Trace3 Research

360VIEW

Trend Report

5/31/2018

Security Operations in Flux

Features in Search of a Platform (FISOAP)

***Disclaimer** – This document has been prepared solely for Trace3's internal research purposes without any commitment or responsibility on our part. Trace3 accepts no liability for any direct or consequential loss arising from the transmission of this information to third parties. This report is current at the date of writing only and Trace3 will not be responsible for informing of any future changes in circumstances which may affect the accuracy of the information contained in this report. Trace3 does not offer or hold itself out as offering any advice relating to investment, future performance or market acceptance.*

Executive Summary

The security market is currently undergoing a large-scale consolidation and reorganization, driven by three major concerns:

- The growing number of security use cases and solutions.
- The increase in the number and sophistication of threats.
- The concern around finding, training and retaining security personnel.

These drivers are causing several security use cases to become features of larger platforms.

Report Scope

This report explores the following topics:

- A synopsis of the consolidation in the security space.
- A study of how those changes impacted the security market.
- A summary of conclusions drawn from changes in the market.
- A set of predictions and recommendations.

Research Method

This report is based on research requests received from Trace3 customers and field engineers. From these requests, relevant areas of the technical landscape were mapped out, including the identification of affected 360 View use cases and primary players in these use cases. This report also relies on relevant publicly available information, such as (but not limited to) announcements about M&A activity and strategic partnerships.

Analysis

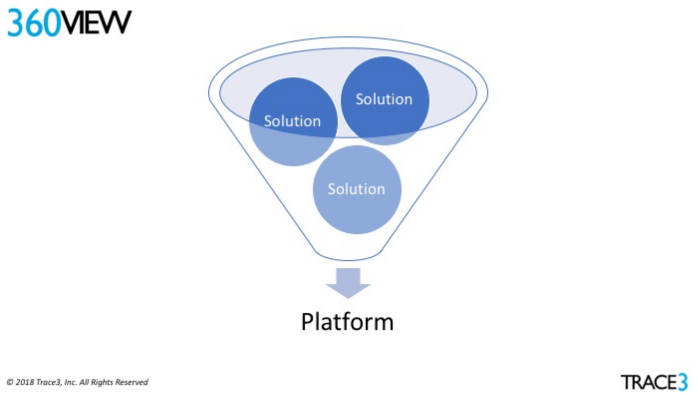
Did You Know...

- Gartner predicts the UEBA market will cease to exist by 2022. [1]
- 68% of breaches took months or longer to discover. [2]
- Frost & Sullivan and (ISC)² report the global cybersecurity workforce will have more than 1.5 million unfilled positions by 2020. [3]

Consolidation in the Security Space

In the past two years, Trace3 Research has observed consolidation in the security landscape due to enterprise customer and solution vendor needs.

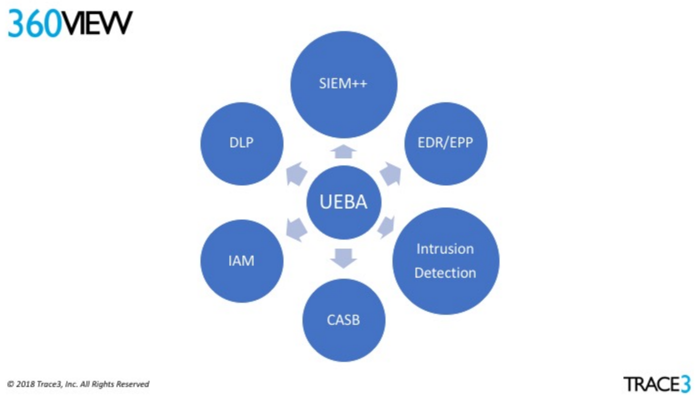
Enterprises demand simplification. Due to budget limitations, IT organizations cannot afford to hire *n* number of security analysts to support *n*+2 different security products. Concerns about the potential shortage of security professionals [3] makes the need for simplification even more urgent.



© 2018 Trace3, Inc. All Rights Reserved

From a parallel perspective, solution vendors must add emerging features to their offerings while making their products simpler and less labor dependent. Vendors are increasingly adopting partnerships, internal development and acquisitions to meet this need. This report looks at a sample of the security use cases affected.

UEBA as a Platform Feature



© 2018 Trace3, Inc. All Rights Reserved

User and Entity Behavior Analytics (UEBA) emerged as a distinct use case several years ago to assist security professionals in detecting both external and insider threats. Since 2016, the UEBA market has undergone major transitions:

1. UEBA products added other SIEM features to become SIEM++ platforms.
2. SIEM products added UEBA features into their offerings to become SIEM++ offerings.
3. UEBA also found its way into platforms like DLP, CASB, EDR/EPP, Intrusion Detection and Identity and Access Management.

SIEM augmented by a full featured UEBA is variously referred to as "Next-Gen SIEM", "SIEM 2.0", "SIEM 3.0" or "SIEM++" (SIEM++ will be used for the remainder of this report). The combination of SIEM and UEBA lays a foundation for improved efficiency by supporting tighter integration and automated triage and correlation. Good examples of this platform-enhancing behavior come from companies like Exabeam and Splunk.

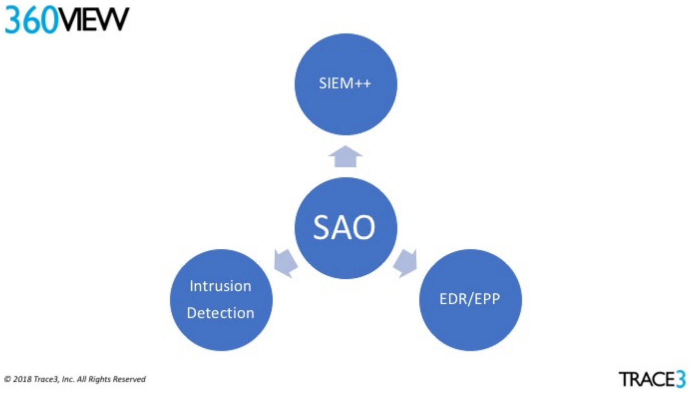
UEBA as a feature is not limited to SIEM++. Crowdstrike and Microsoft have added UEBA to their platforms in the EPP/EDR space, Protectwise and Extrahop in the area of Intrusion Detection, while Skyhigh and Forcepoint (CASB), Centrify (IAM) and Forcepoint (DLP) all added UEBA to their respective platforms.

Since the use of compromised credentials is the most common mechanism in data breaches [2], UEBA is critical to identify and respond to anomalous (threatening) user behavior. It should be noted that not all UEBA-based products are equal. SIEM++ and Intrusion Detection Platform-based UEBA offerings tend to be more full-featured while CASB and

EPP/EDR security platforms tend to implement "UEBA-lite" features able to identify the user or entity involved and to flag suspicious behavior, but lack capabilities like machine learning that facilitate a deep analysis in support of detecting anomalies.

Automation Moving Towards Ubiquity

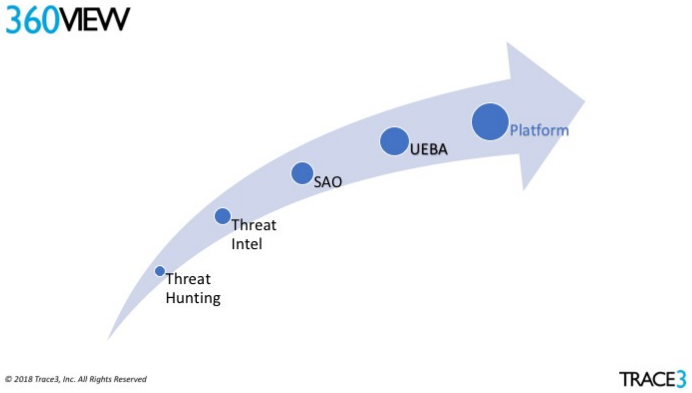
Security Automation and Orchestration (SAO) is another use case where Trace3 observes consistent consolidation. As with UEBA, the drivers are similar in that enterprise IT needs a solution for the problems of attack frequency and sophistication continuing to rise, thereby increasing the difficulty for security professionals to address them in a consistent fashion, promptly and without error. Enterprise customers needs a more integrated and full-featured security operations solution and security vendors are working to meet these needs.



The consolidation of SAO features into platforms is not yet as common as the adoption of UEBA features, but is a growing trend especially where orchestration is concerned. While many vendors have leveraged automation for event correlation and triage, the next target of opportunity is automated response, which will free SOC analysts to focus on more important tasks, such as threat hunting. Enhancing security operations to include automated response capability directly addresses the staffing challenges faced by security teams across the industry.

The same partner, develop or acquire approaches to platform enhancement applies to SAO offerings as they did with UEBA offerings. Splunk's recent acquisition of Phantom provides Automation and Orchestration to their platform, while Exabeam chose internal development to add automation into their platform. In the Intrusion Detection space, Extrahop and Vectra Networks are examples of vendors providing automation as a capability in their platforms, while CrowdStrike is integrating automation in their EPP/EDR space.

What's Next?



Looking ahead at the security operations landscape there are several other use cases emerging as consolidation plays, such as Threat Hunting and Threat Intelligence.

As SAO features merge into security platforms, they set the stage for automated Threat Hunting that proactively and iteratively searches networks to detect and isolate advanced threats that have evaded other existing security solutions. One example of this is Exabeam, who added Threat Hunting to their platform.

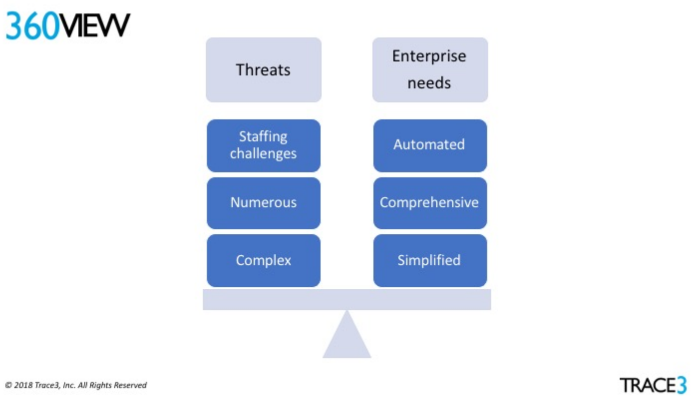
Threat Intelligence logically compliments the functionality provided by UEBA's ability to spot anomalous behavior and identify unknown threats, but what about the known threats? The ability to ingest and search threat intelligence data and other sources of Indicators Of Compromise (IOC) developed government agencies additional coverage to protect against attacks. One might call it a belt and suspenders approach. Alien Vault's USM offering is a prime example of integrating Threat Intelligence into a platform.

Looking even further ahead, it is apparent that there will undoubtedly be many other standalone security operations solutions that become features in search of a platform.

Conclusion

Facing pressure from tightening budgets, staffing challenges and an increasingly complex array of threats, enterprise customers need security solutions that have comprehensive lists of features and are well integrated to maximize value.

The changes in the UEBA, SAO, Threat Hunting and Threat Intelligence spaces this report details indicate the security vendors are responding to these needs and this trend is likely not only to continue, but deepen into other security operations use cases.



360VIEW

Threats

Staffing challenges

Numerous

Complex

Enterprise needs

Automated

Comprehensive

Simplified

© 2018 Trace3, Inc. All Rights Reserved

TRACE3

Trace3's Take

Predictions

1. Due to consolidation in the market, UEBA won't exist as a use case by 2022. [1]
2. Security Automation and Orchestration will follow a similar path as UEBA but will play out over a longer period.
3. Vendors who have integrated UEBA into their platforms will use that as a cornerstone to build out more complex analytics, with a goal of supporting automated responses to security events.
4. Vendors who have integrated Automation will continue leveraging that capability to enhance event correlation and triage. Longer term that capability will come to bear on threat hunting.

Recommendations

1. At this time, it is not recommended to rely solely on a standalone pure-play UEBA product, as these have a limited market window before being absorbed or evolved into a larger security platform.
2. Enterprises would do well to consider Security Automation and Orchestration features when selecting security platforms.
3. Given the recent changes outlined in this report, enterprises should review their current products to ensure they are receiving full value.

Appendix

Featured Use Cases

Cloud Access Security Broker

CASB solutions are on-premise or cloud-based security policy enforcement points placed between cloud service consumers and providers to enforce enterprise security policies as the cloud-based resources are accessed. Security policies under CASB control include authentication, single sign-on, authorization, credentials, device profiling, encryption, tokenization, logging, alerting, malware detection, and prevention.

Data Loss Prevention

Data loss/leak prevention solution is a system that is designed to detect potential data breach / data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).

Endpoint Detection & Response

New Hotness: Falcon Platform by CrowdStrike, Tanium

EDR technologies monitor endpoint activities and aid in the detection, containment, investigation and remediation of malicious behavior.

Endpoint Protection Platform

New Hotness: Protect by Cylance, User Protection Solution by Trend Micro

A solution that converges endpoint device security functionality into a single product that delivers antivirus, anti-spyware, personal firewall, application control and other styles of host intrusion prevention (for example, behavioral blocking) capabilities into a single and cohesive solution."

Identity and Access Management

An identity management access system is a framework for business processes that facilitates the management of electronic identities.

Security Information and Event Management (SIEM)

New Hotness: Splunk Enterprise by Splunk, Security Intelligence Platform by Exabeam

Security information and event management (SIEM) is a term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications.

Threat Hunting

Cyber threat hunting is the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions. This is in contrast to traditional threat management measures, such as firewalls, intrusion detection systems (IDS), and SIEM Systems, which typically involve an investigation after there has been a warning of a potential threat or an incident has occurred.

Other Materials

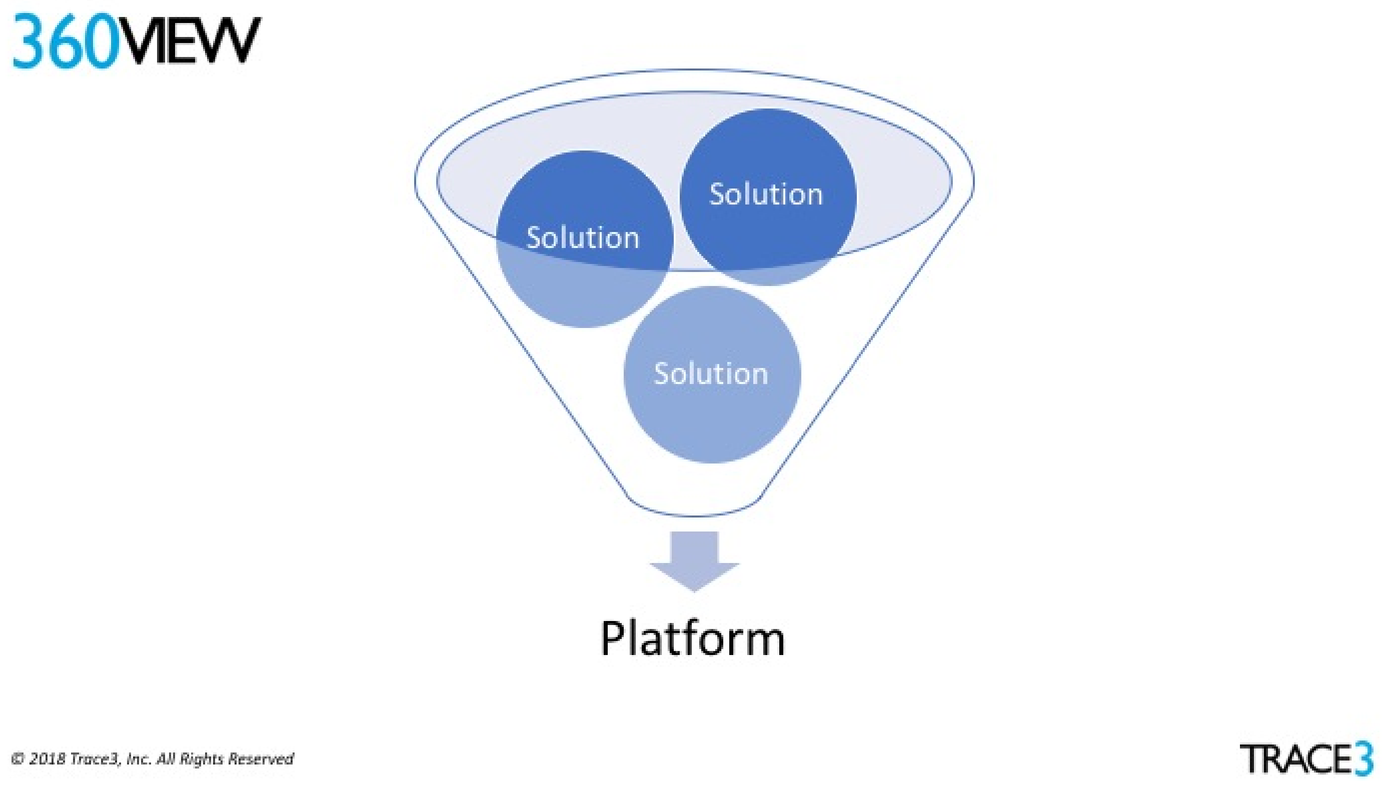
Security Operations in Flux Powerpoint

All slides

Sources

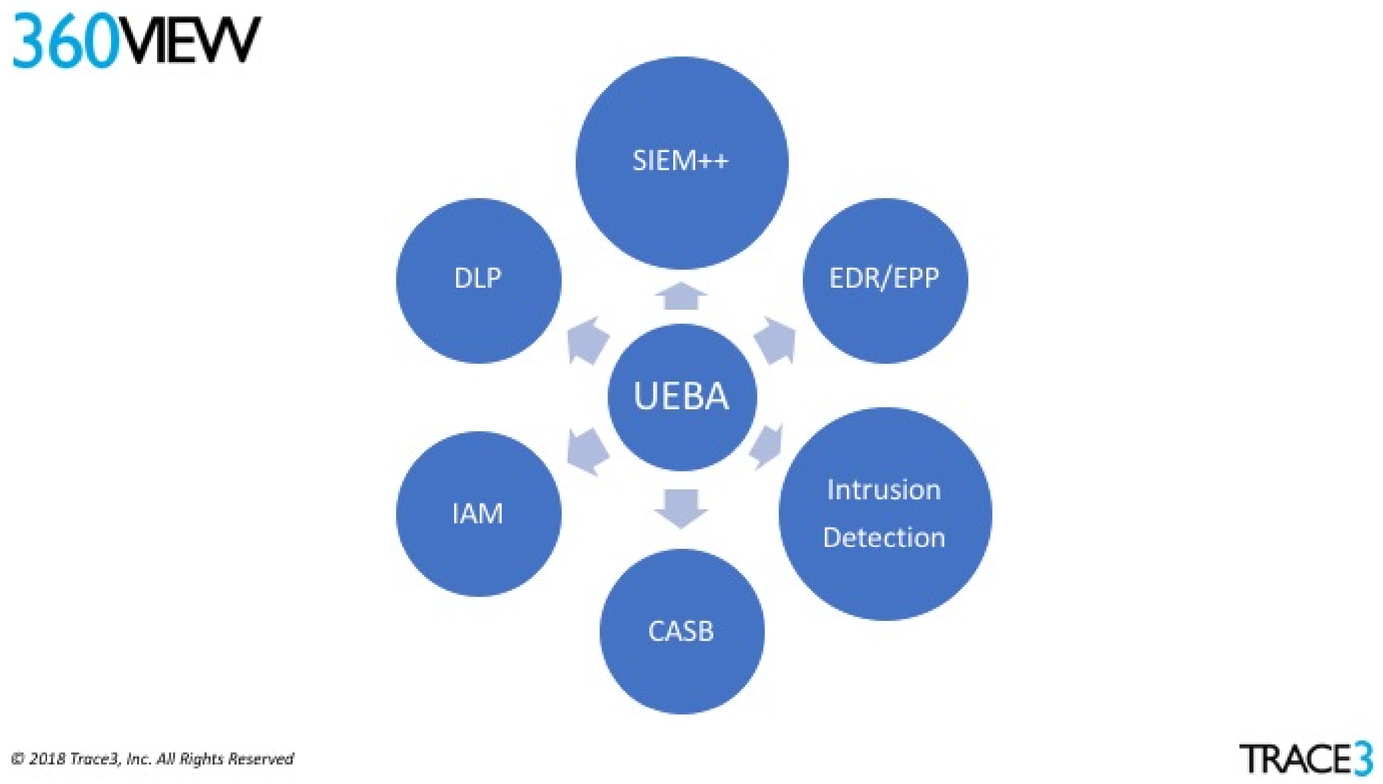
1. "The Disappearing UEBA Market" by Avivah Litan published Jan 3, 2017
2. "2018 Data Breach Investigations Report" - Verizon
3. "(ISC)² Global Information Security Workforce Study" - Frost & Sullivan published Apr 17, 2015

Consolidation in the Security Space

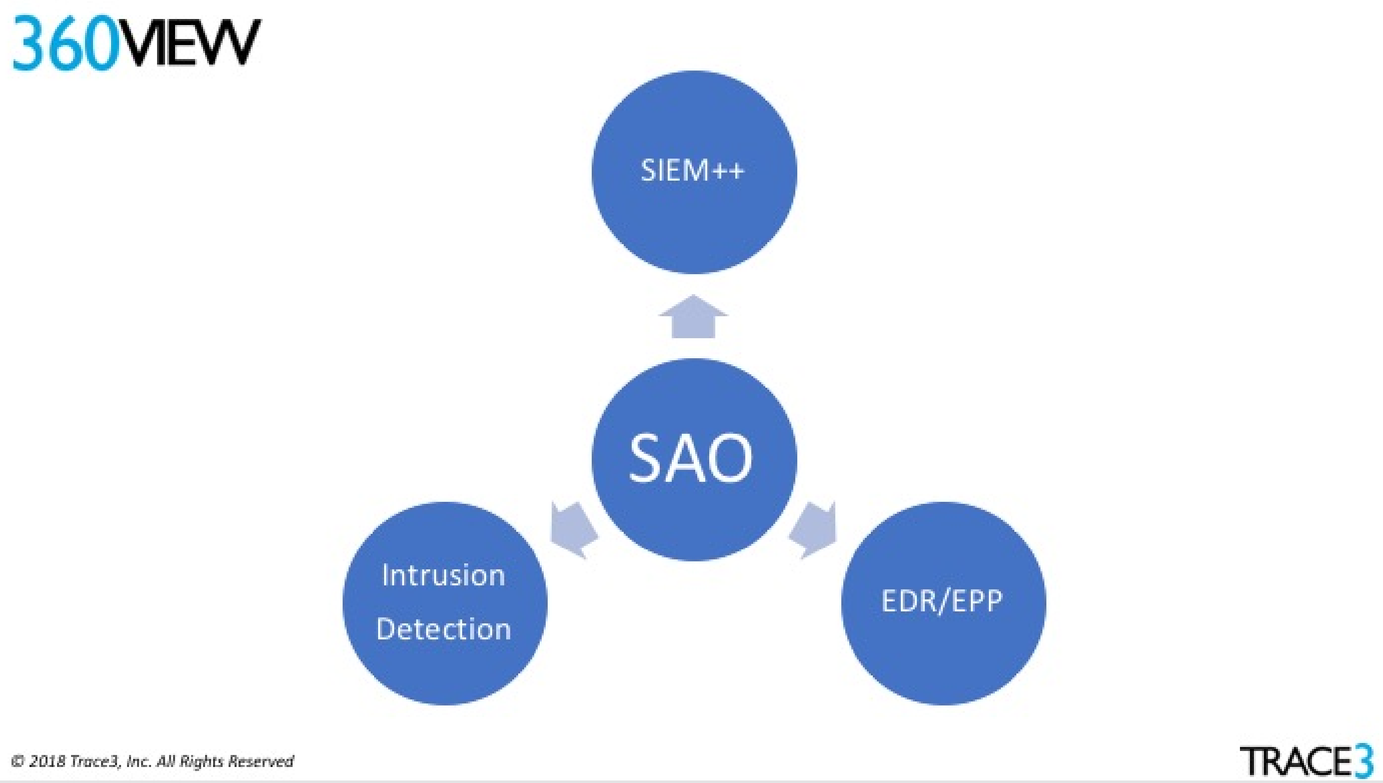


© 2018 Trace3, Inc. All Rights Reserved

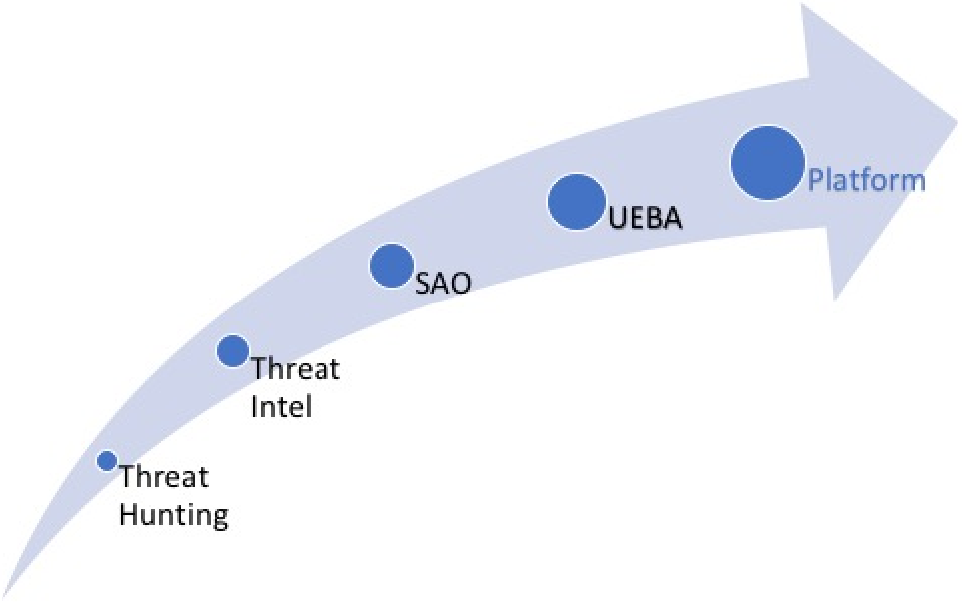
UEBA as a Platform Feature



Automation Moving Towards Ubiquity



What's Next?



Threat Hunting

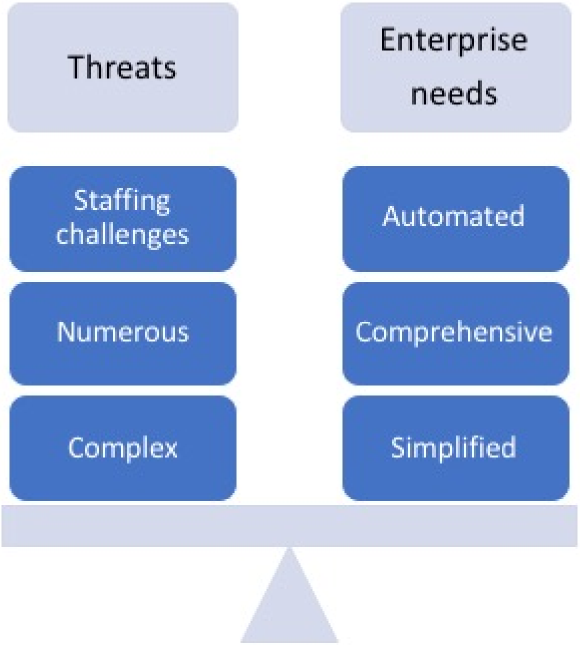
Threat Intel

SAO

UEBA

Platform

Conclusion



Threats

Staffing challenges

Numerous

Complex

Enterprise needs

Automated

Comprehensive

Simplified

About Trace3 Research

To solve the IT problems of tomorrow, Trace3 Research leverages our unique access across the technology landscape to derive impartial insights. By identifying and analyzing technology and market trends, we enable our customers to prepare for and master tomorrow's challenges before they arrive. Trace3 Research leverages our partnerships with 500 established and emerging technology companies, the real-world experience of over 250 engineers, a 3000-client ecosystem and deep relationships with dozens of the top Silicon Valley venture capital firms to spot trends ahead of most industry pundits. This allows our customers to gain an insider advantage on tomorrow's trends and reduce their technical and business risk.

(end of report)