TATA CONSULTANCY SERVICES

Sharpening Threat Detection with User and Entity Behavior Analytics

Abstract

With the adoption of digitization and cloud, cyber security has become a critical item on the CXO agenda, particularly threats from 'insiders'. A recent survey found that 53% organizations are concerned about detecting insider attacks given the financial, reputational, and legal damage they cause. Moreover, cyberattacks are becoming increasingly sophisticated and target vulnerabilities in software or hardware, for which no security patches are available. About 80% of cyberattacks stem from unknown sources.

In such a scenario, cyber defense processes using user and entity behavior analytics (UEBA) become not just good-to-have, but a must-have for large organizations. UEBA uses machine learning and algorithms to track anomalies in user behavior to detect threats from compromised users and malicious insiders.

For a successful UEBA-powered cyber defense, it is critical to focus on covering all data sources, setting the business context, identifying use cases, defining the range of 'usual behavior' and continuous monitoring.

The unknown threat

Cyberattacks are increasingly becoming more complex to detect. Previously, organizations looked for anomalies against a background of 'normal' traffic, which was like finding a needle in the haystack. Today, attackers are generating additional traffic to mask their behavior. Traditional rules and signature-based cyber defense tools that scan for patterns or footprints associated with threats were not designed to detect such sophisticated and advanced behavior.

Organizations face numerous attacks ranging from drive-by download of malware to targeted attacks that use more advanced and sophisticated techniques. Modern threats can be classified into three major categories (see Figure 1).

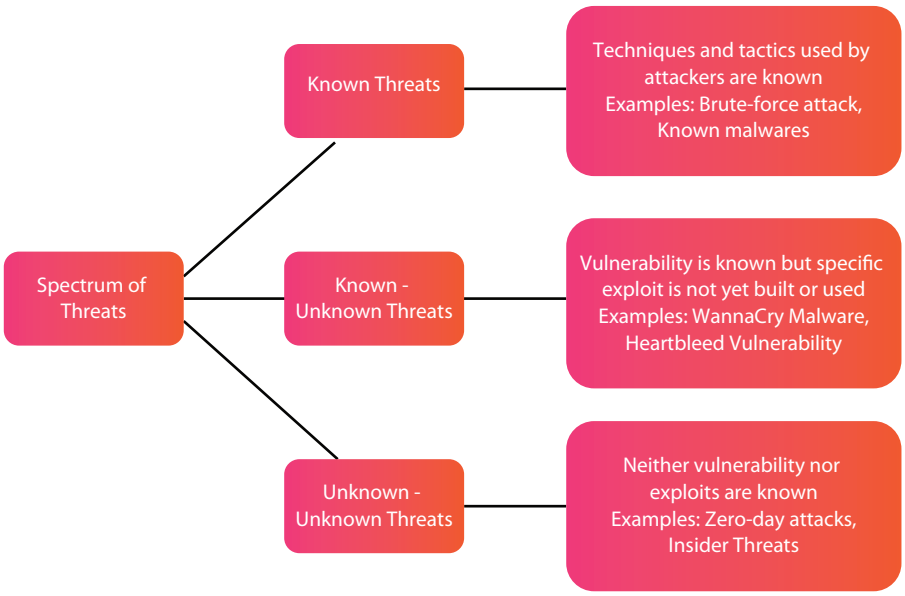


Figure 1: Decoding the spectrum of cyber threats

About 20% of total threats fall under the first two categories of known threats, while 80% are unknown. Recent reports reveal that 30% of unknown breaches involved internal threat factors and 37% of breaches involved stolen or used credentials. Most of the existing technologies solve the problem of known and known-unknown threats. Detecting unknown-unknown threats, however, requires advanced analytical technology.

As per the 2020 Insider Threat Report :

- 68% of organizations feel vulnerable to insider attacks.
- 53% believe detecting insider attacks has become harder after adopting cloud applications.
- 63% of organizations believe that privileged IT users pose the biggest insider security risk.
- Lack of resources (31%) and too many false positive alerts (22%) are the biggest hurdles in maximizing the value of security information and event management (SIEM) processes.
- Only about one-third of organizations can detect anomalous behavior in net flow or packet data (35%), service accounts (39%) and cloud resources (30%).

While the true cost of a major security incident is not easy to determine, the most common estimate is less than $100,000 per successful insider attack (50%). Thirty-four percent expect damages between $100,000 to $500,000.[1] According to the Fortinet Insider Threat report, 2019[2], "Insider threats heavily impact organizations with 61% of organizations facing operational disruptions as a result, 43% facing brand image damage and another 43% suffering from loss of critical data".

Tracking user behavior

Considering the ever-growing volume of threats, writing correlation rules for thousands of possible scenarios is no longer practical. Modern day cyber defense requires specialized tools such as UEBA that leverage ML to detect anomalies. Organizations are increasingly adopting UEBA tools across the threat detection landscape to counter advanced threats.

UEBA offers significant advantages in discovering unknown threats. It baselines user and entity behavior (such as devices, applications, servers, data, storage, file systems or anything with an IP address) and combines these with peer group analysis to search for anomalous activity to detect unknown threats. UEBA solutions uses artificial intelligence (AI), ML, advanced analytics, data enrichment and data science to effectively detect insider and advanced threats.

While several tools are available that claim to profile normal versus out-of-the-ordinary behavior, the devil is in the approach. These not only need to be tailored to the organization's needs, but also leverage the

experience of the defense strategies that have worked well, or not, in the past. Therefore, UEBA tools need to be implemented in sync with the current monitoring and detection tools to provide multi-layer defense for enterprises.

To realize the full potential of UEBA solutions, organizations need to follow these principles:

- Complimenting existing security operations center
- Leveraging data sources including, but not limited to, end-user computing and network data as well as system logs and application data.
- Enriching the insights with contextual data considering both objective as well as subjective information. For instance, correlating user access, activities and privileges with recent employee satisfaction survey responses.
- Enterprise-wide implementation for monitoring and correlation of data, activity, and events.
- Adopting risk score-based investigation with immediate 'blocking' actions for high risk and classified cases and investigation for other flagged cases. For instance, immediately blocking access of a high-risk user to a crown jewel application and reinstating it only after the risk has been investigated.
- Using security orchestration and automation along with UEBA to reduce the dwell time.

Five building blocks and AI techniques

The most critical aspect of UEBA implementation is getting the building blocks right. These include:

- **Data sources:** Getting data about access and activities of all types of users – humans and systems – is the first step in UEBA. Information needs to be collected from the perspective of the user as well as of the application. Who accesses what for their job requirements can be sourced from logs, reports, files, database and even packet-level information.
- **Business context:** User context -- in terms of user details, peer groups, privileged access details, critical network segments, critical assets data and threat intelligence -- is important to analyze the user data.

- **Use cases:** For proper analytics, it is important to first define the purpose and the relevant user base.
- **Analytics:** Identifying the range of behavior and response that can be called 'usual behavior' plays a key role in detecting anomalies. This definition should be based not only on users' past behavior, but also on what that role group accesses over a given period.
- **Continuous monitoring:** Monitoring for anomalies is a continuous process and the feedback cycle is the core to designing any solution and ensuring its viability.

To action these UEBA building blocks, cyber security warriors need to use AI-powered arsenal. Machine learning algorithms can be designed to target five behavior areas – behavior analysis, peer group analysis, event rarity analysis, robotic behavior and sequence analysis (see Figure 2).

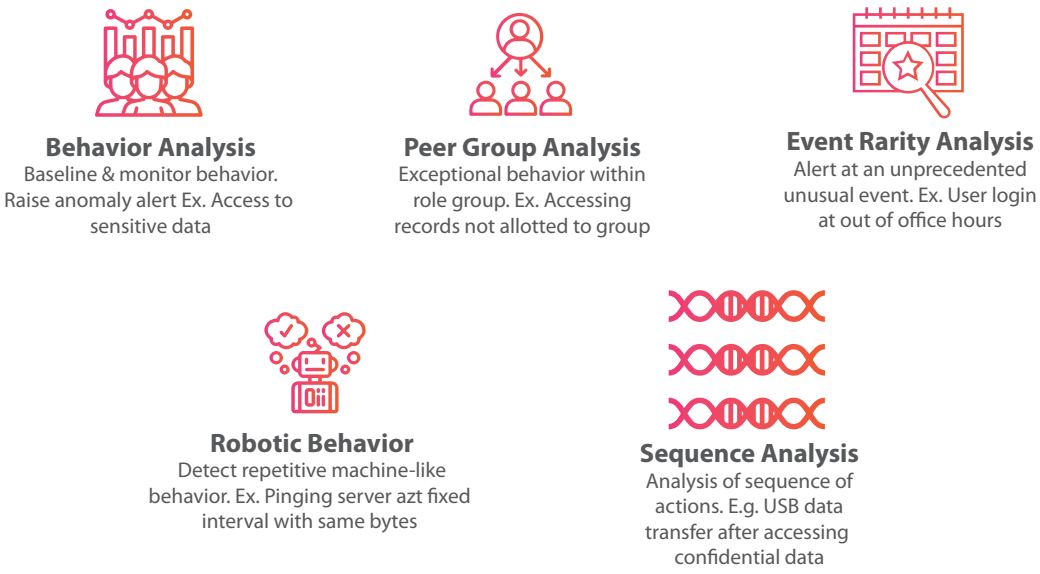


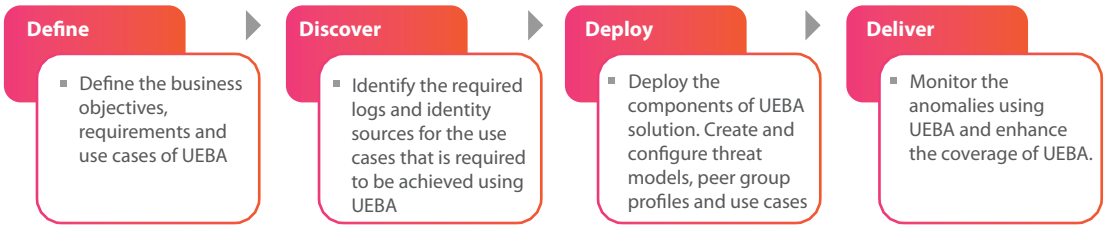
Figure 2: UEBA detection techniques

Going beyond detection

With these AI techniques, organizations can strengthen their defense against unknown cyber threats. Tracking user patterns using machine learning can significantly improve early detection of vulnerabilities and even allow automated corrective actions. UEBA not only provides insider and advanced threat detection, but also extends into the business realm including functions such as fraud management in financial services, customer experience as part of consumer operations, partner value analysis in manufacturing supply chains, sales, and marketing as well as efficient operations across the board. Here are some of these examples adopters of UEBA frequently use as pilot use cases and the indications to be monitored.

UEBA applications	Potential indicators
Account compromise: Identifies where user credentials have been stolen and are being used by an unauthorized user; also detects shared account usage and generic account abuse.	▪ Unusual authentication patterns (e.g., dormant account access) ▪ Concurrent logins from multiple locations ▪ Account activity from unusual locations or time
Malicious insider threat: Identifies network endpoints and users that have been compromised, infected by malware, or are otherwise behaving suspiciously.	▪ Deviation from peer group ▪ New or unusual system access, login time or abnormal password activity ▪ Disabled account login, multiple lockouts and excessive authentication failures. ▪ Unusual file access and modifications
Data exfiltration: Detects unauthorized or malicious data exfiltration by action of authorized users.	▪ Suspicious data transfers or malicious payload drops ▪ Abnormal traffic patterns ▪ Blacklisted communication
Specific sensitivity to particular line of business or transactions: Predicts and detects vulnerabilities and threats based on parameters such as sensitivity of transactions, industry, competition activity, and individual or group sentiment.	▪ Frequently or long period of access to codebase, applications, data related to sensitive transactions ▪ Download of data unrelated to role or function in the organization ▪ Suspicious internet browsing activity ▪ Frequent communications with external parties

Recommendation



To more effectively bolster the enterprise security posture, it is essential to augment the existing cyber defense strategy with UEBA to predict, detect, respond, and defend against advanced and insider threats. UEBA goes beyond uncovering threats to detect vulnerabilities and use them as a source to improve other business critical areas such as customer experience, partner viability, role mining, operational efficiencies, fraud management, sales, and marketing.

In addition to analytics, different streams of automation and AI also play an important role in bolstering the confidence levels in the field of UEBA. A critical aspect is to have a level playing field in terms of what these algorithms recommend, the threshold to which the recommendation is acceptable and what governance measures to use while acting on these recommendations.

References

https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

[1] 2020 Insider Threat Report, Cybersecurity Insiders: https://gurucul.com/2020-insider-threat-survey-report

[2] 20119 Insider Threat Report, Fortinet: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf

About the Authors

Geetali Raj

Geetali Raj heads the delivery for solution center and professional services for IAM as part of the Cyber Security unit at TCS. With over 16 years of experience in the IT industry, she has worked across various roles and streams such as enterprise integration, service oriented architecture (SOA)business process management, automation and AI. She holds a Masters degree in Marketing.

Chintan Savai

Chintan Savai is the lead security consultant within managed detection and response centre of excellence (CoE) team as part of the Cyber Security unit at TCS. With over eight years of experience in security operation center, endpoint security, data protection and data leakage prevention, he is experienced in designing and implementing various security technologies. He holds a Bachelors degree in Engineering from the Gujarat University.