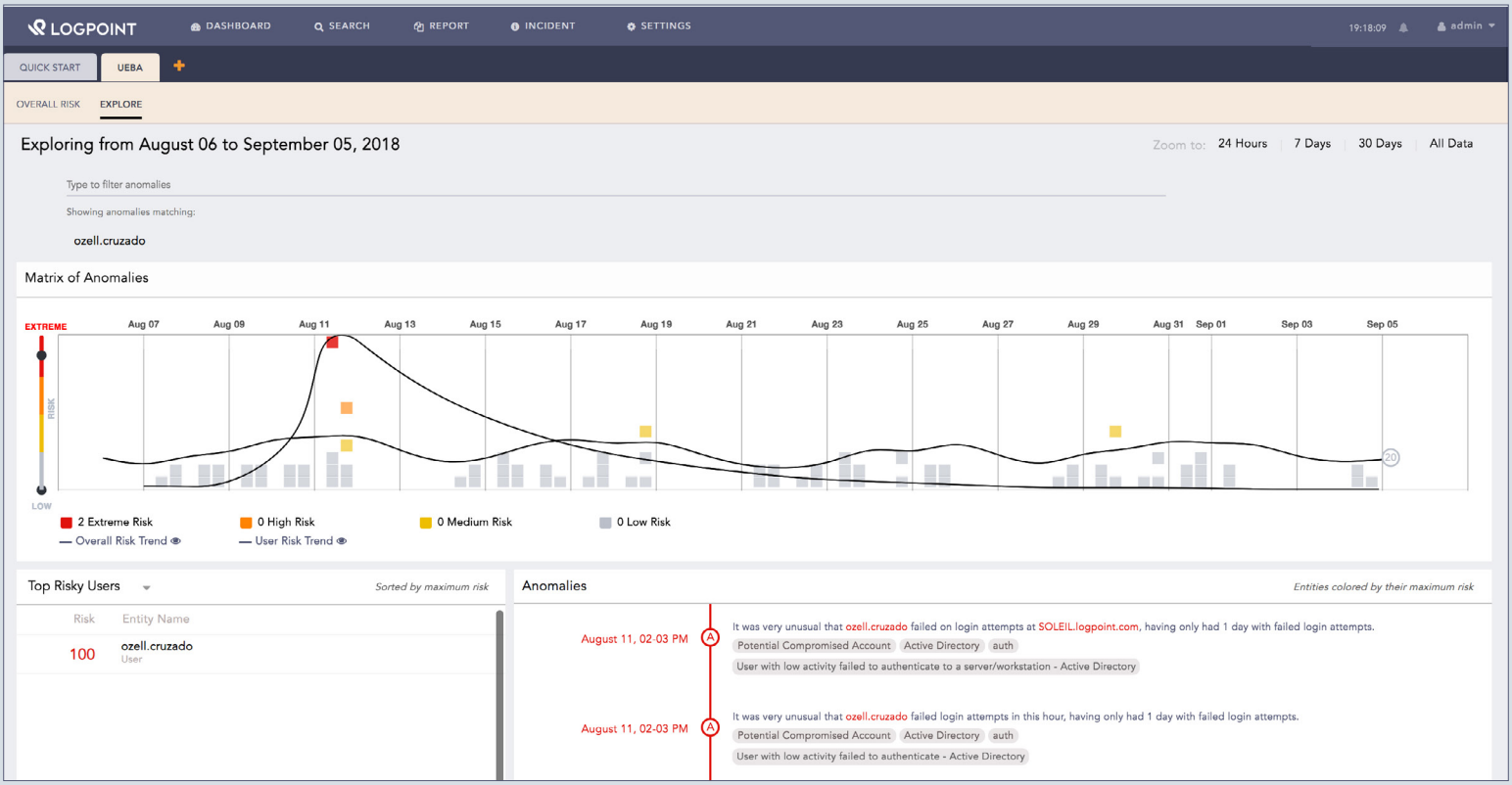
Anomaly 4

As times goes by, the malicious employee keeps using this secondary account to access sensitive information and use it to support his personal vendetta.

UEBA Platform as a Service

LogPoint UEBA 2.0 is uniquely available as a service, thus removing unnecessary hassles for hardware and deployment.

LOGPOINT



Risk behavior timeline: With LogPoint, you can easily filter out the events causing the increased risk score, along with the number of events arranged into a transparent timeline of risky behavior.

Repository / Account Misuse

The UEBA module instantly detects that the newly created user accessed information in the space R&D and copied 17 files one-by-one to different newly created folders within a few hours. Knowing that these actions differ a great deal from the normal business behavior in your organization, the UEBA further elevates the user's risk score.

Finally, your employees last day comes and he decides to go „all-in" by importing the sensitive information collected over the past weeks to his workstation.

Anomaly 5
HR System / Violation

By this action, the user triggered an extreme violation of his user privileges.

Anomaly 6
Repository / Data Staging

Besides violating HR policies, by copying more information than usual in a shorter than usual period of time just to export it to a workstation, the UEBA also classifies his actions as potential data staging.

Not suspecting that his risk scores are already skyrocketing, the user goes on and copies the data to an application server, devides it into several smaller zip files and uploads them to the cloud.

Anomaly 7
Endpoint / Data Staging

Compressing 45 GB of data within 1 hour to several small zip files was flagged as highly unusual behavior by the UEBA module therefore the system identified it as potential data staging and insider threat.

Strengthen your security posture

The use of user behavior monitoring is accelerating; 94% of organizations deploy some method of monitoring and 93% monitor access to sensitive data.

LOGPOINT

Summary

If malicious employees would attempt to jeopardize the integrity of your organization in a similar manner, LogPoint UEBA would help you detect and catch the insider attack in the very first stages so that you can take counter measures immediately. Investigation can start as soon as UEBA detects the Potential Account Misuse.

To combat the risk, your analysts can quickly start incident response by deactivating the user, and alerting HR. You can similarly analyze the potential threats in every stage of the attack and perform defensive actions based on what the situation requires.

Conclusion

With LogPoint UEBA, you can easily detect both suspicious user behavior as well as other entities such as cloud, mobile or on-premise applications, endpoints, networks and external threats – out of the box.

LogPoint UEBA analytics' high fidelity threat scoring can reduce the time to respond to attacks, placing the advantage of time back into your hands. By taking advantage of advanced Machine Learning we enable your security teams to identify unusual patterns and act before the infrastructure is compromised.

Unlike any other UEBA solution, the LogPoint UEBA module will work instantly across all data sources in your network. There is no need for time-consuming and expensive integrations, and our UEBA module will provide unparalleled time-to-value for your business, along with vastly cutting the investigation time by your security team.

Leveraging LogPoint's user centric approach, with licensing on LogPoint UEBA, you can pick and choose the most important users and entities in your organization, so you only monitor where it really matters.

- **Automated Threat Detection:** Utilizing machine learning and behavioral analytics can counter the shortage of experienced Cyber Security analysts and optimize the use of your existing resources.
- **Reduce Risk:** Compromised user accounts are the keys to the kingdom resulting in the most damage from any breach, early detection of a compromised user and/or credentials is essential in mitigating risk and data loss.
- **Reduced Mean Time To Respond:** LogPoint UEBA analytics high fidelity threat scoring can reduce the mean time to respond to attacks, placing the advantage of time back into your hands.

About LogPoint

LogPoint enables organizations to convert data into actionable intelligence, improving their cybersecurity posture and creating immediate business value. Our advanced next-gen SIEM, UEBA and Automation and Incident Response solutions, simple licensing model, and market-leading support organization empower our customers to build, manage and effectively transform their businesses. We provide cybersecurity automation and analytics that create contextual awareness to support security, compliance, operations, and business decisions. Our offices are located throughout Europe and in North America. Our passionate employees throughout the world are achieving outstanding results through consistent customer value-creation and process excellence. With more than 50 certified partners, we are committed to ensuring our deployments exceed expectations.

If you have any questions or want to learn more about LogPoint and our next gen SIEM solution, do not hesitate to contact us.
Email: sales@logpoint.com