Infopercept

User Behavior Analytics Importance in Cyber Security

Infopercept

Definition

- User behavior analytics (UBA) is tracking, collecting and assessing of user data and activities using monitoring systems.

- It is a category of cybersecurity tools that analyze user behavior on networks and other systems, and apply advanced analytics to detect anomalies and malicious behavior. These can be used to discover security threats like malicious insiders and privileged account compromise, which traditional security tools cannot see.

Infopercept

Abstract

Focus on User Behavior Analytics (UBA) modules that track and monitor behaviors of users, IP addresses and devices in an enterprise. Anomalous behavior is automatically detected using machine learning algorithms. Such anomalous behavior indicative of potentially malicious activity is alerted to analysts with relevant
contextual information for further investigation and action.

Infopercept

What Does a UBA System Comprise?

- Data collection, parsing and aggregating of security events, via log data or agents installed on IT systems.
- Central storage where raw data, metadata, and the results of analyses are stored.
- An analysis engine that analyzes events, identifies anomalies, and prioritizes them to pinpoint security incidents.
- Automated response some UBA solutions can integrate with other security tools or IT systems and perform automated actions in response to a security incident.

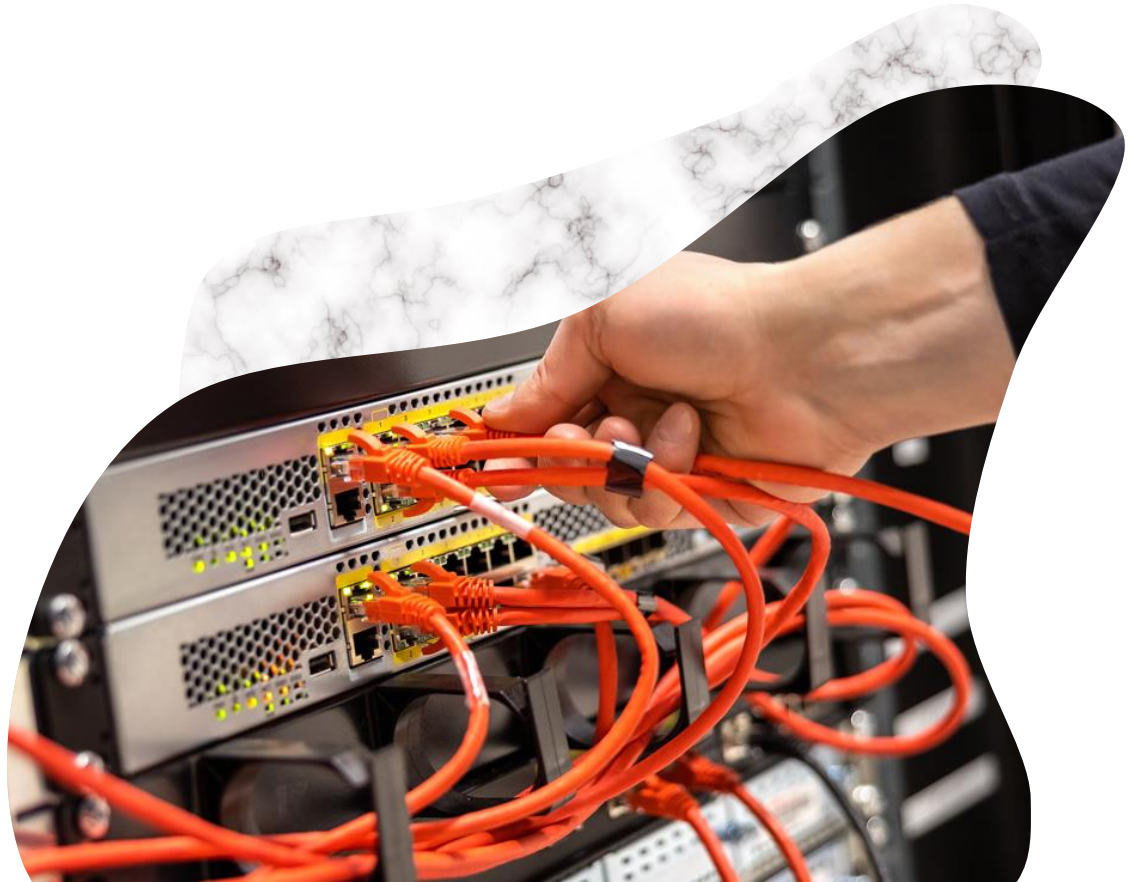
Infopercept

Three Pillars of UBA

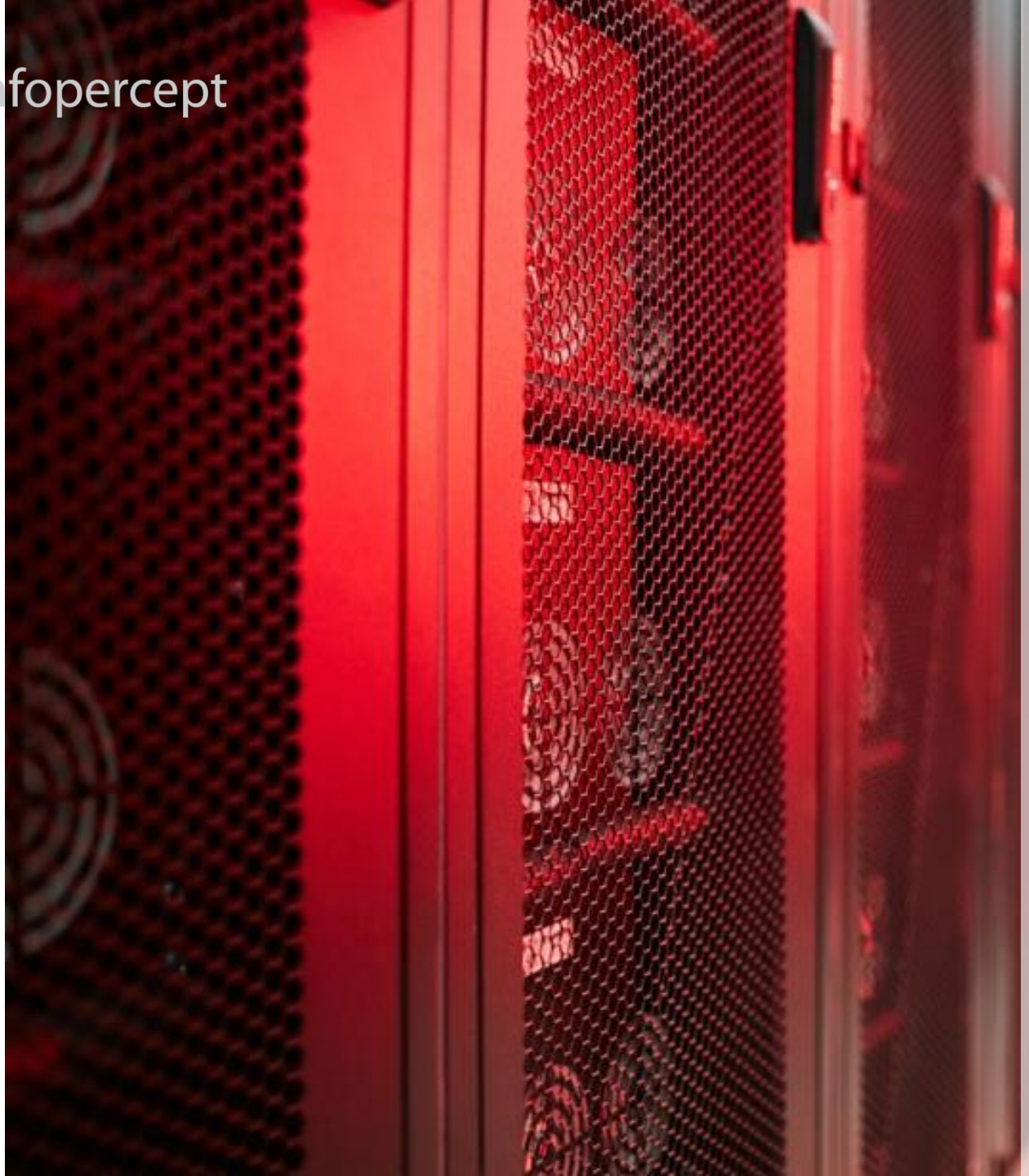
1. **Use cases** - UBA solutions provide information on the behavior of users and other entities in the corporate network. They perform monitoring, detection and alerting of anomalies and are applicable for multiple use cases.

2. **Data sources** - UBA solutions are able to ingest data from a general data repository such as a data lake through SIEM.

3. **Analytics** - UBA solutions detect anomalies using a variety of analytics approaches like statistical models, machine learning.



Infopercept



UBA Security Use Cases

1. **Discovering compromised accounts**- UBA can identify user accounts taken over by attackers, because they exhibit anomalous behavior compared to the real business user.

2. **Identifying malicious insider threats**- Insider threats are a major, growing threat, and are extremely difficult to detect via traditional security tools. UBA tools can identify malicious insiders by analyzing their behavior compared to similar, non-malicious users.

3. **Identifying privileged account abuse** UBA can help monitor
accounts with administrative or escalated privileges, to ensure they are not being misused, either by their designated owner or by others.

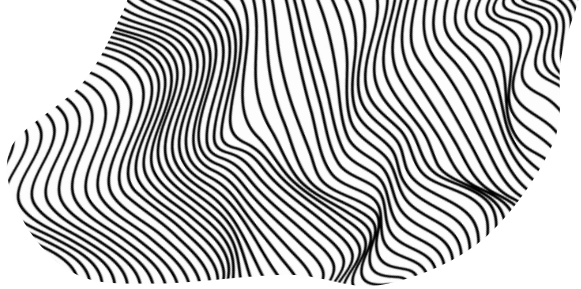
Infopercept

4. **Cloud security monitoring**- Cloud assets are provisioned dynamically and used remotely, making them difficult to capture with traditional tools. UBA can look at cloud-based assets and discover if they are acting normally or abnormally.

5. **Entity monitoring**- UBA can be used to monitor Iot devices, such as critical medical equipment or sensors deployed in the field.

Infopercept

UBA Analytics Methods



1. **Supervised machine learning**- It is sets of known good behavior and known bad behavior that are fed into the system.

2. **Bayesian networks**- It can combine supervised machine learning and rules to create behavioral profiles.

3. **Unsupervised learning** - The system learns normal behavior, and is able to detect and alert on abnormal behavior.

4. **Reinforced / semi-supervised machine learning**- A hybrid model where the basis is unsupervised learning and actual alert resolutions are fed back into the system to allow fine tuning of the model and reduce the signal-to-noise ratio.

4. **Deep learning -** The system trains on data sets representing security alerts and their triage outcomes, performs self-identification of features and is able to predict triage outcomes for new sets of security alerts.

Infopercept

Working

- The true power of a UBA solution is in its ability to cut across organizational boundaries, IT systems and data sources and analyze all the data available for a specific user or entity.

- A UBA analyze data sources, example -

1. Firewall, Intrusion Detection and Prevention Systems (IDPS)

2. Anti-malware and antivirus systems

3. Endpoint Detection and Response systems

4. Network Traffic Analytics

Infopercept

Focusing on Insider Threats

01

The flow of insider threats consists of five steps: reconnaissance, circumvention, aggregation, obfuscation, and exfiltration.

02

The first thing an infiltrator who penetrates a system does is to start looking. What files can I access? What kind of security systems are in place? This is the reconnaissance phase.

03

The second step is "circumvention" in which the infiltrator attempts to circumvent the installed security tools.

04

The third step is "aggregation" in which the attacker aims to gather data in one location.

05

In the fourth step, "obfuscation" the infiltrator hides the traces of his/her behavior.

06

The fifth and final step is "exfiltration" If we examine each of these steps and study the behaviors, we can detect abnormal behaviors and stop such behaviors before attackers leave with data.

Infopercept

The Idea of "Trust But Verify"

- The primary approach to cyber security for the last 10 years has been to "lock everything down."
- When we hire somebody, we should trust them. When we employ them, we put them through a vetting process, carry out due diligence, and study how they performed in their former jobs.
- When we stop users from doing things that they should be able to do to do their jobs, they always find another way around these measures.

If we trust our employees, we should give them broad access without restrictions so that they can do their jobs well because they need to use a variety of means to be quick and innovative, but at the same time, we must verify what they do.

It is important to verify the content of users work, create a mechanism to detect and stop bad behavior and when an employee makes a mistake, teach them how not to do it again.

Infopercept

Key Capabilities

1. **Monitor and analyze behavior -** It has the ability to collect data from IT systems and create a behavioral baseline of entities on the network.

2. **Detect anomalous behavior -** A deviation from the behavioral baseline that is significant and could indicate an insider attack or other security threat.

3. **Leverages machine learning and advanced analytics -** It makes it possible to detect unknown threats and learn from big data sets, even if an attack has never been seen before.

4. **Combines multiple activities into one security incident** - It is able to identify security incidents across multiple users, entities or IPs, and also combine data from many different sources, such as anti-malware, firewall, proxies, and VPN..

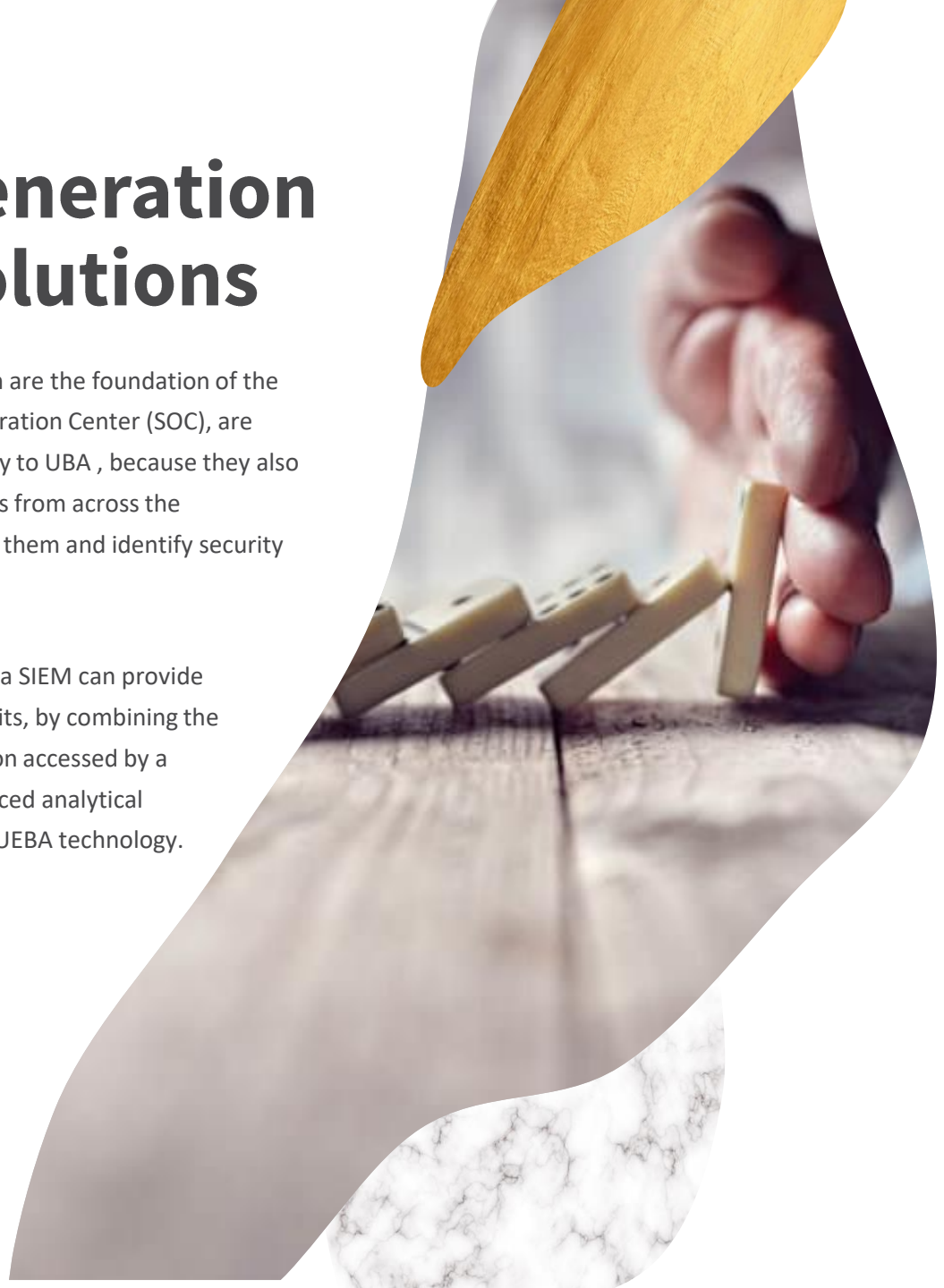
5. **Near-real time performance-** To be effective as an incident response tool, UBA technology collects data and alert security analysts very soon after an event has occurred.

Infopercept

Next-Generation SIEM Solutions

- SIEM solutions, which are the foundation of the modern Security Operation Center (SOC), are highly complementary to UBA , because they also collect security events from across the organization, analyze them and identify security incident.

- Incorporating UBA in a SIEM can provide strong security benefits, by combining the breadth of information accessed by a SIEM, with the advanced analytical capabilities of UBA / UEBA technology.



EXAMPLE

1. Exam beam's Security Management Platform Exam beam Capabilities
2. Rule and signature-free incident detection.
3. Automatic timelines for security incidents..
4. Dynamic peer groupings.
5. Lateral movement detection

THANK YOU

For More Information Please Visit our Website

www.infopercept.com