BLINDSPOTTER

REAL-TIME USER BEHAVIOR ANALYTICS TO IDENTIFY INTERNAL AND EXTERNAL ATTACKERS

"The new perimeter is our users"

Many companies' worst nightmare – a sophisticated external attacker or malicious insider – is already within its perimeter. Nowadays, attackers are intelligent, well-funded, and their attacks are increasingly complex and well targeted. The most recent, high-profile breaches were carefully planned and went undetected for some time, with the attackers moving freely inside the victim's IT environment. Malicious insiders hold an advantage over a company's primary security tools, because these tools are designed to protect against external threats, not against trusted employees. Targeted attacks by humans use a combination of IT vulnerabilities, social engineering, and ordinary crime to gain unauthorized access. It means that the new perimeter – and the area that needs renewed focus – is your users, not your infrastructure. Blindspotter represents the new generation of IT security solution, concentrating on privileged user behavior.

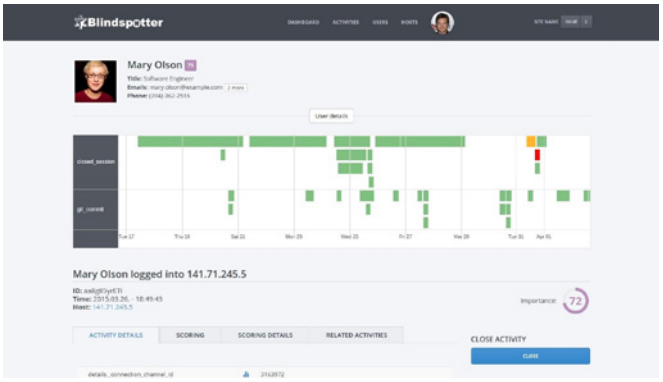
"More monitoring less control"

Blindspotter represents the new generation of IT security solution, concentrating on privileged user behavior and revealing suspicious activity. It has been developed by Balabit, an IT security vendor specializing in log management and advanced monitoring technologies.

By detecting deviations from normal behavior and assigning a risk value, Blindspotter helps companies focus their security resources on important events, and also allows them to replace some controls, yielding greater business efficiency. Adding more tools that restrict users does not make your company safer; rather it makes your employees less productive.

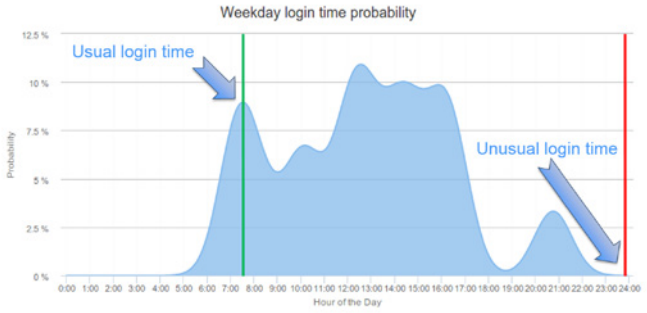
Blindspotter integrates a variety of contextual information in addition to standard log data, processes it using unique sets of algorithms, and generates user behavior profiles that are continually adjusted using machine learning. It tracks and visualizes user activity in real-time for a better understanding of what is really happening inside the IT system, and offers a wide range of outputs from a priority dashboard to automatic interventions. It does not require predefined correlation rules; it simply works with your existing data. The built-in algorithms have customizable parameters that allow you to fine-tune the output without being a skilled data scientist.

Blindspotter is the only User Behavior Analytics solution capable of analyzing not only metadata such as where and when a user accesses certain systems, but biometric information such as their typing characteristics or mouse movements. Typical keyboard analysis includes typing speed, elapsed time between typical keystroke sequences or typical typos. Although users maybe executing the same task, each has their own idiosyncratic pattern of behavior – for example, the acceleration of the mouse cursor, the curvature of the span, or simply the number of individual movements. Blindspotter's biometric analysis features are not only able to identify identity breaches, but work as an additional layer of biometric authentication, enabling security analysts to continuously authenticate whether the user is who he says he is.



Data is analyzed in multiple ways to adjust the risk and deviation level of each activity. Blindspotter reveals all new deviations from normal operation in a well-prioritized dashboard. With advanced monitoring across every aspect of an IT system, Blindspotter prevents sensitive and critical data from potential security breaches, from both internal and external attackers.

Blindspotter is a part of Balabit's Contextual Security Intelligence Platform, and as such is tightly integrated with the company's log management tool, syslog-ng, and Privileged Activity Monitoring tool, Shell Control Box. Blindspotter maximizes the benefit of log data using syslog-ng, and builds a unique profile of individual users based on data received from Shell Control Box, which records the details of remote-access user activities like a CCTV camera. With these two world-class monitoring tools, Blindspotter gives you a deeper understanding of your users than any other solution. Balabit delivers an extremely comprehensive security analytics portfolio which gives you peace of mind about your IT environment.



KEY BENEFITS

- Decrease the likelihood and impact of breaches by identifying suspicious activities and detecting unknown threats coming from both inside and outside the organization
- Increase the efficiency of security teams
- Enhance the flexibility of business while improve security
- Exploit the real value of compliance investments

USE CASES

Detect hijacked accounts

Lowers the impact of potential breaches and provides an effective defense against APTs. Attackers, who are stealing valid user credentials behave differently from real users. Blindspotter is able to detect the level of deviation from normal user activity. If the deviation is high, it sends an alert to the Security Operation Center for further investigation.

Detect misuse of privileges

Significantly decreases the chance of misusing privileges. Malicious insiders also behave differently from normal employees. If a disaffected employee wants to steal company data, Blindspotter is able to detect this anomalous activity and will alert the security team for further investigation.

Improve investigation efficiency by providing contextual information about users

Security analysts need to act really fast. Blindspotter collects, sorts and reports on information specific to the privileged user context, allowing analysts to quickly identify the first signs of an attack. They need as much relevant information about their users as possible, so as to quickly determine if an event is the first sign of an external attack or a business as usual event for that user.

Detect system accounts used by humans and personal accounts used by scripts

System accounts used by humans, shared accounts and personal accounts used by scripts are typical red flags and are potential security risks. If an attacker finds a way to gain access to the stored credentials the script is using, he can gain access to all the services the script had access to. Security analysts are able to detect improper account usage with the help of Blindspotter, can take action before a security hole turns into a data breach.

Reveal the gap between policies and the real-life usage of the IT-system

In large organizations the phenomenon known as "privilege creep" is a big issue: the people, especially IT staff and managers, get more and more privileges to be able to perform new tasks over the time. Blindspotter gives an overview of how different services are used within the company, and what kind of privileges individual users should have.

Balabit's Contextual Security Intelligence™ platform protects organizations in real-time from threats posed by the misuse of high risk and privileged accounts. Solutions include reliable system and application Log Management with context-enriched data ingestion, Privileged User Monitoring and User Behavior Analytics. Together they can identify unusual user activities and provide deep visibility into potential threats. Working in conjunction with existing control-based strategies Balabit enables a flexible and people-centric approach to improve security without adding additional barriers to business practices.

Visit our website now: https://www.balabit.com/blindspotter

Schedule a call with our team of experts and gain a first impression about Blindspotter.