Blindspotter

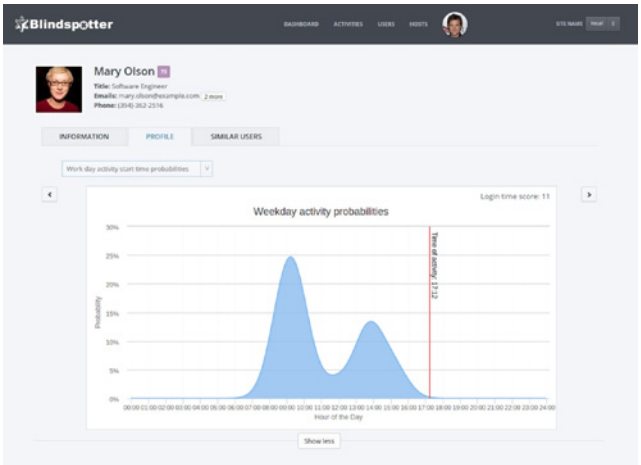
THE REAL-TIME USER BEHAVIOR ANALYTICS SOLUTION

Blindspotter is a user activity monitoring tool that collects information in various IT systems to detect security problems by identifying unusual behavior.

Blindspotter is designed to help IT organizations' security teams.

Traditional IT security products and techniques utilize some form of pattern-based technology to prevent, detect, and stop attacks. These tools, whether preventive security products like anti-virus software or monitoring solutions like IDS and SIEM solutions, provide some form of built-in knowledge of attack vectors, sometimes extended with simple heuristics. These patterns either supplied by the vendor or created by the IT security team. However, in both cases the products can only detect events or attacks that they recognize. While heuristics can extend the capabilities of these security tools to detect polymorphic viruses or previously unseen attacks using similar patterns, it cannot address previously unknown attack techniques as it is not feasible or simply not possible to create heuristics, or "universal" patterns, for such cases.

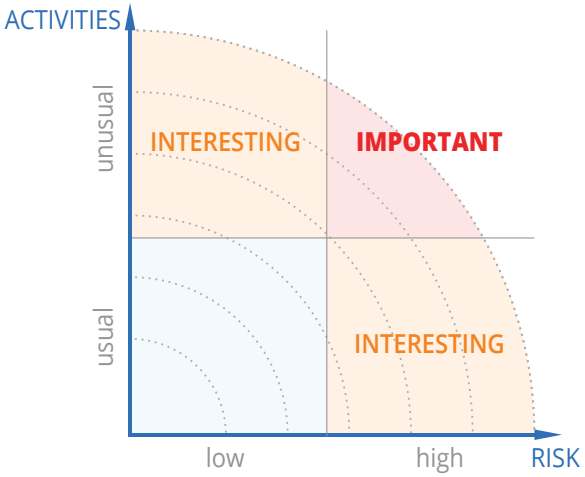
By utilizing different machine learning algorithms, Blindspotter detects unusual behavior, anomalies which have been previously unknown. Machine learning algorithms work autonomously and learn about user behavior. This way they can cover the blind spots of legacy technologies and not just identify anomalies, but also provide intelligence and reasoning why a spotted activity is considered an anomaly.



Blindspotter collects user related events and user session activity in real-time or near real-time, it then compares each and every action to the corresponding baseline of users and their peers to spot anomalies in their behavior. Malicious user activity can appear completely normal when investigated from a certain point of view. Detecting the anomaly might require a particular point of view. By utilizing multiple algorithms, Blindspotter can view actions from many different perspectives and detect otherwise hidden anomalies.

Once an unusual activity or anomaly is detected, Blindspotter can automatically react. Automatic reaction is important to provide both a real-time response and to automate and support the investigation process. Automated responses can also significantly reduce the time a malicious attacker has before any counter measure is taken. In most attack scenarios, the high-impact event is preceded by a reconnaissance phase. Detection and response during this phase is critical to preventing any further high-impact activity. Unusual activity can be confirmed with users: the account owner is notified about the suspicious activity. This method could be used to increase the speed and accuracy of detecting identity theft.

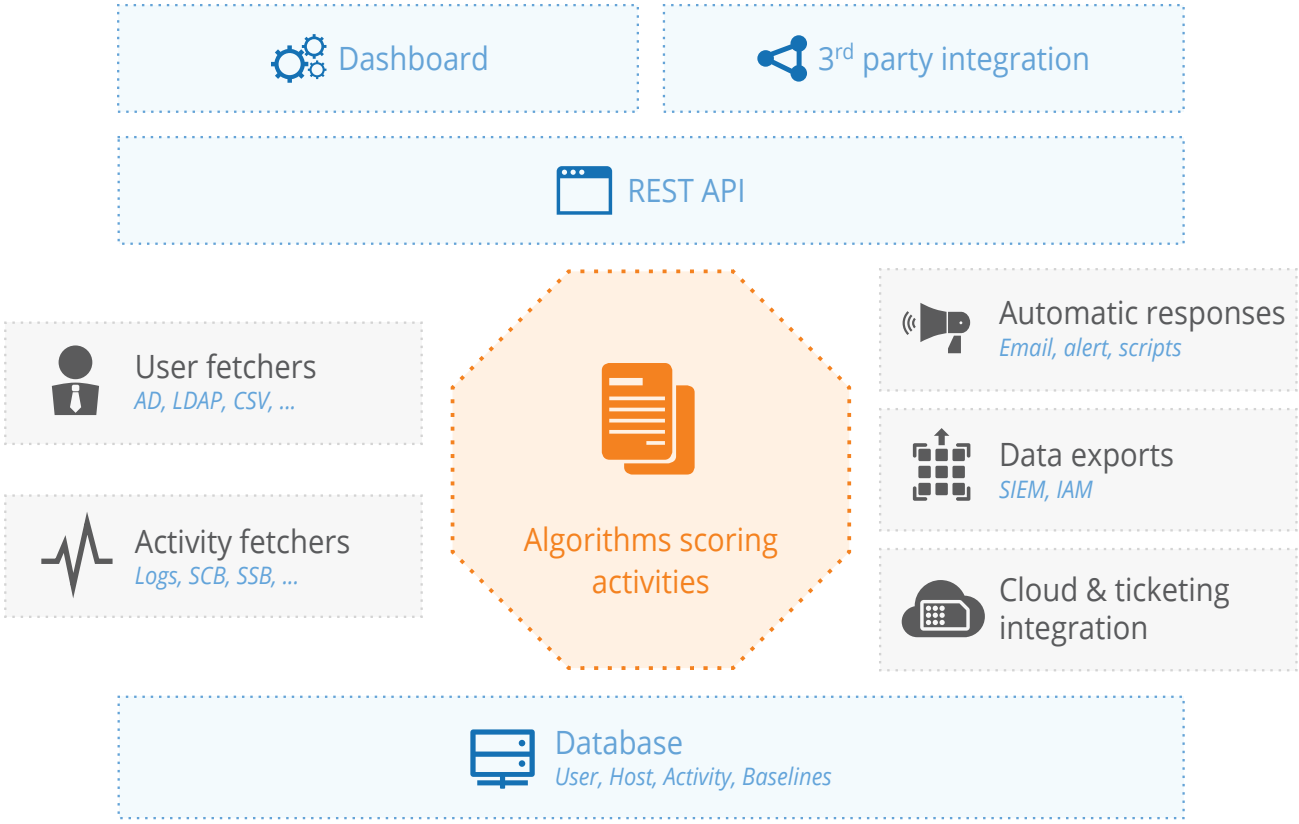
To gain a better understanding on what is going on in the IT system and to help focus security team's attention on important information, Blindspotter provides a prioritized list of activities ranking the most interesting/risky activity at the top. This way, security personnel can spend their time on investigating the real important events instead of being overloaded with notifications and alarms.



This unusual activity by risky users is the most important. Of course, unusual activity of lower risk users may be worth investigating but only after higher risk activity. Likewise, being aware of less unusual activity of high risk users is also valuable. This "risk-aware" scoring yields a unified importance score for each activity, providing a comparison of all activity on a large-scale.

What should I know?

To build a successful security architecture, both known attacks and yet unknown attack vectors must be taken into consideration. In many cases, the real challenge is to identify what we want to monitor, what alerts we want to setup, "teaching" the system about attacks that we want to detect. The problem is really "asking the proper questions", rather "providing answers" without overloading the security team with useless answers or alerts. Blindspotter helps by "answering" a higher level question: "Show me what I should know about my IT system?" This enables security team to focus on previously overlooked events. Information gained from investigating these events can also be incorporated into the existing security architecture to leverage their capabilities by "asking better questions".



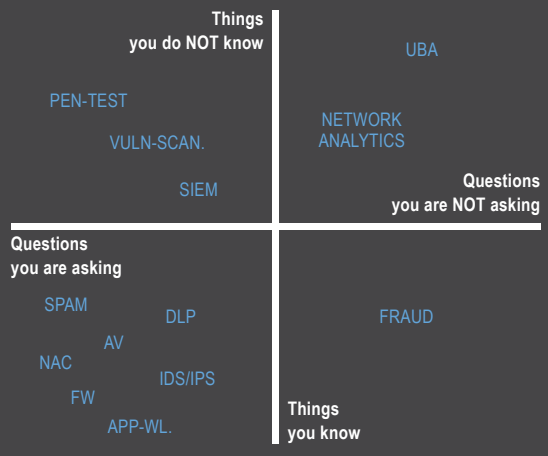
Architecture of Blindspotter

Blindspotter consists of multiple, loosely coupled components that provide high flexibility during deployment. Data connectors, algorithms, databases and the front-end can be separated to scale to large deployments with high data-volume and numbers of users. It can be installed on a single server or scaled horizontally as the load grows.

Integrating custom applications is straightforward by modifying or adding a new add-on to fetch events and ingest into Blindspotter. Blindspotter provides an extensive API to ease the development of new add-ons.

Humans, by their very nature, have distinctive behavioral characteristics that can be identified by algorithms and analytics. User profiles or baselines are built using historical data. Blindspotter learns about user behavior by analyzing past activity.

0-knowledge threats



In data science, there is a very important distinction between the things we do not know ("unknowns") and the things we cannot even ask questions about ("unknown unknowns"), as we do not even know what it is that we are looking for. In IT security, there are threats in both of these categories. Most products deal with the first group by looking for known attacks in the system. The real problem, however, is the case where the attacks are previously unknown, commonly referred to as 0-day or 0-hour attacks. We need some way of handling the "unknown unknowns" of IT security, which are the main challenges of today and tomorrow.

Anatomy of an APT attack

1

Credentials of DB operator is stolen

Most APT-style attacks start by compromising the machine of someone within the enterprise through phishing, "watering hole" attacks or other means. Gaining control of an endpoint device means gaining access to most credentials of its user as well: fetching stored passwords or logging keystrokes are just two of the endless possibilities. From this point on the attacker can act on behalf of this insider and start exploring the system to find the data he is after.

2

Multiple access to database servers

The attacker, using the stolen credentials, accesses multiple database servers to map out the IT system and its assets. The successful logins are recorded and logs are collected by the syslog-ng Store Box and also forwarded to the SIEM. However, as the logins are successful there are not alerts triggered by the SIEM.

Algorithm *principal component classifier*

Algorithm *logintime* → Normal working hours

Algorithm *hostlogin* → Usual servers

Algorithm *activity count*

Algorithm *stochastic outlier selection*

Algorithm *frequent item set*

3

Too many connections

Blindspotter fetches logs in real-time from the syslog-ng Store Box and analyzes the sessions. Multiple algorithms are used, however neither the "logintime" nor the "hostlogin" algorithms detect any unusual activity as both the time of the login and the accessed database servers are considered normal according to the victim account's profile. Nevertheless, the frequency and the number of parallel connections analysis indicate suspicious activity.

4

Dynamically increase User risk

Blindspotter does not rank this as high-priority but it does dynamically raise the risk level associated with this user. This higher risk level triggers session recording to be activated on the Shell Control Box including command level analysis.

5

Access database, try to steal data

At this point, the attacker dives deeper into the database servers and starts to steal data. However, this time, all executed commands are recorded and logged in Shell Control Box. Blindspotter also fetches command execution events and analyzes them in real-time.

Algorithm *Screen Content Analysis*

6

Unusual command for database admin

The analysis reveals that the executed commands are unusual for database operators and administrators. This automatically triggers another dynamic risk level increase.

7

Notification of the user and/or the security team about the suspicious activities

The victim doesn't confirm that the suspicious activities were implemented by her which indicates an identity theft has occurred.

Disable account

Run further investigation

9

The attacker was neutralized

As the victim didn't confirm the attacker's activities, the security team disabled the account with the stolen credentials so the attacker was stopped before accessing or exfiltrating any data.

8

The security team has all the relevant information (logs from the syslog-ng Store Box and audit-trails from the Shell Control Box) in Blindspotter to quickly investigate the attack and make any further counter measures. The early detection by Blindspotter was able to prevent the attacker from stealing the organization's data.

Blindspotter facilitates the investigation process by showing the context: it shows the behavioral profile of the user and highlights why and how does the current situation differ from what is usual. It allows the investigator to quickly overview the users' activities and compare them to the actions of her peers.

Comparison of Blindspotter and SIEM solutions