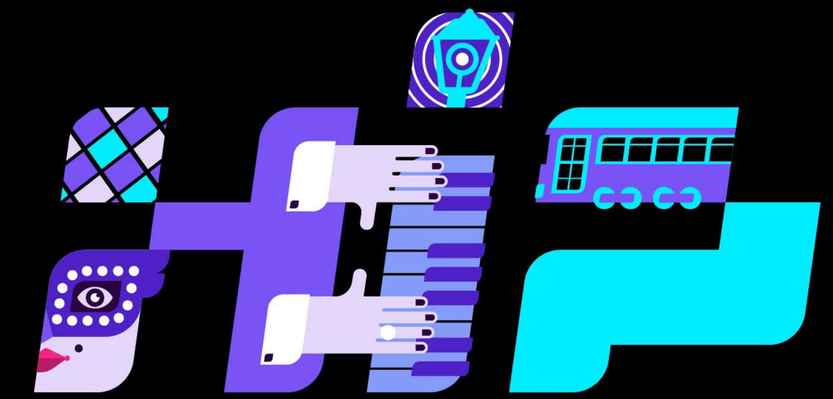
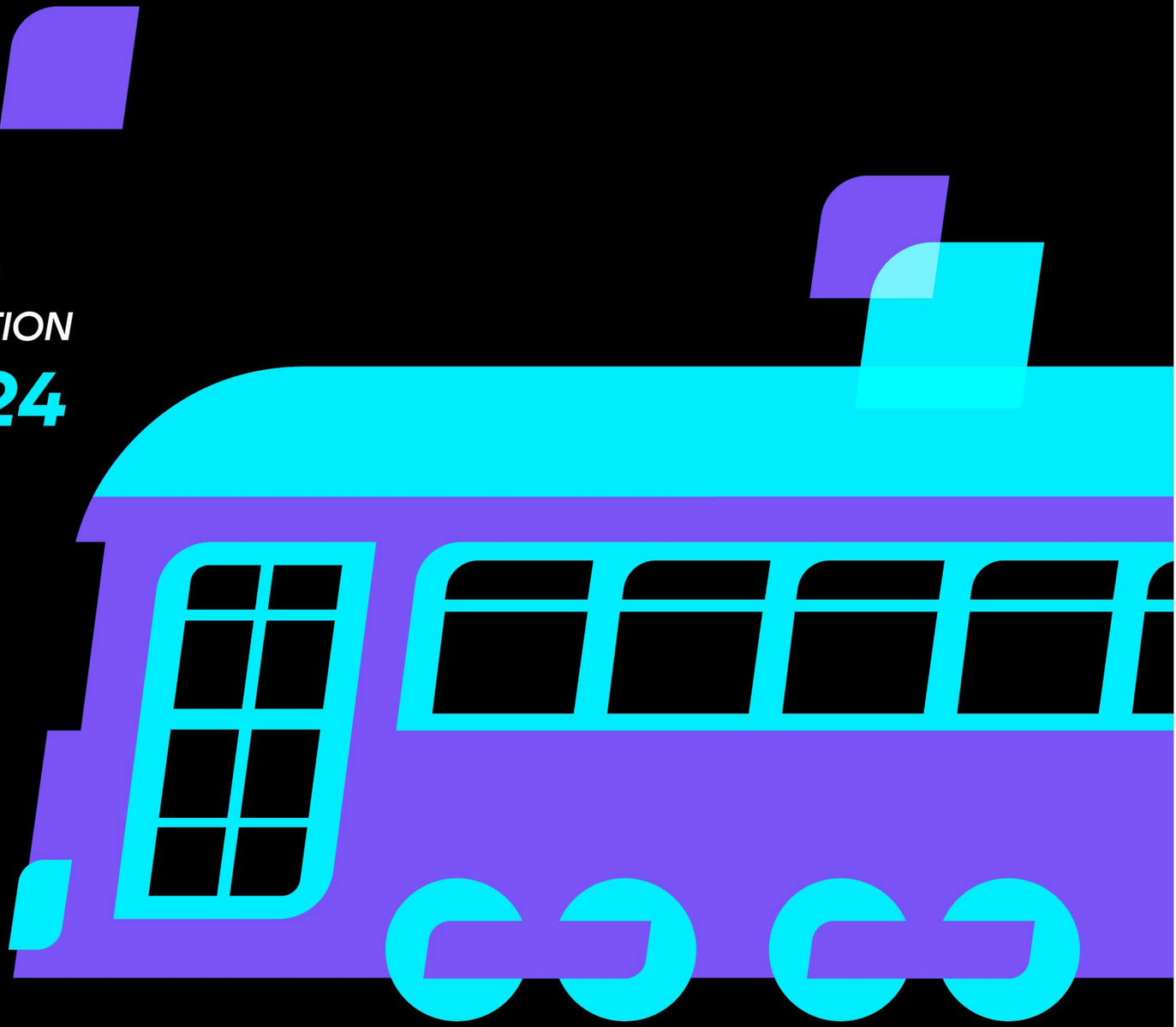


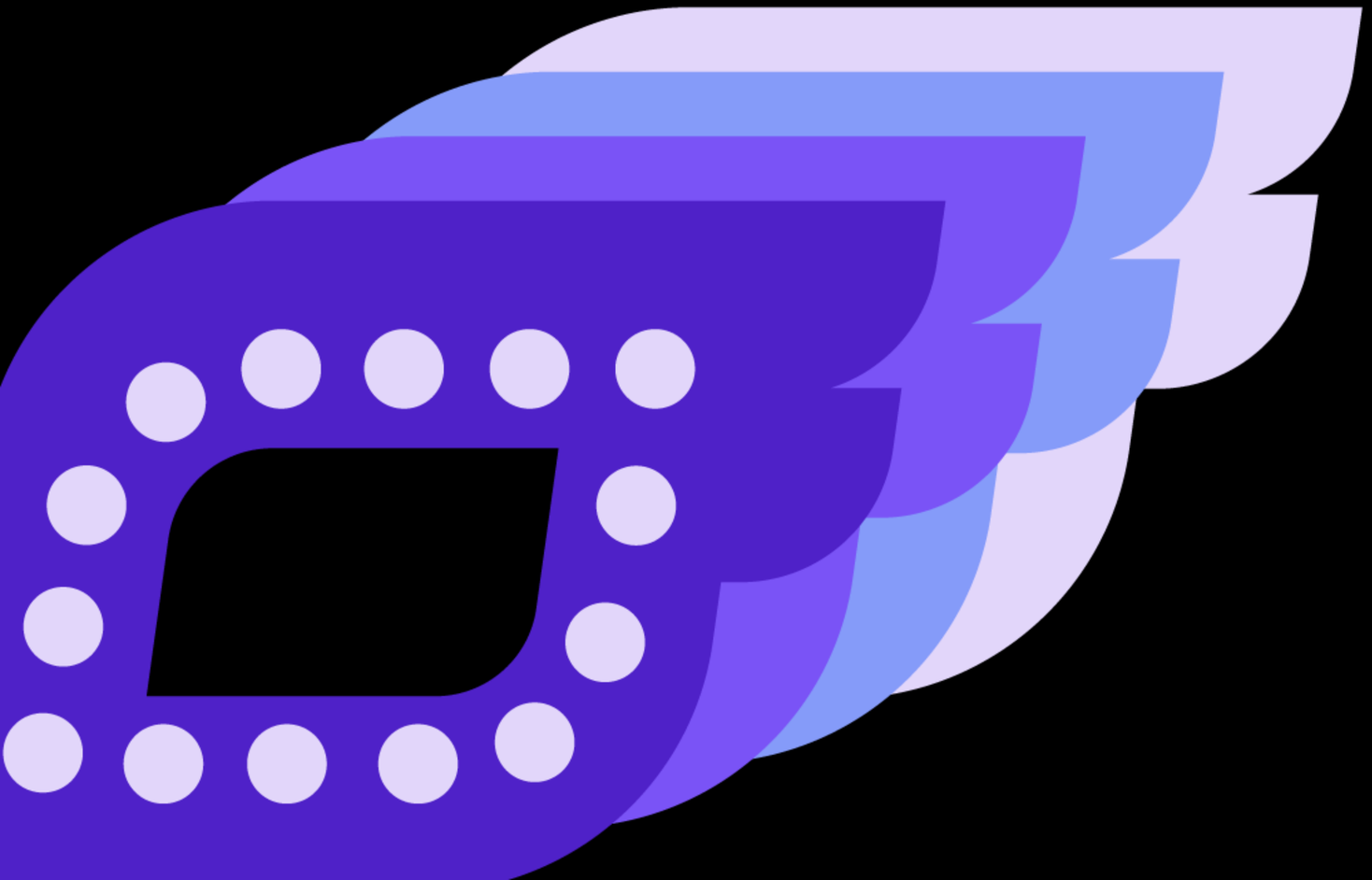
HYBRID
IDENTITY
PROTECTION

conf24

NEW ORLEANS



HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS



Prevention Alone Isn't Enough:

How EDR and ITDR Provide Layered Defense Against Identity-Based Attacks

Darren Mar-Elia
VP of Products, Semperis
Karan Sondhi
VP and CTO Public Sector, Trellix

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Darren Mar-Elia

VP of Products, Semperis

Darren is VP of Products at Semperis. He was a 14-time Group Policy Microsoft MVP and has a wealth of experience in Identity and Access Management and information security. Previously, he was the CTO and founder of SDM Software, a provider of Microsoft systems management solutions. Prior to launching SDM, Darren held senior IT infrastructure architecture roles in Fortune 500 companies and was also a CTO of Quest Software. Darren has written and spoken on Windows networking, Active Directory and Group Policy, and cybersecurity and was a Contributing Editor for Windows IT Pro Magazine for 20 years.

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Karan Sondhi

VP and CTO – Public Sector, Trellix

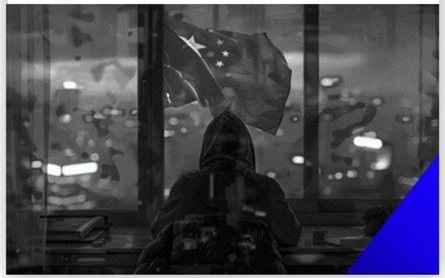
Karan Sondhi is Trellix's Vice President and Chief Technology Officer. Karan has over two decades of experience in the DoD and Intelligence Community. His most recent experience was serving as CTO for Microsoft’s $10 Billion JEDI contract with the DoD. Before Microsoft, Karan spent 12 years leading and executing innovation efforts in Cybersecurity, Blockchain, and Automated Machine Learning at the Central Intelligence Agency (CIA).

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Recent Threats

China increases attacks:

China-linked threat groups generate nearly 70% of all detections.



Shifting ransomware ecosystem:

Global law enforcement action to disrupt ransomware gang LockBit has led to copycats and a shifting ecosystem.

EDR evasion:

An EDR evasion tool called “Terminator” from cybercriminal developer Spyboy was used in a new campaign targeted at the telecom sector.

GenAI usage by cybercriminals:

Free ChatGPT 4.0 Jabber tool allows threat actors to adopt GenAI into their operations and to create a GenAI knowledge base.

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Market Trends

68%

of organizations experienced one or more endpoint attacks that successfully compromised data and/or the IT infrastructure

Source: Ponemon Institute

86%

of cyber attacks involve stolen credentials

Source: Google Cloud's Threat Horizons Report

80%

of successful breaches are new or unknown "zero-day" attacks

Source: Ponemon Institute

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

WIDESPREAD ATTACKS

In the attackers' crosshairs

Active Directory has become a **prime target** for business-crippling attacks in recent years. And on-premises AD is increasingly used as a stepping-stone to access cloud environments.

READ THE 2024 RANSOMWARE RISK REPORT

- SOLARWINDS 2020
- NTT COMMUNICATIONS 2020
- COLONIAL PIPELINE 2021
- MICROSOFT EXCHANGE 2021
- KASEYA 2021
- MAERSK 2017
- OLYMPUS 2021
- JBS 2021
- IRELAND HEALTH SERVICES 2021
- OLDSMAR, FLORIDA 2021

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

A Powerful Partnership

Unified detection across endpoint and identity systems:

- Detect threats across endpoints and Active Directory (AD) environments in real time
- Correlate security alerts from identity systems and endpoints to prevent lateral movement

Automated incident response for faster recovery:

- Automatically isolate infected endpoints and roll back malicious AD changes
- Reduce downtime and prevent manual remediation delays with workflow automation

Comprehensive security visibility:

- Centralized view of endpoint activities and AD modifications in a single pane
- Improve SOC efficiency by prioritizing the most critical alerts

Post-attack forensics and continuous monitoring:

- Identify attack vectors quickly and secure compromised identities
- Roll back unauthorized changes and ensure minimal operational disruption

80% of breaches involve credential abuse

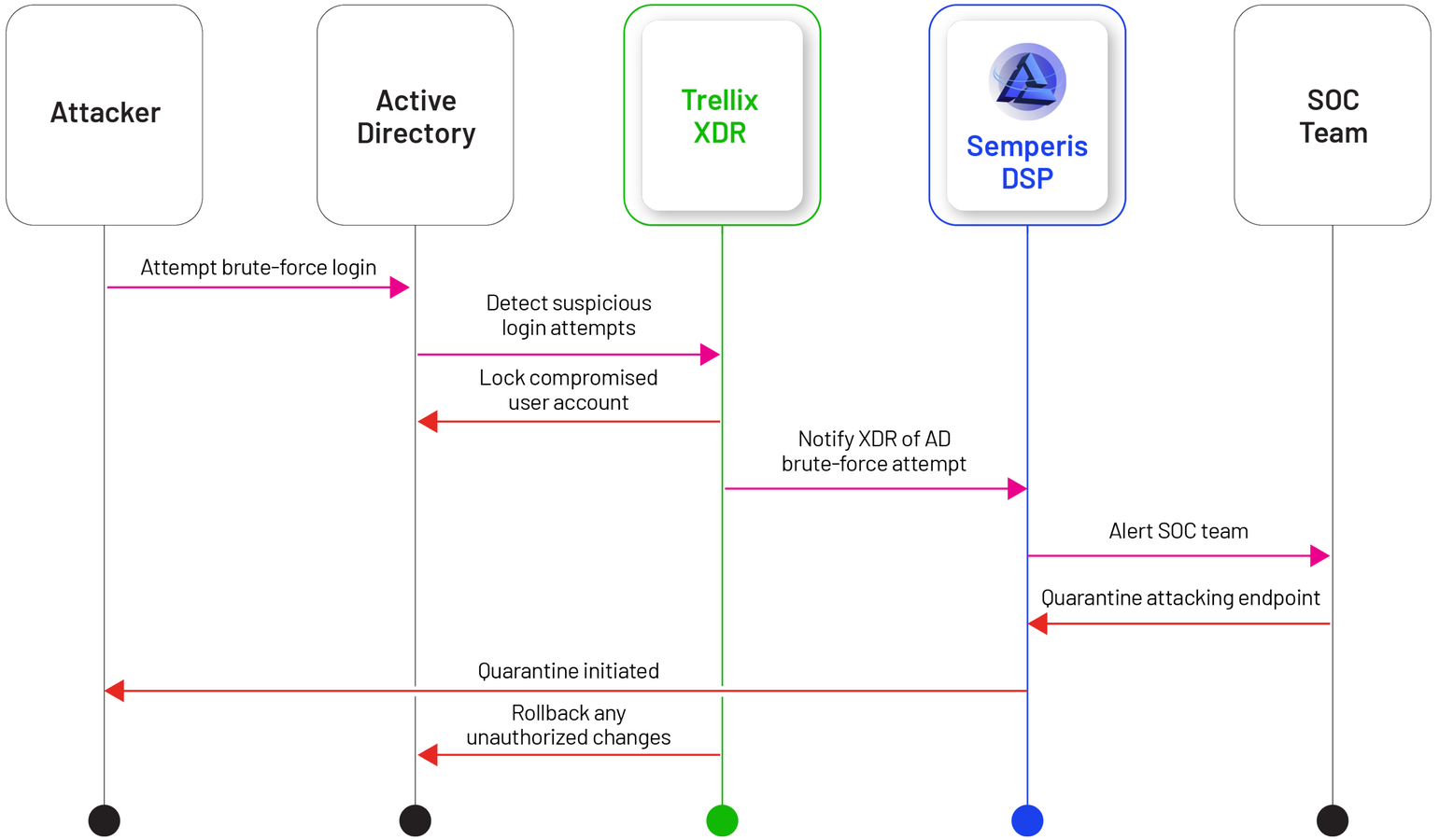
AD security is now more critical than ever

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS


#1: Automated response for Active Directory threats

Summary: Trigger automated workflows in Trellix XDR based on critical AD events detected by Semperis DSP, such as brute-force attacks, password spraying attacks or unauthorized privilege escalations.

Scenario: A brute-force login attempt is detected on AD, and Trellix XDR quarantines the endpoint attempting the attack while Semperis DSP locks the compromised user account and rolls back any changes.

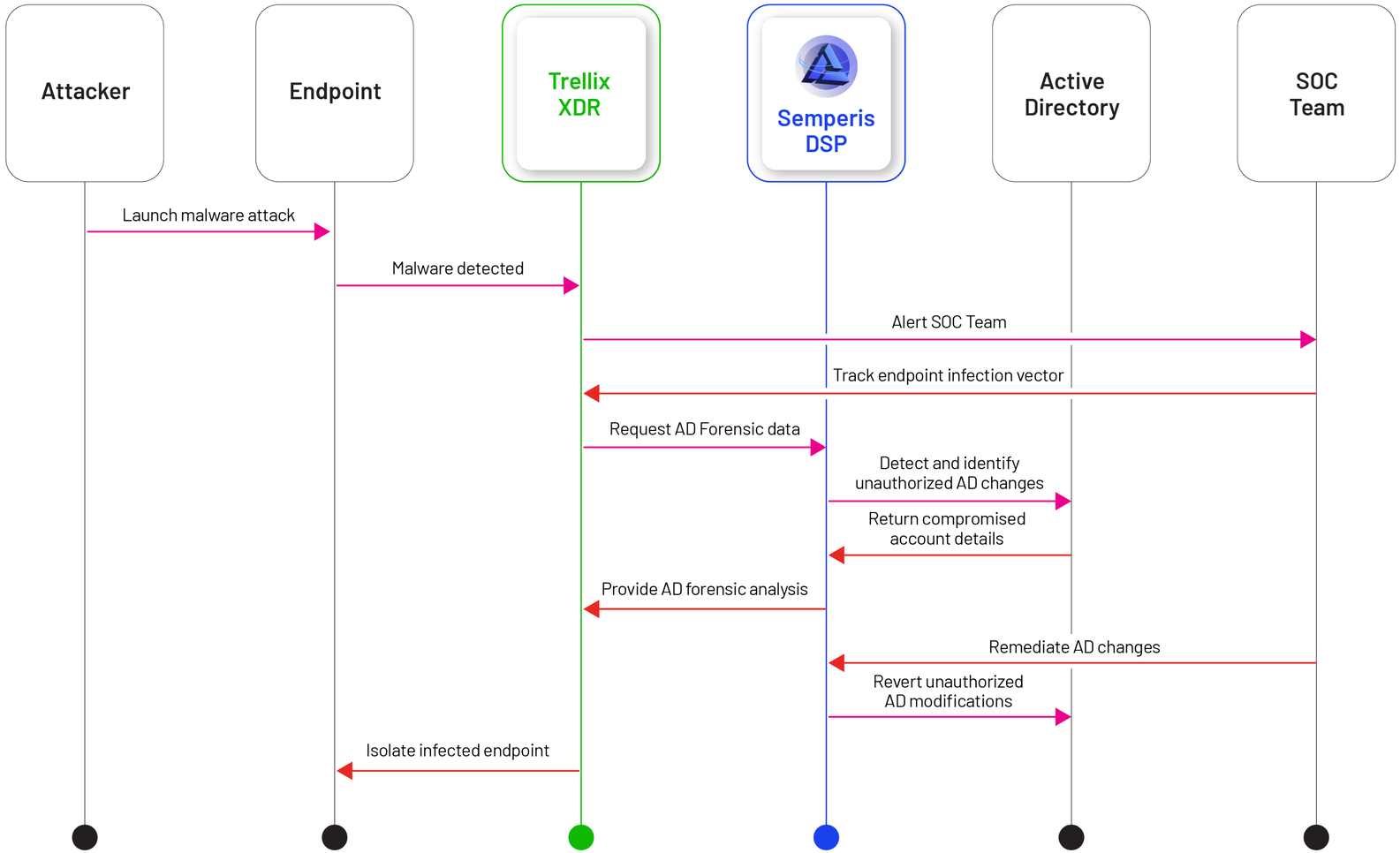


HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS


#2: AD post-attack forensics and response automation

Summary: After an attack, use Trellix XDR to track the initial attack vectors on endpoints, and Semperis DSP to identify and remediate AD changes.

Scenario: A malware attack results in a compromised endpoint that escalates privileges in AD. Trellix XDR uncovers the source of the infection, while Semperis DSP reverts unauthorized AD changes and secures critical assets.



HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

What We Just Saw

Unified security solution:

- Trellix XDR and Semperis DSP deliver end-to-end protection—from the **endpoint to identity systems**

Advanced identity threat detection and response (ITDR):

- Real-time detection of AD/Entra ID compromises and **automated response** workflows to stop threats

Automated recovery and rollback:

- Quickly recover from unauthorized changes with **AD rollback capabilities**—minimizing downtime and damage

Faster incident response:

- AI-driven threat detection prioritizes critical alerts, accelerating **containment and resolution**

Comprehensive security monitoring:

- Continuous visibility into AD activities and integration with XDR for **faster detection of complex threats**

Post-breach forensics and analysis:

- Understand attack vectors and **remediate identity-based threats** to prevent future incidents

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

> “In the world of cybersecurity, identity is the new perimeter and business leaders are taking notice. Semperis is on the cutting edge of identity security, protecting critical Tier 0 IT infrastructure like Active Directory and Entra ID that global enterprises trust as primary identity systems.”

Malcolm Turnbull
Former Australian Prime Minister
Semperis Strategic Advisor

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

37-Year Heritage

1987 — McAfee founded

1996 — McAfee acquired FSA Corp

1998 — McAfee acquired Foundstone, FIREEYE founded

2004 — McAfee Security Innovation Alliance launched

2007 — McAfee integrated with Intel Security Division

2011 — FireEye acquired MANDIANT

2013 — McAfee independent, acquired Skyhigh Networks

2017 — McAfee public, FireEye acquired Cloudvisory

2020 — McAfee and FireEye combined by Symphony Technology Group

2021 — Trellix founded

JAN 2022 — Soulful Work launched

MAR 2022 — Sister company Skyhigh Security founded

SEP 2022 — Trellix Xtend Palma appointed to NSTAC, Xtend Partner program launch

FEB 2023 — Trellix Endpoint Security Suite and Global Threat Intel aaS launch, Trellix XDR achieved FedRAMP High ATO

APR 2023 — aws expanded integrations

MAY 2023 — AI and CISO community launch

JUL 2023 — Great Place To Work. Certified 2023 — Great place to work certified in US

SEP 2023

DEC 2023 — Trellix Ransomware Detection and Response solution launch

FEB 2024 — IDC names Trellix as Modern Endpoint Security Leader

Rich History of Machine Learning & Artificial Intelligence

2014 — Created analytics such as Impossible Travel

2016 — Launched Guided investigations

2016 — Launched NextGen EPP with ML

2023 — Launched AI driven auto investigations

HYBRID IDENTITY PROTECTION conf24
NEW ORLEANS

Thank You

Questions?