Reveal security

The Future of Identity Threat Detection & Response is Here

Harness the power of machine learning based behavioral analytics to defeat attackers

Doron Hendler

CEO and Co-Founder, Reveal Security

January 31, 2024

Reveal Security

Leading innovation in identity threat detection and response

Detect and respond to identity threats **post-authentication** in and across **SaaS applications and cloud services.**

Born out of Security Innovation

Deep threat detection and SaaS knowledge. Focused on the **most accurate detection** of anomalous behavior for the **highest fidelity** input to the SOC.

salesforce | Microsoft | okta | servicenow | W

SAP | aws | Google Cloud | Dynamics 365 | box

SaaS Applications

Reveal security

- Founded in January 2021
- HQ in New York City, USA
- R&D in Tel Aviv, Israel
- 45 employees

$23M

Series A Venture-Funded

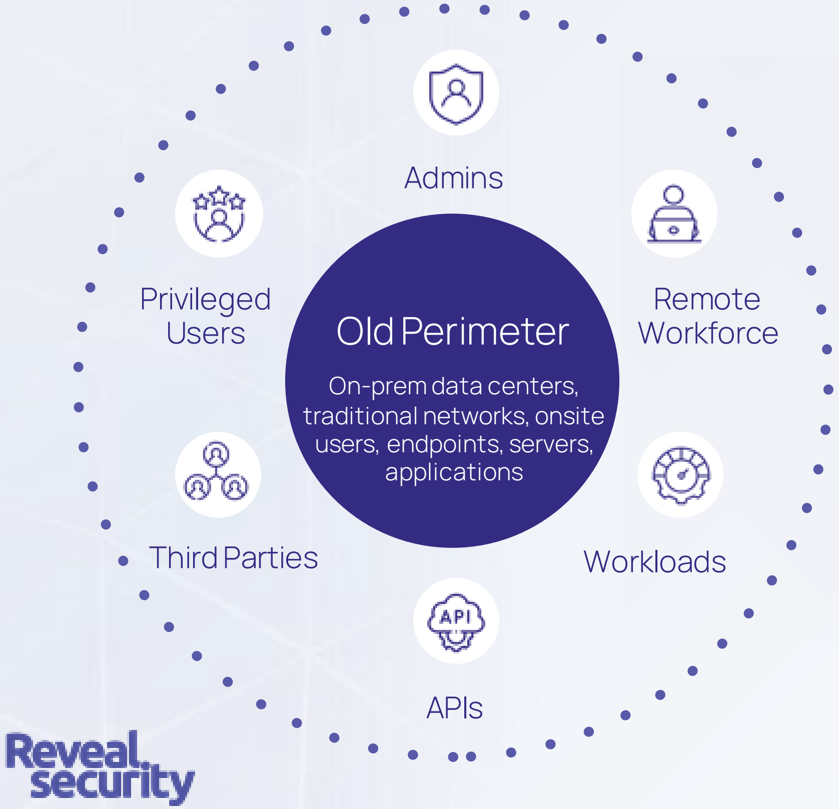
Hanaco | SYN | SILVERTECH VENTURES | WORLD TRADE ventures

2023 SINET16 INNOVATOR AWARD

it-sa 2023 IT Security Award

New Identities, New Environments, New Attack Methods

Identity is the New Perimeter and Applications are the New Cyber Battleground



Admins

Privileged Users

Remote Workforce

Old Perimeter

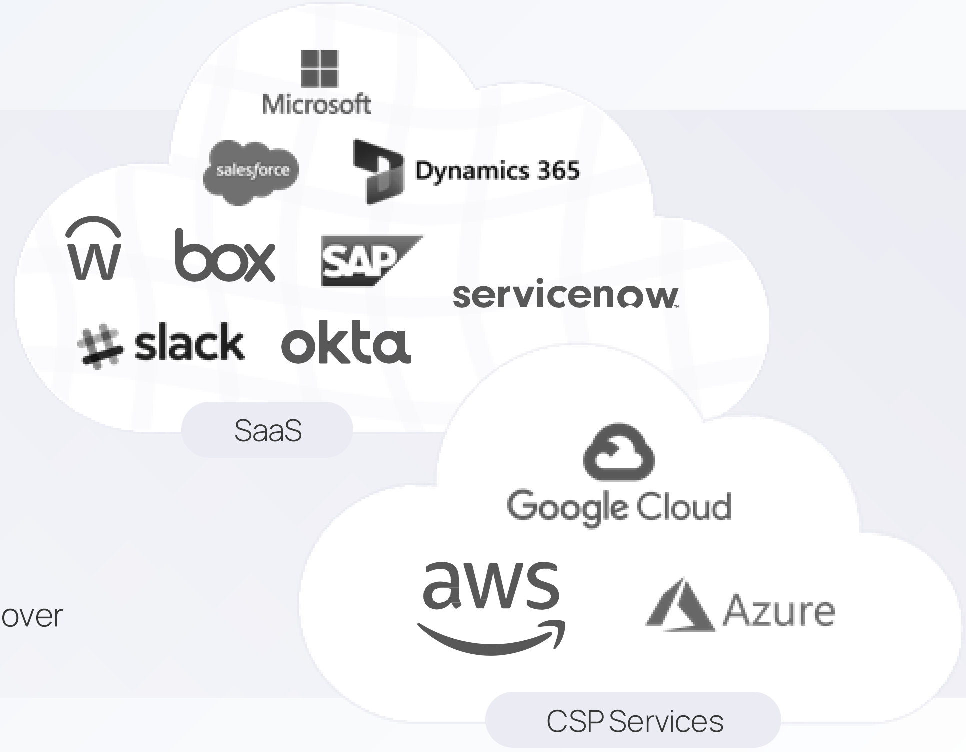
On-prem data centers, traditional networks, onsite users, endpoints, servers, applications

Third Parties

Workloads

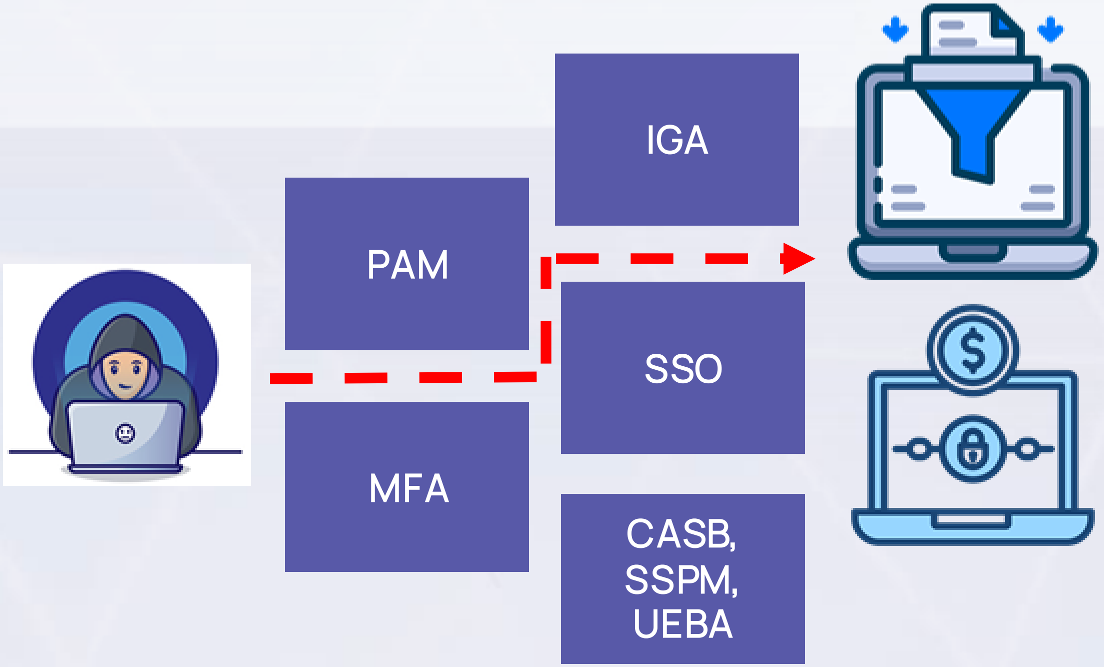
APIs

- Account Takeover
- Over entitlement
- Insider Threat
- MFA, IdP, PAM bypass
- Misconfiguration
- Privileged Account Takeover
- Third Party Access



Despite significant investment in IAM controls….

The financial impact of data breaches, ransomware (cyber criminals) and data leaks (negligent employees) in application environments continue to rise each year.



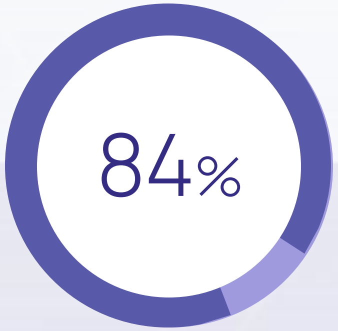
PAM

MFA

IGA

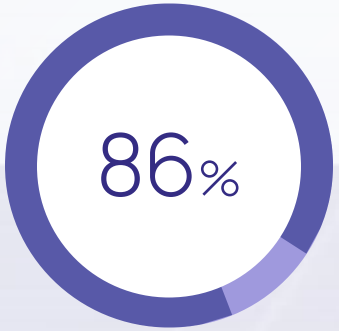
SSO

CASB, SSPM, UEBA



84%

Experienced an identity-related breach last year

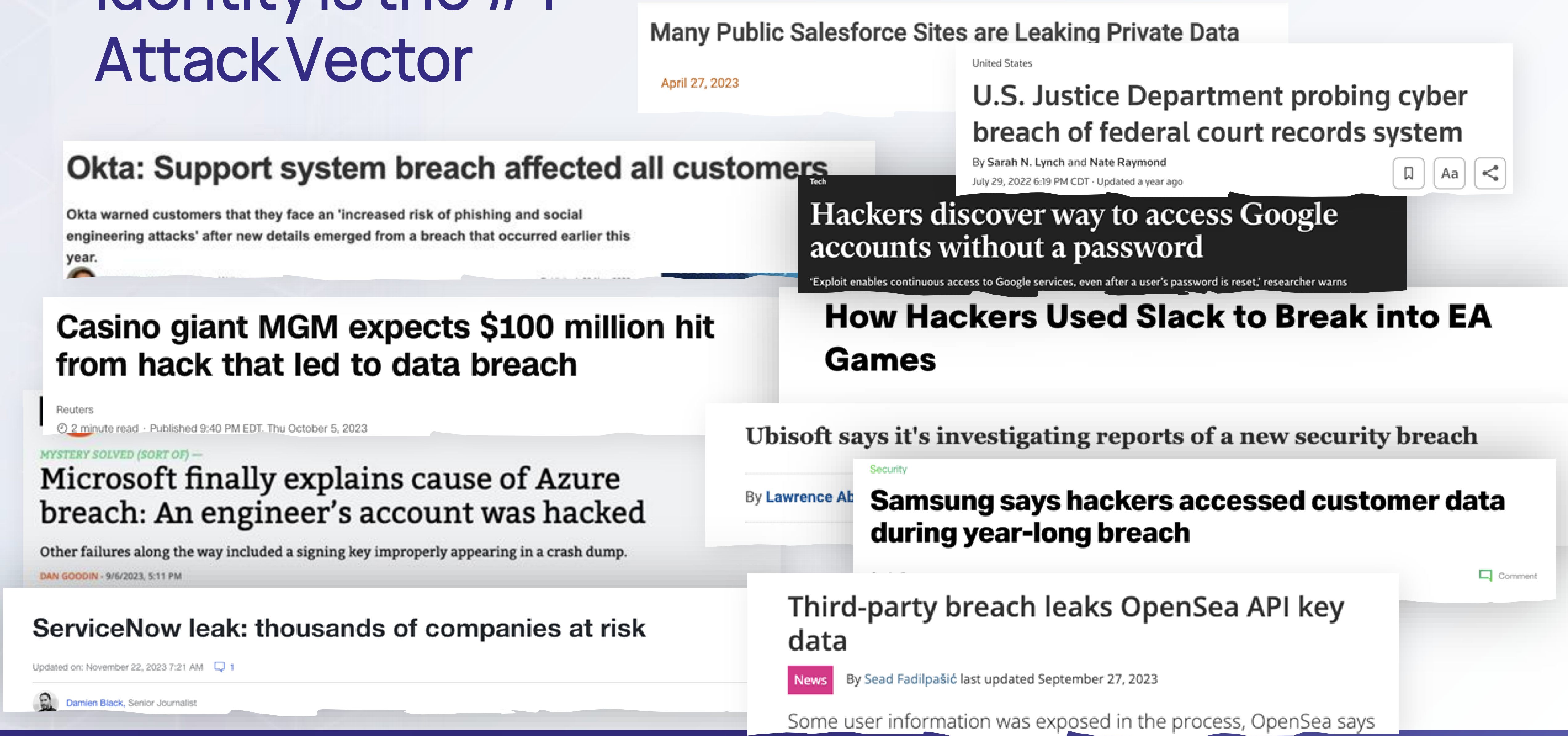


86%

Of application breaches involve the use of stolen credentials.

Source: Identity Security Alliance, Cloud Security Alliance, Crowdstrike,,IBM, Verizon DBIR

Identity is the #1 Attack Vector



Many Public Salesforce Sites are Leaking Private Data

April 27, 2023

United States

U.S. Justice Department probing cyber breach of federal court records system

By Sarah N. Lynch and Nate Raymond

July 29, 2022 6:19 PM CDT · Updated a year ago

Okta: Support system breach affected all customers

Okta warned customers that they face an 'increased risk of phishing and social engineering attacks' after new details emerged from a breach that occurred earlier this year.

Tech

Hackers discover way to access Google accounts without a password

'Exploit enables continuous access to Google services, even after a user's password is reset,' researcher warns

Casino giant MGM expects $100 million hit from hack that led to data breach

Reuters

2 minute read · Published 9:40 PM EDT, Thu October 5, 2023

How Hackers Used Slack to Break into EA Games

MYSTERY SOLVED (SORT OF) —

Microsoft finally explains cause of Azure breach: An engineer's account was hacked

Other failures along the way included a signing key improperly appearing in a crash dump.

DAN GOODIN - 9/6/2023, 5:11 PM

Ubisoft says it's investigating reports of a new security breach

By Lawrence Ab

Security

Samsung says hackers accessed customer data during year-long breach

Comment

ServiceNow leak: thousands of companies at risk

Updated on: November 22, 2023 7:21 AM 1

Damien Black, Senior Journalist

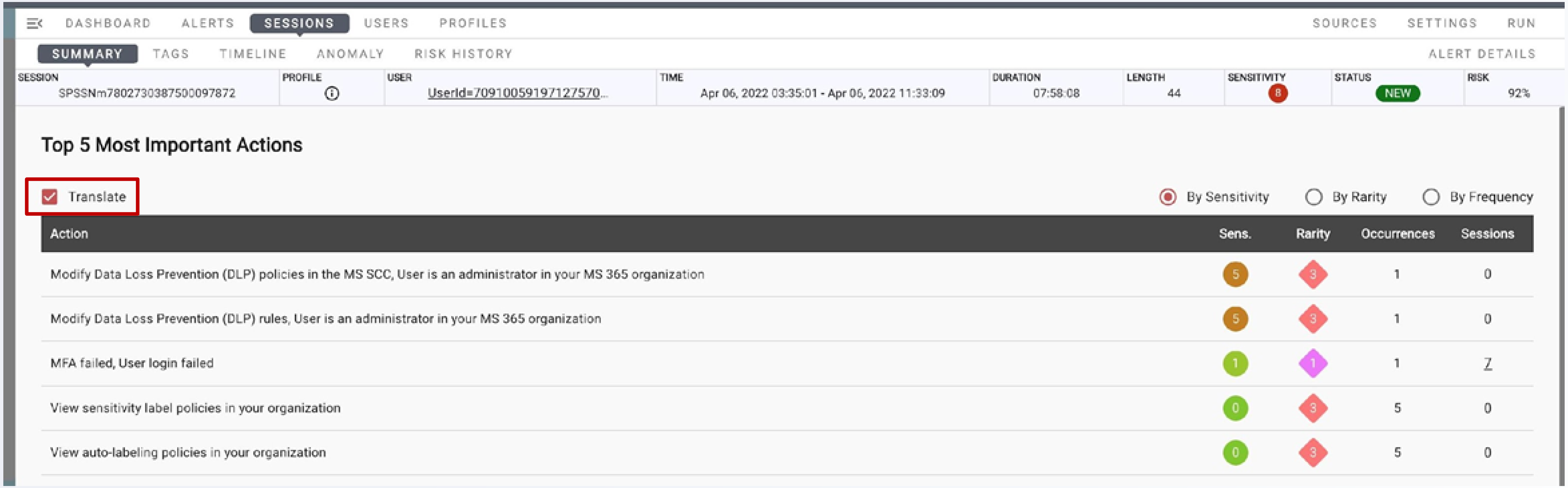
Third-party breach leaks OpenSea API key data

News By Sead Fadilpašić last updated September 27, 2023

Some user information was exposed in the process, OpenSea says

Detect attacks early in the kill chain

Microsoft 365



SESSION	PROFILE	USER	TIME	DURATION	LENGTH	SENSITIVITY	STATUS	RISK
SPSSNm7802730387500097872	ⓘ	UserId=70910059197127570...	Apr 06, 2022 03:35:01 - Apr 06, 2022 11:33:09	07:58:08	44	8	NEW	92%

Top 5 Most Important Actions

☑ Translate

● By Sensitivity ○ By Rarity ○ By Frequency

Action	Sens.	Rarity	Occurrences	Sessions
Modify Data Loss Prevention (DLP) policies in the MS SCC, User is an administrator in your MS 365 organization	5	3	1	0
Modify Data Loss Prevention (DLP) rules, User is an administrator in your MS 365 organization	5	3	1	0
MFA failed, User login failed	1	1	1	7
View sensitivity label policies in your organization	0	3	5	0
View auto-labeling policies in your organization	0	3	5	0

Reveal security

Reveal Security for MS365

- Phishing attacks / Unauthorized access: attacks that attempt to trick users into revealing login credentials
- User and group management operations
- Data exfiltration - Anomaly sequence of file operations (e.g. download, modify, etc.)
- Application management operations
- Content management operation
- Mailbox management operations (e.g. defining mailbox rules)
- Any combination of the above, for example:
    - Anomaly sequence of login activities and user management operations
    - Anomaly sequence of file operations and permission management operations
    - Anomaly sequence of permission management operations and mailbox management operations.

SAP Findings by Reveal Security Identity Detection and Response

How does Reveal Security assists Reduce Risk (fraud) in SAP (complementing SAP Access Control system / SAP GRC)

- In contrast to the traditional approach of auditing employees' permissions once a year, Reveal Security provides:
  - **Ongoing detection** for any deviation from the access rights / permissions the employees should have – Roles and Department
  - **Rank anomalies** detected **based on their business meaning**
- Reveal Security is complementary to SAP GRC that allows **accurate early detection** of abnormal usage, which is usually an indication for access-control issue

Examples of Alerts Detected For SAP

- Employee performing a sequence of actions they have never done before
  - Viewing/updating of classified and sensitive information
- Employee using credentials of another employee (e.g., after the other employee has left the organization)
- Developer performing business transactions in SAP production environment (without proper authorization)
- Creation of a new user (AU7) or modification of user permissions (AUB) by employees who should not have permission to do so
- Direct update of tables in SAP by employees who should not perform these operations
- Abnormal authentication (e.g., “dialog” login using password – which is not allowed by the organization)
- an employee who does not work in the HR department, carrying out HR transactions after receiving HR permissions

Security Gap: Monitoring Identity Behavior in Applications Post Authentication

SOLUTION	FOCUS	POST AUTH MONITORING?	IDENTITY BEHAVIOR IN APPLICATIONS?
XDR	Infrastructure: endpoint, network, cloud	☑	⚠
EDR	Monitoring devices to detect abnormalities and threats	☑	⚠
NDR	Network-centric threat detection and traffic analysis	☑	⚠
IAM/ Access	Access controls and identity threats up to login	⚠	⚠

Reveal security

How would you know if:

▷ All your CS tickets were leaked out of ServiceNow?

▷ Your customer data had been compromised in Salesforce?

▷ Sensitive company documents were leaked out of Box?

▷ Your MFA controls had been bypassed?

▷ How would you know if you have privileged user accounts not managed in PAM?

…This Is a Growing Challenge

SuccessFactors SAP

salesforce

aws

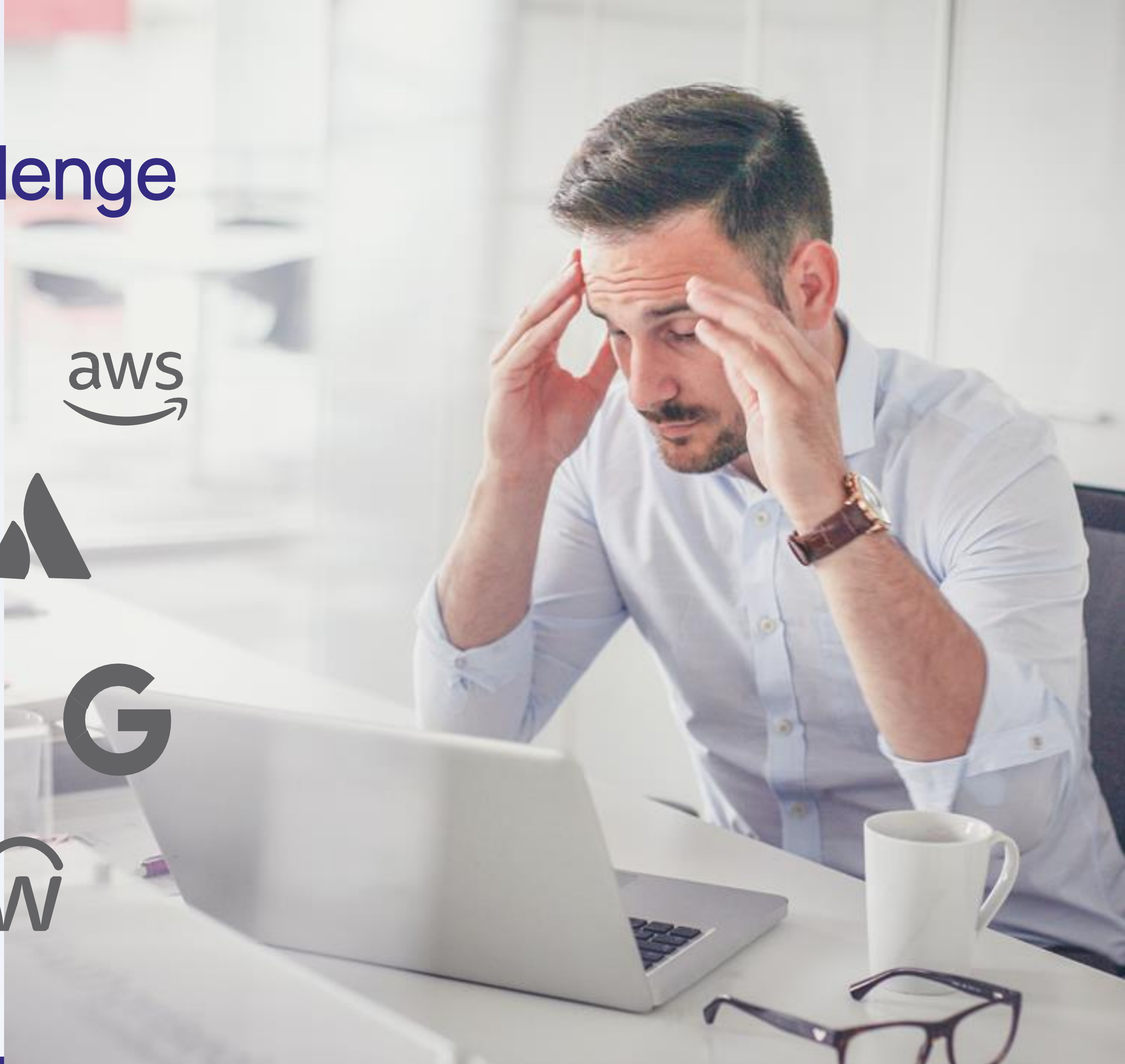
servicenow

Dynamics 365

box

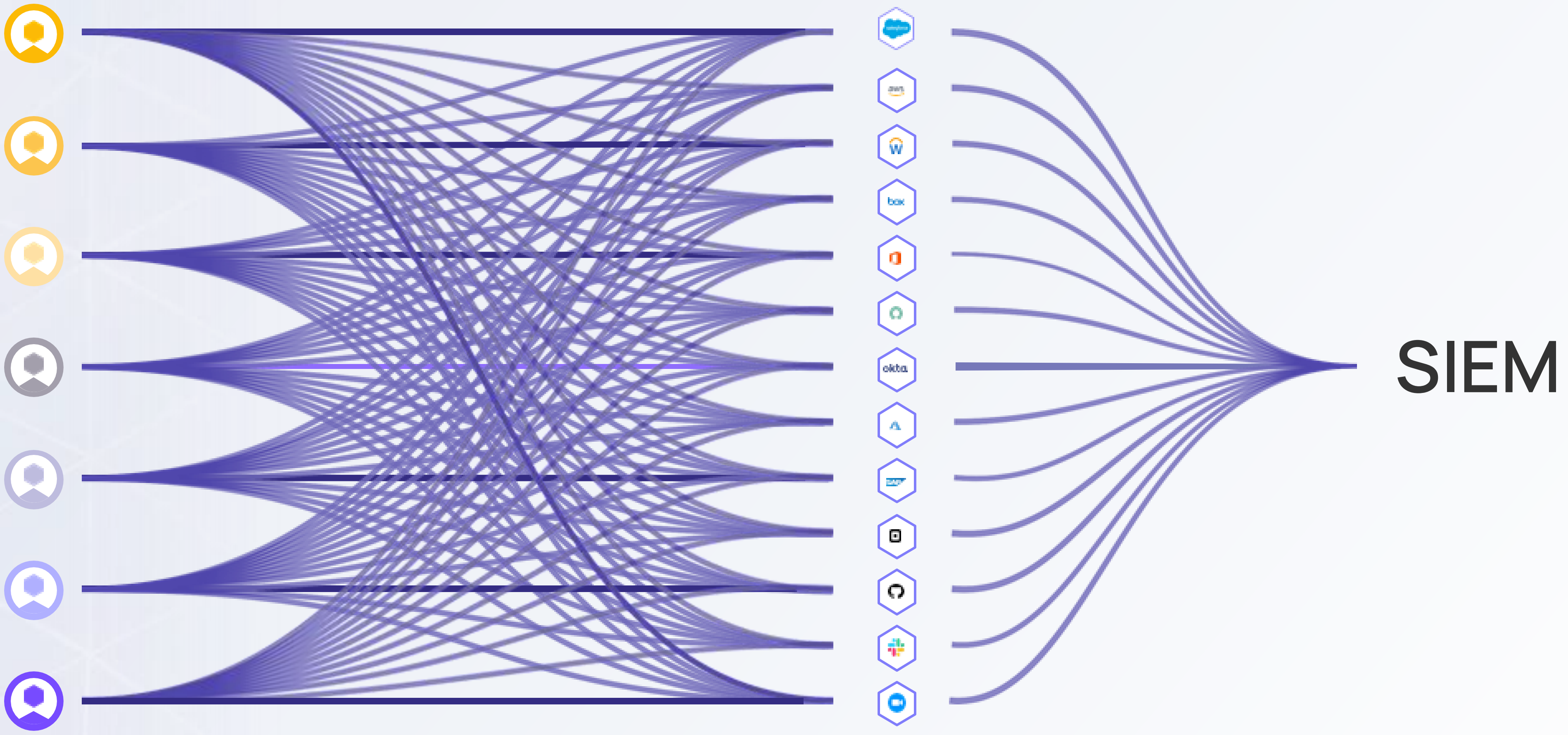
Microsoft 365

okta



Reveal security

How do you know what to look for in your business applications?



Reveal security

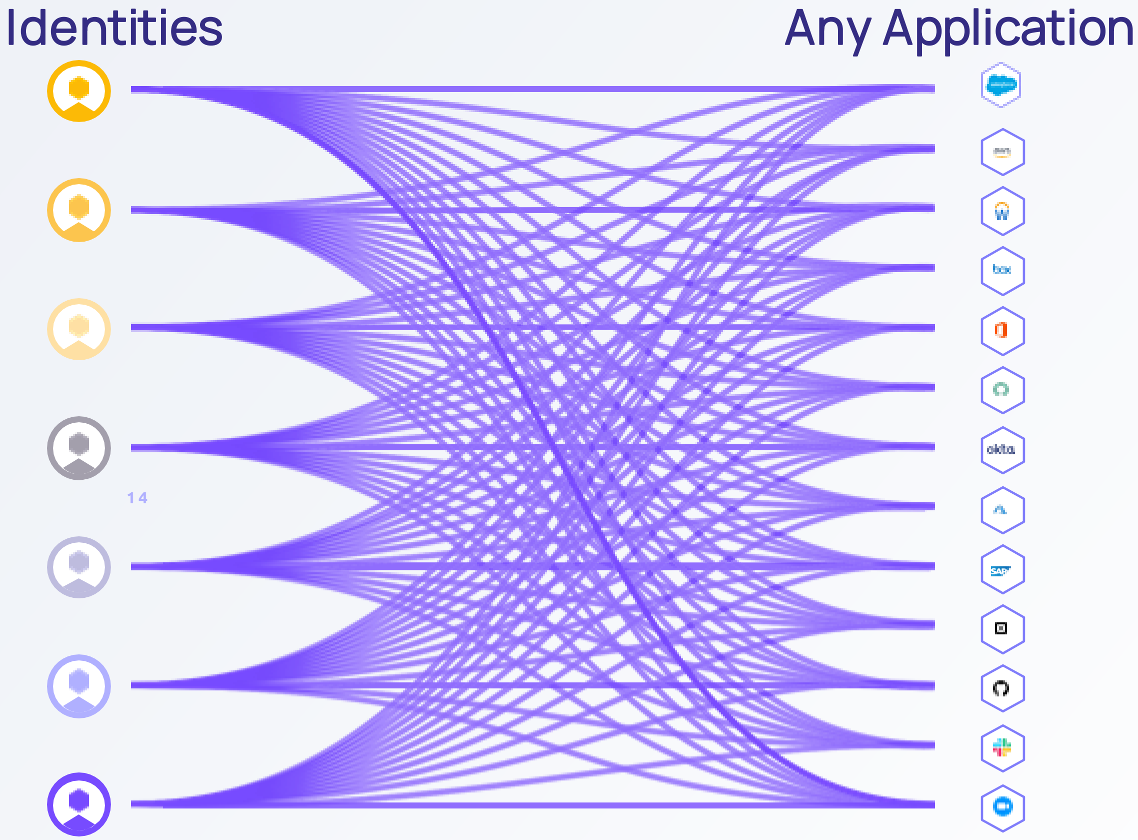
Technology Challenges

Each application / API has a unique set of operations

Each application has its own language for logging, making it impossible for security teams to translate and build rules / detection logic

Each user has many activity flows per application

Traditional security tools built on known and identified rulesets and signatures are adept in detecting known threats, but cannot scale to fully address the complexity of in application security threats, such as insider threats or compromised accounts.



Each line represent a person-to-app relationship

Sample activity flow between users and applications

What Is Needed

Continuous monitoring of identity behavior in applications is now a requirement

"There are major detection gaps between IAM and infrastructure security controls. IAM is traditionally used mainly as a preventive control, whereas infrastructure security is used broadly but has limited depth when it comes to detecting identity-specific threats."

Gartner

01

Comprehensive understanding of behavior

- In and across applications
- Content of business flows
- Identity Journey Analytics
- Distinguish between legitimate and malicious use

02

Machine learning approach

- Automatically learn behavior
- Scale analysis and output
- Accurately pinpoint anomalies
- Detect sophisticated and novel threats

03

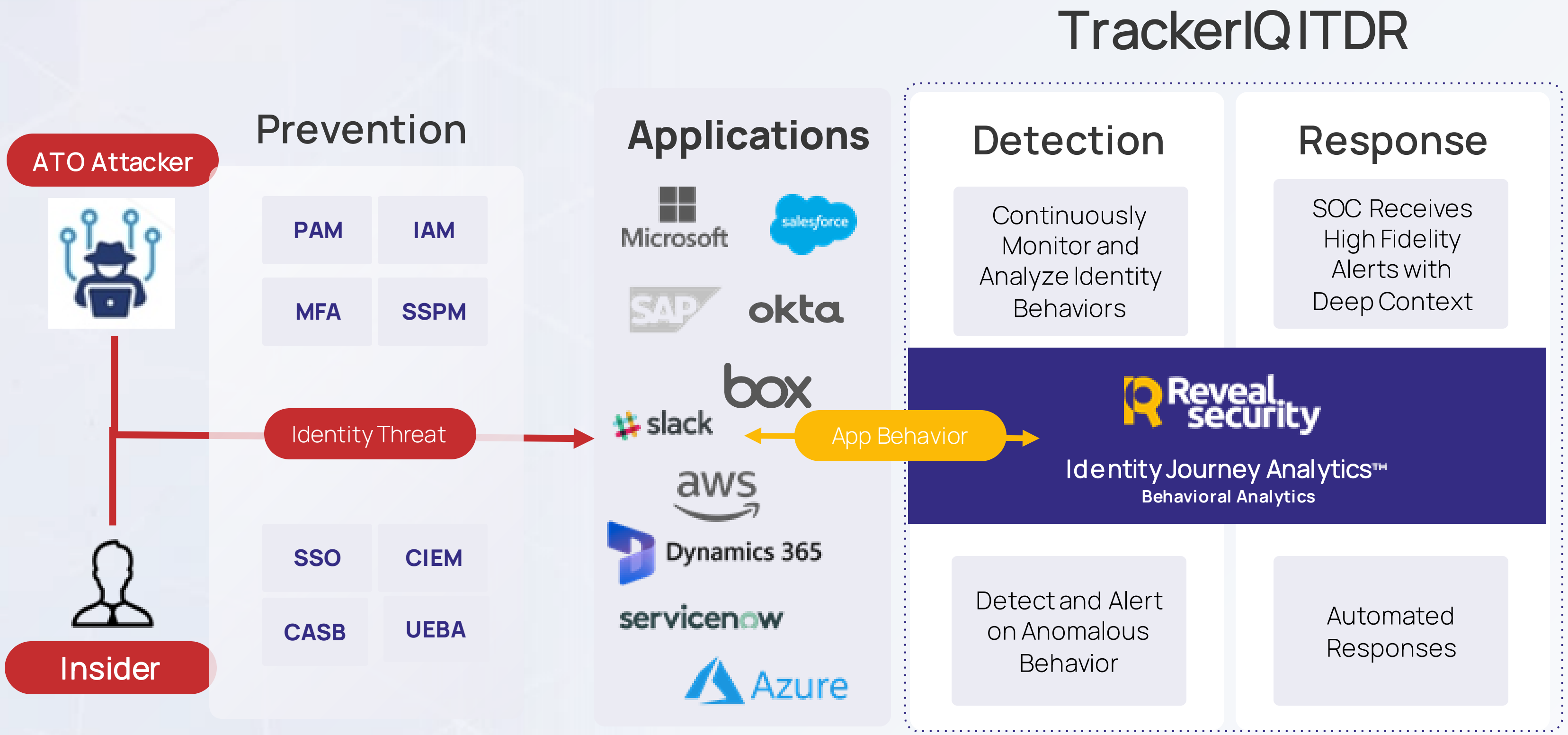
Proactive response

- Initiate an investigation
- Trigger an auto response
- Works with existing tooling (SIEM, SOAR, IAM, etc)

Reveal security

TrackerIQ - Identity Threat Detection & Response

Continuously analyze behavior in application environments to accurately detect threats



TrackerIQ ITDR

ATO Attacker

Insider

Prevention

PAM	IAM
MFA	SSPM
SSO	CIEM
CASB	UEBA

Identity Threat

Applications

Microsoft, salesforce, SAP, okta, box, slack, aws, Dynamics 365, servicenow, Azure

App Behavior

Detection

- Continuously Monitor and Analyze Identity Behaviors
- Detect and Alert on Anomalous Behavior

Response

- SOC Receives High Fidelity Alerts with Deep Context
- Automated Responses

Reveal security

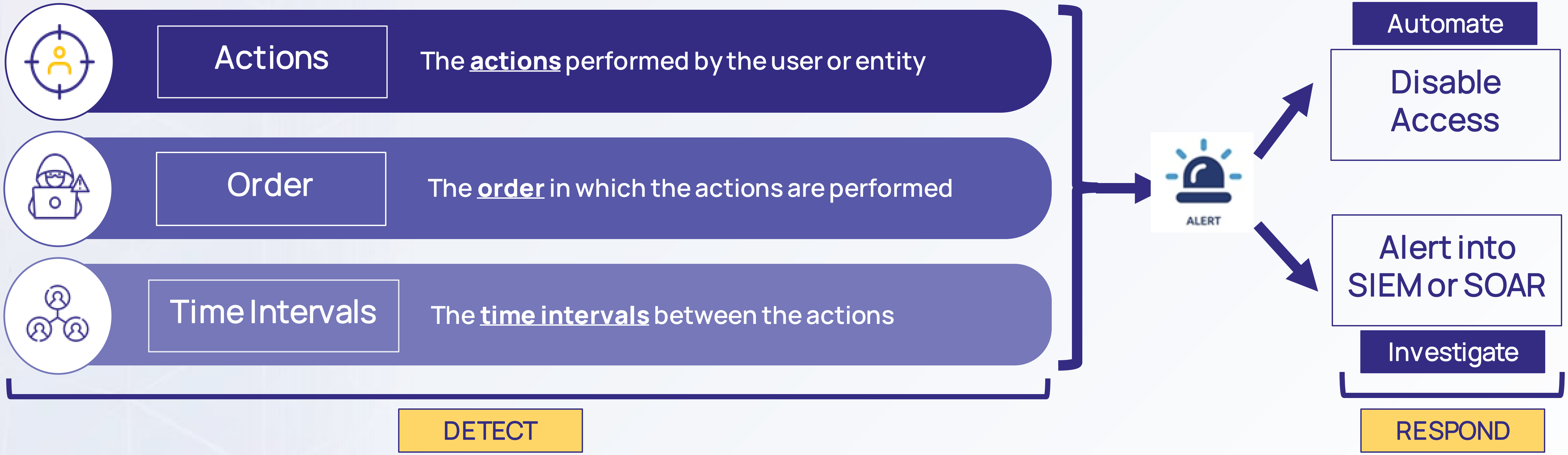
Identity Journey Analytics™

Behavioral Analytics

A single identity threat detection solution that works with human users, privileged users, APIs and other entities, to protect against:

- Account Takeover
- Insider Threats
- Third-Party Risk
- Fraud

How it Works……….



Actions — The **actions** performed by the user or entity

Order — The **order** in which the actions are performed

Time Intervals — The **time intervals** between the actions

DETECT

ALERT

Automate

Disable Access

Alert into SIEM or SOAR

Investigate

RESPOND

Reveal security

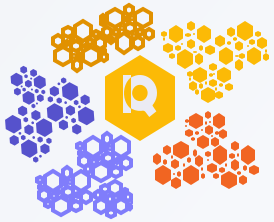
> “We saw something that with **the standard tools we weren’t able to see,** and in this case it was something that permitted us to be more proactive.
>
> We saw the anomaly starting before creating damage."

Nicola Sotira
CERT | Posteitaliane Group

Posteitaliane

Case Study: Detecting Imposters with malicious intent

40M	events/month (125,000 users)
7,000	behavior profiles
500	events/month Risk > 75%
60	events/month Risk >90%



Data clustering

Analysts can focus on a small number of accurate & high-risk alerts

Economic Value

Bolster Identity Threat Detection, While Saving Time and Costs

Maximum protection

Detect threats that rules-based detection solutions are blind to.

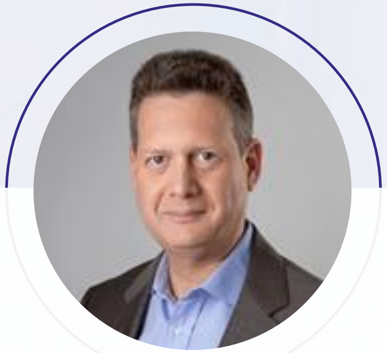
A more efficient SOC

Highly accurate alerts improve SOC agility and minimize the time chasing false positives.

Lightning-fast time to value

No installation required and measurable results in just a few short days.

Leadership Team



Doron Hendler

CEO & CO-FOUNDER

NICE TRIVNET SURF mPrest

Dr. David Movshovitz

CTO & CO-FOUNDER

f5 salesforce

Scott Schneider

CRO

McAfee cyberGRX BITSIGHT FireEye iSIGHTPARTNERS

Christy Lynch

CMO

deepwatch Checkmarx CYBERARK

Board of Directors

Alon Lifshitz

Hanaco Venture

Charlie Federman

Silvertech Venture

Patrick Heim

SYN Ventures

Jim Pflaging

Independent Board Member

ADVISORS

Charles Blauner

Frmr Global Head of
Information Security, Citi

Sounil Yu

Frmr Chief Security Scientist
Bank of America

Jim Routh

Frmr CISO,
MassMutual

Gary Owen

Fmr CISO
Wells Fargo, Current CISO
iCapital

Reveal security

Thank You

Doron Hendler

CEO and Co-Founder, Reveal Security

doron@reveal.security

Reveal security