FROST & SULLIVAN

UEBA DEMYSTIFIED:

LEVERAGING MACHINE LEARNING

FOR 360 VISIBILITY OF IT RISK POSTURE

A Frost & Sullivan

White Paper

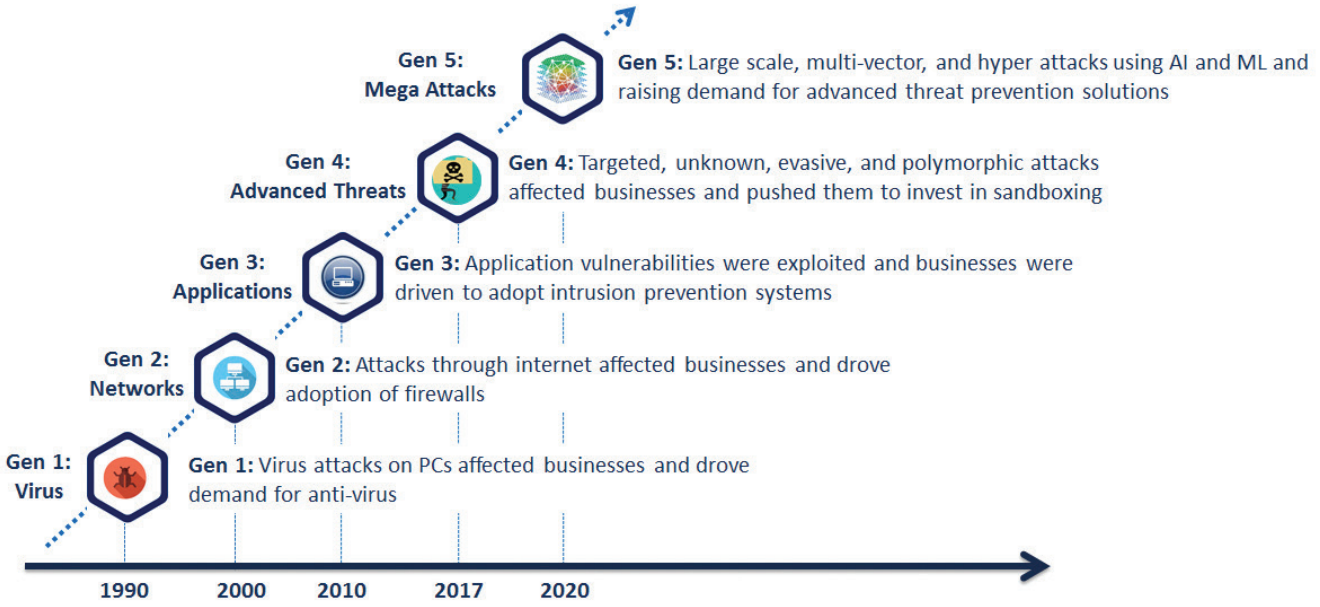
CONTENTS


EVOLUTION OF
THREAT
LANDSCAPE

Not more than three decades ago, "cyber-attacks" and "computer viruses" were mostly the work of teens and young adults, whose motivations were often simply the challenge, the thrill of making news headlines, and perhaps impressing their friends.

Today, organisations are being attacked by several types of different actors with more varied, complex, and less obvious motivations than usually associated with the mainstream image of a "**hacker**".

EXHIBIT 1: EVOLUTION OF CYBER ATTACKS



Source: Frost & Sullivan

Until recently, governments and financial firms were the primary targets of cyber attacks. Today, with every company more connected to the internet, the threat is now universal. Consider the chaos caused by three recent events. From 2011 to 2014, energy companies in Canada, Europe, and the United States were attacked by the cyber espionage group Dragonfly. In May 2017, the WannaCry ransomware held hostage public and private organisations in healthcare, telecommunications, and logistics in 150 countries and caused losses estimated at USD 4 Billion. Also in 2017, NotPetya ransomware attacked major European companies in a wide variety of industries, which caused losses estimated at USD 10 Billion. And in 2018, Meltdown and Spectre were exposed as perhaps the biggest cyber threats of all, showing that vulnerabilities are not just in software but hardware too.

In the past, cyber risk has primarily affected IT. But as the IoT grows and more companies hook their production systems up to the Internet, operating technology (OT) is coming under threat as well. The number of vulnerable devices is increasing dramatically. In the past, a large corporate network might have had between 50,000 and 500,000 end points; in the IoT era, the system expands to millions or tens of millions of end points. Unfortunately, many of these are older devices with inadequate security or no security at all, and some are not even supported anymore by their makers. By 2020, the IoT may comprise as many as 30 billion devices, many of them outside corporate control. Already, smart cars, smart homes, and smart apparel are prone to malware that can enlist them for distributed denial-of-service (DDoS) attacks. By 2020, 46% of all internet connections will be machine-to-machine, without human interaction, and this number will keep growing. Also, billions of chips have been exposed to be vulnerable to Meltdown and Spectre attacks, weaknesses that must be addressed.


IMPORTANCE OF
SECURITY
MONITORING

Malicious actors are known to exploit security vulnerabilities that enable access to sensitive data. Organisations understand that by continuously monitoring their IT infrastructure, they can limit their exposure to operational and compliance risks by detecting malicious activity quickly. Many industries, such as the financial sector, must adhere to regulations that require security monitoring. Also, most cyber security best practices and frameworks – such as HIPAA, ISO 27001 and PCI DSS - include monitoring as an enabling technique to detect incidents (both accidental and malicious).

Examining the top cyber threats in 2018 (refer the exhibit below); Malware is the highest experienced cyber risk. On the other hand, web-based attacks and web application attacks are confirming the argument that the wider the attack vector the higher the risk potential. Interestingly, phishing, data breaches, spam, and physical manipulation/ damage/theft/loss, all constitute significant cyber risks as well, which primarily come from inside the organisation. The impact of these cyber risks is quite significant. These result in operational outages, which cause productivity reduction, physical safety risks, and impact revenues; also, degradation of brand awareness and loss of business-critical data.

EXHIBIT 2: OVERVIEW AND COMPARISON OF THE THREAT LANDSCAPE 2018 AND 2017

Source: The European Union Agency for Cyber security (ENISA)

As intrusions employ a wide variety of attack vectors and methods, companies have to seriously consider continuous security monitoring, which provides real-time visibility of users and their devices when they attempt to connect to or work on an enterprise network. Security monitoring gives companies the ability to constantly look over their network to outpace cyber threats. With security monitoring, IT professionals can keep an open eye on and verify security compliance requirements regardless of data residing locally or in a datacentre, or even in the cloud.

Below, there are different scenarios where security monitoring is genuinely important, there are different types of user access should be monitored, examined and reported.

UNAUTHORIZED USE OF USER CREDENTIALS

A system user, either an authorized insider or an unauthorized outsider, gains access to the network and steals the credentials of another user. The malicious user then accesses critical assets containing sensitive data that the user is not authorized to view. Security monitoring practices can help detect such malicious behaviour by monitoring user activity logs, including correlation and analytics based on known user access policies. Anomalies and suspicious activity such as accessing unusual data or systems, or writing and executing binaries, can be detected and reported quickly.

MALICIOUS ACCESS ATTEMPTS

A malicious actor gains access to a network to access sensitive data, upload malware, or access different layers of the network architecture. Collecting log data on login and access events, both successful and failed, can help detect such intrusion attempts, particularly if a high number of failed authentication attempts or logging in at unusual times or frequencies are found.

SIMULTANEOUS LOGINS

A user's credentials are used to log in on two or multiple devices on the network at the same time. Although there are legitimate use cases with system administrators; one of the connections could have been made by a malicious actor who gained authorized user access and has used it to connect to the network.

Simultaneous access of user accounts can be detected by collecting log data on the time, duration, and system associated with each user session. Once alerted, IT professionals can validate this malicious access by communicating with the user and then take the required actions.

ACTIVITY FROM MULTIPLE GEOGRAPHIC LOCATIONS

A user's credentials are used to log in, within a short period, from two or multiple different locations (simultaneously or subsequently) that are geographically far apart. This situation indicates the user has logged in by using different network connections such as Wi-Fi and virtual private network, or a second connection was established from a second location, possibly by a malicious actor who has gained access to the credentials of the authorized user and has used them to connect to the network.

In light of the complexity of intrusions, risk surface, threat vectors and variety of risk actors, companies should have comprehensive tools to monitor the network, detect threats and report results. Advanced tools are employing Artificial Intelligence and Machine Learning to historically examine, correlate security events and incidents, and provide unprecedented intelligent analysis.


FROM SECURITY
MANAGEMENT AND
CORRELATION TO
SECURITY
ANALYTICS

When companies consider all the challenges facing IT security teams today, one of the most difficult is detecting threats that come from within their organization. i.e. Insider breaches and threats. Traditional cyber defence tools were not designed to deal with the sophisticated, multi-vector and targeted attacks that companies now face. Companies still need to deal with advanced attacks that arrive without any warning and bypass perimeter defences.

What is most important for companies today is to have security tools that analyse user behaviours that are connected to the organisation's network and entities or end-points such as servers, applications, etc. to figure out the anomalies. Companies need to keep a track of where do users usually log in from and what applications or file servers they use, what is their degree of access, etc. Additionally, information correlation is required to gauge if a certain activity performed by the users is different from their daily tasks and establishes a baseline of what is usual behaviour. Wherever an activity doesn't comply with the baseline, the security department should be on alert against a potential threat.

SIEM tools come into play to cover the detection and collocation puzzle, but typically lack effective and intelligent threat detection and response. SIEM tools can be bypassed by advanced attackers with relative ease, and focus more on real-time threats than extended attacks.

When it comes to coloration, SIEM still has some challenges and limitations:

- Can miss attacks because the rules lack context or miss incidents that have never been seen before
- Rules require too much maintenance
- Improperly filtered rules can make incident response execution slow
- Noisy alerts may be tedious work for SOC to analyse; potential serious threats could be left without analysis
- Complex to implement and manage

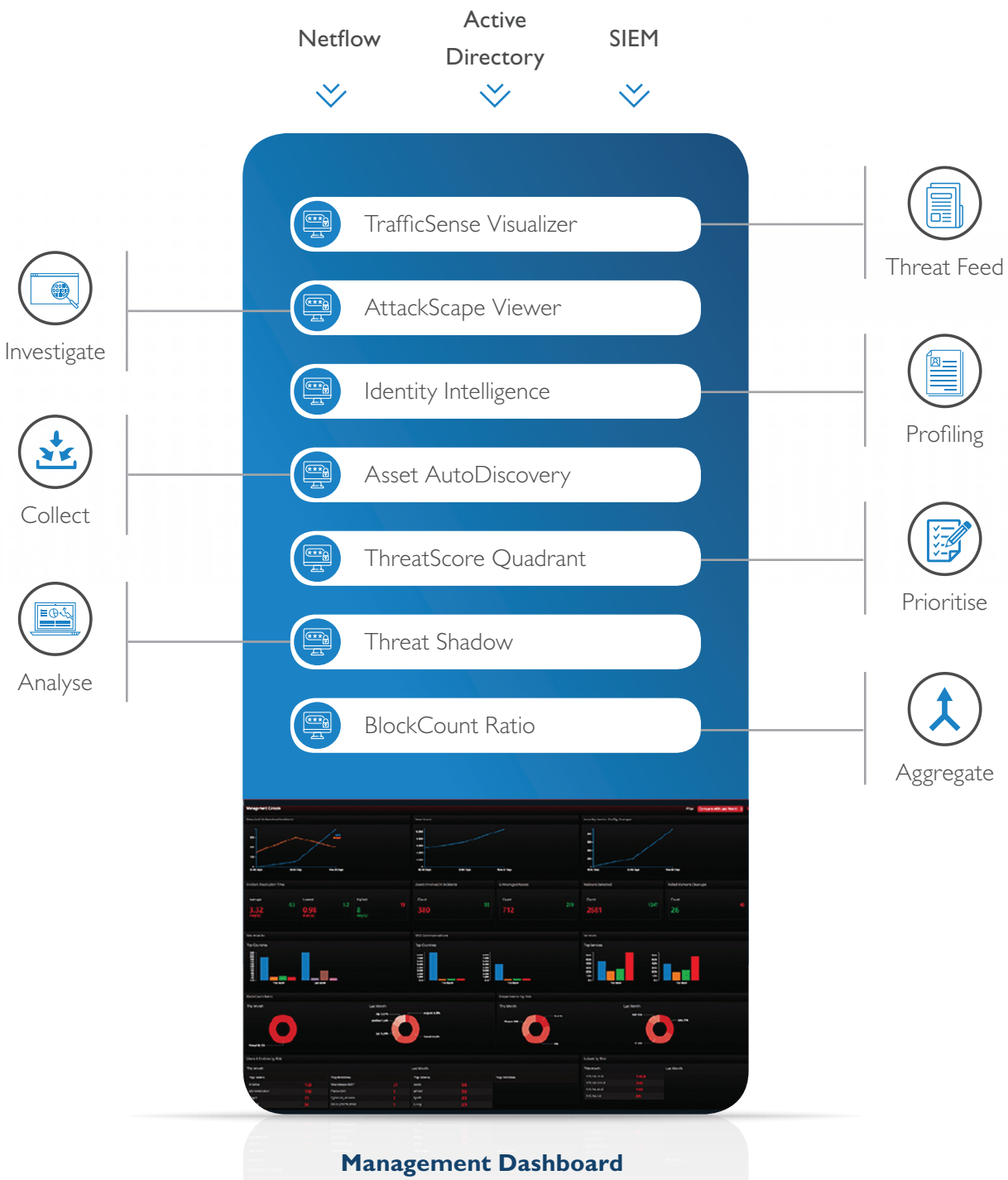
To overcome the limitations and challenges of SIEM correlation rules, UEBA comes and delivers immediate remediation:

- Reduces false positives
- Enables teams to prioritize alerts
- Makes it possible for the security professional to focus on the most credible and high-risk alerts
- Tracks anomalous user behaviour from external resources like cloud services, mobile devices, and IoT assets
- Saves time by analysing user behaviour through logs
- Provides automated incident response

However, UEBA is a vital component of any SIEM system (Exhibit 3). UEBA tools work jointly with SIEM solutions to provide insight into behavioural patterns within the network. By combining both solutions, companies gain the benefits of threat detection techniques that examine both human and machine behaviour.

Expanding SIEM to ingest behavioural anomalies detected by UEBA also provides additional context around known and unknown threats, as well as identifies the threats more accurately. This can save security professionals' time and increase SOC efficiency by eliminating false positives and only focus on threats that can't typically be detected through rules-driven correlation.

EXHIBIT 3: UEBA SOLUTION ARCHITECTURE



Management Dashboard

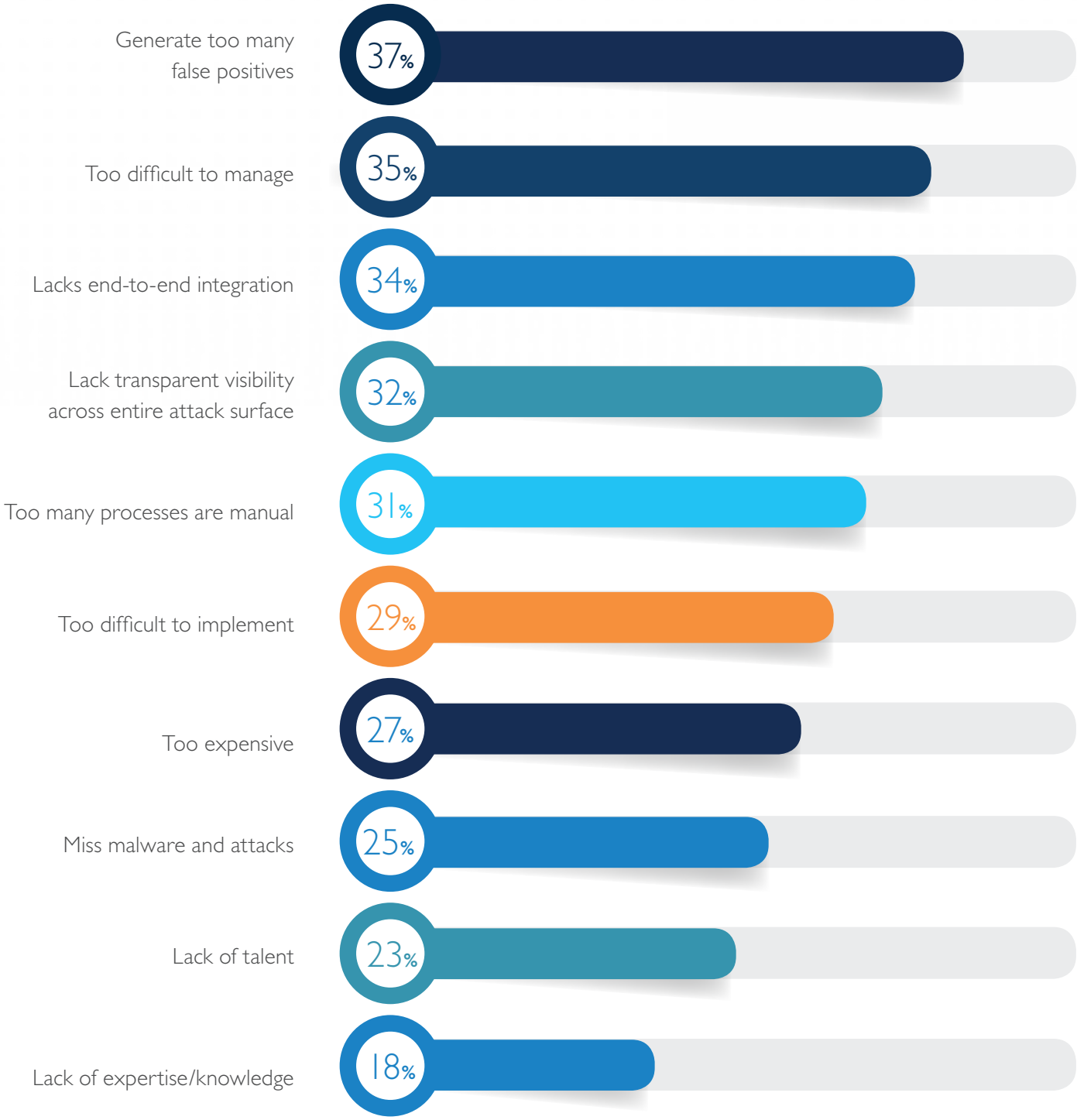
Source: Linkshadow

UEBA:
SALVATION FROM THE BIGGEST SECURITY ISSUES

Exhibit 4 below validates our argument about security issues that companies face.

Q: What are the top three security challenges?

EXHIBIT 4: MAJOR SECURITY CHALLENGES



Source: Frost & Sullivan

Interestingly, UEBA tools solve major security issues.

UEBA tools can simply pick anomalies and continuously improve analytical capability by analysing data. Data models improvise with security analyst feedback and volume, thereby reducing the numbers of false-positive alerts. Drawing the line between false positive and critical incidents is made simple and easy!

Organisations install multiple security solutions across the network in an attempt to achieve compliance and comprehensive security. But without full integration or lack of proper management, even security infrastructure can expose new threats. Specialized UEBA tools could help assess the performance of these security tools enabling companies to maximize their ROI and optimize the use of security assets.

Attacks involving compromised users and entities are notoriously difficult to detect because cyber criminals can avoid perimeter defences by using legitimate credentials to access corporate resources. UEBA tools automate the detection of these attacks with analytics-driven visibility. Artificial intelligence techniques, including supervised and unsupervised machine learning, are applied to data from network security infrastructure (e.g., packets, flows, logs, alerts, etc.). This information is used to create threat scores for all users and entities and seemingly disparate security events are observed and correlated over time.

By measuring the changes and/or anomalies associated with each entity, UEBA tools identify advanced attacks, which might appear to be a legitimate user activity but are likely an attacker disguised as a legitimate employee. These anomalies can only be detected by intelligently correlating orphan alerts over a long period.

UEBA tools can solve the issue of manual processes done by security professionals. This can be done by automatic attack detection and incident investigation without rules, configuration, and signatures.


BEYOND
EUBA & SIEM:
THE ERA OF
THREAT
HUNTING

It is said that "the absence of evidence is not the evidence of absence". The fact that organisations don't realise they have been breached doesn't mean they are not! While everything may appear fine, it could simply mean that security teams aren't looking where they should be looking.

No doubt that SIEMs are powerful detection tools that aggregate logs and alerts, but they rely on predefined correlation rules that are not able to dynamically spot the footprints of advanced attackers operating outside expected patterns. On the other hand, UEBA does not rely on signatures or rules and instead utilises advanced Machine Learning-based algorithms and risk scoring methodologies to correlate events over a longer timeline.

Many low and slow attacks go under the radar and don't trigger a rule such as internal users' activities, upload of a suspicious file into the FTP server, or admin logging into a server that has never been logged on before. As the number of such attacks increases, it will become more sophisticated and near-impossible for security staff to deal with, analyse, investigate, and efficiently take action; many of these attacks will get ignored and left uninvestigated.

Threat hunting platforms come in place to reduce the gap between the time of the attacks and detecting them, resulting in reducing dwell time drastically. These are tools for collecting and managing various data so that the security analysts (hunters) have access to the most comprehensive data on their network and systems. Threat hunting platforms are also equipped with advanced search, visualisation, and analytics capabilities to automate the detection of anomalies associated with potential cyber threats.

The security teams must get complete visibility across data. Threat hunting platforms provide the right quantity and quality of data to search through and conduct the required investigation. So the analysts' time would not be wasted in manually digging through immense data sets.

In a nutshell, threat hunting platforms combine techniques such as link analysis, UEBA, threat scoring, and Machine Learning, providing complete visibility to analysts to explore entities and their relationships. This makes it a simple yet powerful tool for security teams.


CRITICALITY OF
MANAGEMENT
SECURITY
DASHBOARD

Today, enterprises must handle numerous and highly sophisticated threats. In response to this hazardous landscape, it is no wonder that businesses are increasingly demanding security dashboards.

An effective security dashboard provides employees, ranging from security analysts to Chief Officers, with the tools to report on incidents and evaluate security risks. Different audiences have different objectives and responsibilities within their organisation.

One of the major responsibilities of a CISO/CIO is to ensure that the organisation is kept secure and protected against reputational and financial damage. CISOs/CIOs concerns are:

- To have a single pane glass view on the security posture and effectiveness of existing security systems
- Determine if they are achieving ROI from existing security investments
- Identify and monitor key security metrics that matter
- Compare key security metrics; Quarter to Quarter / Month to Month
- Obtain a summary of the ratio of attacks blocked at each layer of the security infrastructure, and what percentage went through.
- On the other hand, security analysts set out to harden endpoints, reduce the attack surface, investigate and respond to security incidents.

With a wide spectrum of information and insights that UEBA tools generate and the requirements of different views for different audiences in organisations, flexible dashboards become important.

KEY FEATURES OF UEBA: **WHAT TO LOOK FOR BEFORE IMPLEMENTING**

Many vendors claim UEBA capabilities in their products/tools, nevertheless, in reality, there are growing numbers of true UEBA providers. These providers' products function in a similar manner. Essentially, they are all built with a core engine running proprietary analytics algorithms that take in data feeds from existing sources and analyse the data. The UEBA tools then display the information and insights in a proper dashboard. The goal is to provide security IT professionals and higher management with actionable information and insights.

However, a number of features should be looked at before deciding to invest in a UEBA solution:

IDENTITY INTELLIGENCE

With increasingly sophisticated malware hitting enterprise networks daily, it is critical to guard data effectively to combat these threats, especially, since their identification is becoming tougher and tougher. However, such threats can be prevented.

The EUBA solution should provide the ability for organisations to analyse and profile network entities to uncover early signs of a breach, and underlying malicious behaviour to pinpoint threat actors hiding in plain sight. EUBA alerts if a system is misused by detecting whether the entity is behaving normally by comparing historic and current port usage patterns, whether the right protocols are being utilized on accessed ports, and gaining visibility into relationships with other network entities.

ASSET AUTO DISCOVERY

With the dynamic nature of the network environment, it is fundamental to continuously monitor and collect real-time data across systems, to adapt security programmes and better protect the business.

UEBA solutions should allow organisations to classify nodes through automated discovery of the entire IT infrastructure within the organisation, to ensure all assets are protected and up-to-date for compliance audits. To drill down into details to answer critical questions around how many systems are managed and unmanaged in the network, do they have endpoint security or not, and types of devices.

THREAT SCORING

New threats emerge every day from inside and outside the perimeter. Detecting these threats that bypass other security controls is important, but predicting their impact is even more crucial. Understanding behavioural patterns and correlating this information enables organisations to identify potential attacks with varying magnitudes of consequences and severity, and then prioritize actions to respond.

UEBA solution should perform anomalous behaviour detection as all traffic coming in and out of the organisation is constantly scanned. Detect threats, learn and adapt to user patterns, and keep track of everything, so that each attack can be scored for proper prioritisation. See which entity is most dangerous to the organisation by understanding where it can cause a crisis or is something to be wary of, or should be watched closely, or needs to be acted on immediately.

MANAGEMENT DASHBOARD

The management dashboard gives a holistic view of the security posture of the organisation. The management dashboard should be built to be completely configurable and customizable and must allow CISOs to find the information they need to monitor and take decisions regarding their network. Additionally, it must allow CISOs to monitor key security metrics by choosing the key metrics that matter for their organisation.

GEO-LOCATION TRAFFIC VISUALISATION

Organisations need to be attentive to traffic coming from or going to IP addresses belonging to countries known to host low reputation servers including phishing sites or malicious software. In addition, attempts to access published web sites or services from locations in which there are no customers, suppliers or remote employees should be scrutinized.

UEBA solutions should identify, monitor, and block network communication based on the geographic location of the source or destination IP address. Use Geo-Intelligence technology to get insights into where the traffic is headed, the source of incoming traffic, etc., enabling organisations to pay close attention to known traffic vs. unknown traffic and make informed decisions on whether there is a compromised node or insider threat scenario.

CONCLUSION

UEBA strengthens security by monitoring users and other entities, detecting anomalies in behaviour patterns that could be indicative of a threat. It takes a more proactive approach to security and gains more visibility into user and entity behaviour. Hence, today's organisations are able to build a stronger security posture and more effectively mitigate threats and prevent security breaches.

UEBA solutions significantly help to offload security professionals who deal with security tools on a regular basis. Instead of security teams examining millions of alerts per day, a UEBA solution can do the sifting. UEBA solutions identify critical breaches and notify security professionals instantly, so they can focus on responding to highly prioritized threats.

DISCLAIMER

This Whitepaper prepared by Frost & Sullivan is based on analysis of secondary information and knowledge available in the public domain. While Frost & Sullivan has made all the efforts to check the validity of the information presented, it is not liable for errors in secondary information whose accuracy cannot be guaranteed by Frost & Sullivan. The Whitepaper is intended to set the tone of discussions; information herein should be used more as indicators and trends rather than representation of factual information. It contains forward-looking statements, par ticularly those concerning global economic growth, population growth, energy consumption, policy support for water supply. Forward-looking statements involve risks and uncertainties because they relate to events, and depend on circumstances, that will or may occur in the future. Actual results may differ depending on a variety of factors, including product supply, demand and pricing; political stability; general economic conditions; legal and regulatory developments; availability of new technologies; natural disasters and adverse weather conditions and hence should not be construed to be facts.

ABOUT LINKSHADOW

LinkShadow is a US registered company with regional offices in the Middle East. It is pioneered by a team of highly skilled cybersecurity solution architects, product specialists and programmers with a vision to formulate a next-generation cybersecurity solution that provides unparalleled detection of even the most sophisticated threats. LinkShadow was built with the vision of enhancing organizations' defences against advanced cyber-attacks, zero-day malware and ransomware, while simultaneously gaining rapid insight into the effectiveness of their existing security investments

LinkShadow offers a wide spectrum of products and solutions which focus on how to overcome the challenges in the smart cyberattacks era. These products include Threatscore Quadrant, Identity Intelligence, Asset Autodiscovery, Trafficscene Visualizer & Attackspace Viewer, CXO Dashboards and Threat Shadow. Combining these products with the state-of-art capabilities, LinkShadow delivers supreme solutions which include Behavioral Analytics, Threat Intelligence, Insider Threat Management, Privileged Users Analytics, Network Security Optimization, Application Security Visibility, Risk Scoring and Prioritization, Machine Learning and Statistical Analysis and finally, Anomaly Detection and Predictive Analytics.

Organizations need to ensure that their essential security controls are in place and protected from breaches including SIEM blind spots and noisy alerts, compromised privileged user credentials, malicious insiders information, data exfiltration discovery, limited network traffic visibility, and lack of AI and behavioral analytics. LinkShadow precisely, help organizations to have tight grip on security controls. LinkShadow cybersecurity analytics platform is designed to manage threats in real-time by using artificial intelligence based machine learning to analyze event, perform UEBA, hunts for threats using cutting-edge threat hunting technologies and provide threat anticipation. LinkShadow help organizations enhance their defense against advanced cyberattacks, zero-day malware and ransomware.

To provide the organization with holistic view on the security posture, LinkShadow developed a revolutionary dashboard with unprecedented capabilities; this dashboard is fully customizable and completely configurable, allowing different levels in the organizations to view what they need. VPs and C-Level management get rapid insights with respect to the organization's security and risk posture, ROI or their existing security technology in terms of efficiency and performance, this capability allows higher management take fast responses and decisions regarding the organization's network state. Additionally, the dashboard is a great tool to keep a close eye on the risky users and assets, providing an insight about compliance per department which eventually expedites the organization to achieve the compliancy standards.

The sophisticated and broad cyberattacks surface brings organizations into the challenge of detecting the external attacks in addition to the internal attacks. Internal attacks could be in a form of malicious employees, who are make use of organizations data for personal benefits, or in a form of intruders, whose devices are infected and could constitute a threat to the organization's assets. Linkshadow provides behavioral analytics and privileged users' analytics leveraging the capabilities of Artificial Intelligence and Machine Learning, by studying and analysing the regular pattern of behaviour of the end users. This unique capability made LinkShadow leading cybersecurity solution provider in the UEBA domain.

Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubai
Frankfurt
Gurgaon
Herzliya
Hong Kong
Houston
Irvine
Istanbul
Jakarta
Johannesburg
Johor
Kolkata
Kotte Colombo
Kuala Lumpur
London
Mexico
Miami
Milan
Moscow
Mumbai
Nanjing
New York
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Silicon Valley
Singapore
Sydney
Taipei
Tokyo
Toronto
Valbonne
Warsaw

Dubai:
2601, Swiss Tower,
Cluster Y, 9th Floor,
PO Box 33372,
Jumeirah Lake
Towers, Dubai, UAE

Riyadh:
Servcorp Al Akaria Plaza
- Level 6, North Wing,
Gate D, Al Akaria Plaza,
Riyadh 12244 - 1622,
Kingdom Of Saudi Arabia

For over five decades, Frost & Sullivan has become world-renowned for its role in helping investors, corporate leaders and governments navigate economic changes and identify disruptive technologies, Mega Trends, new business models and companies to action, resulting in a continuous flow of growth opportunities to drive future success. Contact us: Start the discussion

For information regarding Frost & Sullivan's whitepaper, please write to:

SAURABH VERMA
Business Head, ICT, Middle East, Frost & Sullivan
P: +971 (0)44 33 1889 | M: +971 (0)52 238 2679 | E: saurabh.verma@frost.com

ANAS HAJ KASEM
Senior Consultant, ICT, Middle East, Frost & Sullivan
P: +966 (0)11 4868465 | M: +966 (0) 55 422 2794 | E: anas.kasem@frost.com

HANI AL SAYED
Business Development Manager, ICT, Middle East, Frost & Sullivan
P: +966 (0)11 4868464 | M: +966 (0) 50 196 9363 | E: hani.sayed@frost.com