Detecting, Understanding & Responding to Cyber Attacks

Paris Kaskas

Cyber Security Consultant, Greece, Cyprus & Malta

Infocom Security April 11th, 2024

SCAN ME

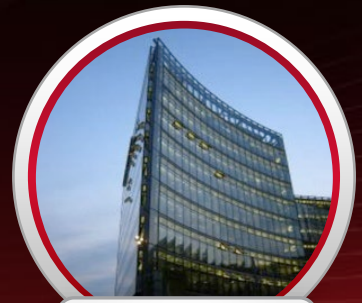
Trend Micro

- **35 years** focused on security software
- Headquartered in **Japan**, Tokyo Exchange Nikkei Index
- Annual sales over **$2B**
- Customers include **45 of top 50 global** corporations
- **7000+** employees in over **65 countries**

500k commercial customers &
250M+ endpoints protected

Eva Chen, CEO and Co-founder of Trend Micro

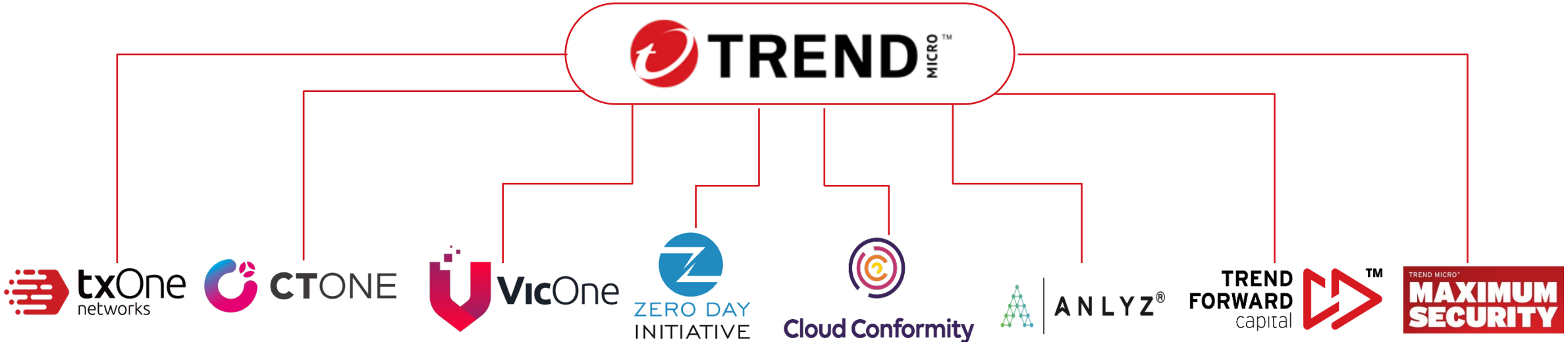
Enterprise



Midsize Business

Small Business

End-To-End Cybersecurity Industry Group



OT/IOT Security	5G/6G & Telco tower Security	Autonomous Vehicle Security	Threat Intelligence, Vulnerability Research & Bug Bounty	Cloud Security & Compliance	SOC, SIEM, SOAR	Venture Capital & CySec Startup Investment	Consumer Seucirty & Home Network Security Devices

Rising Complexity & Scale of Attack Surface

Security Tool Sprawl

40

Avg. Number of tools in SOC*

Data Lakes with duplicated security telemetry

Overlapping solutions

Data lake & cost proliferation

Poorly integrated

People costs rising

Challenging to measure effectiveness

*SAPIO Research –commissioned by Trend Micro, 2021

TREND MICRO

Overwhelmed security teams

Too many alerts

Where to **focus?**

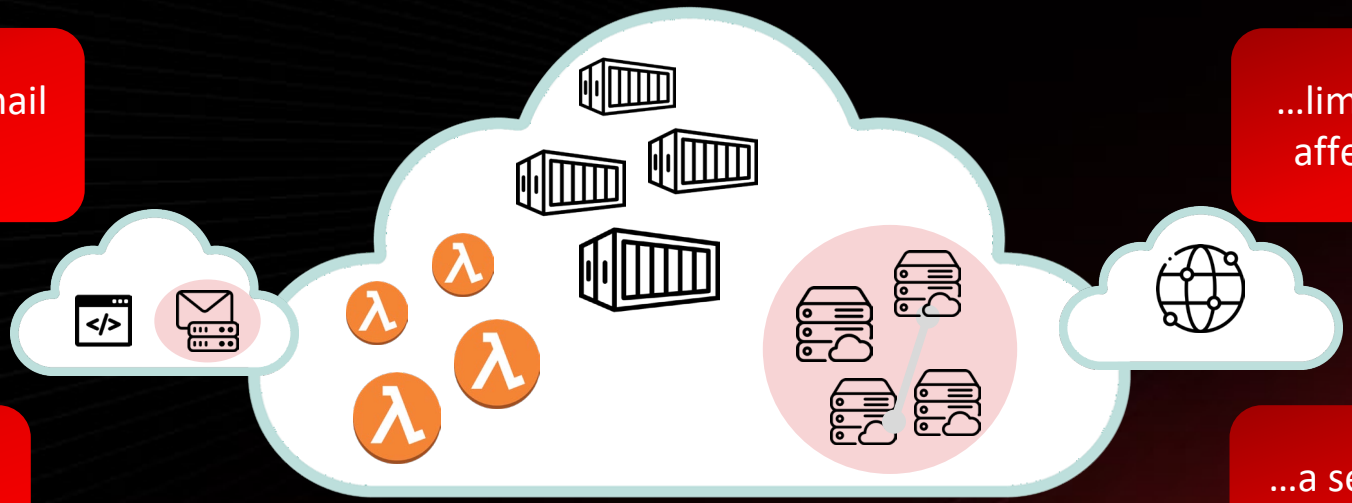
What to **prioritize?**

Skills shortage

Siloed Telemetry

…and little visibility into email traffic and mailboxes

…limited visibility to threats affecting cloud workloads



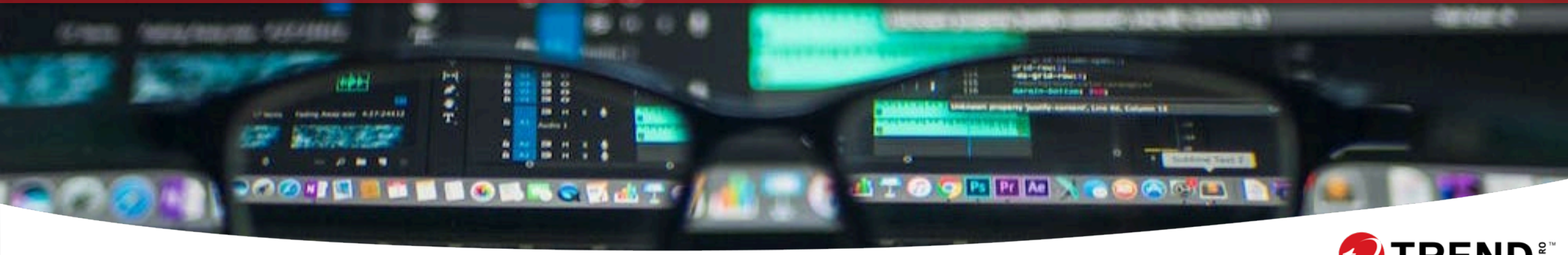
Today, the SOC gets siloed insight into endpoints (EDR)…

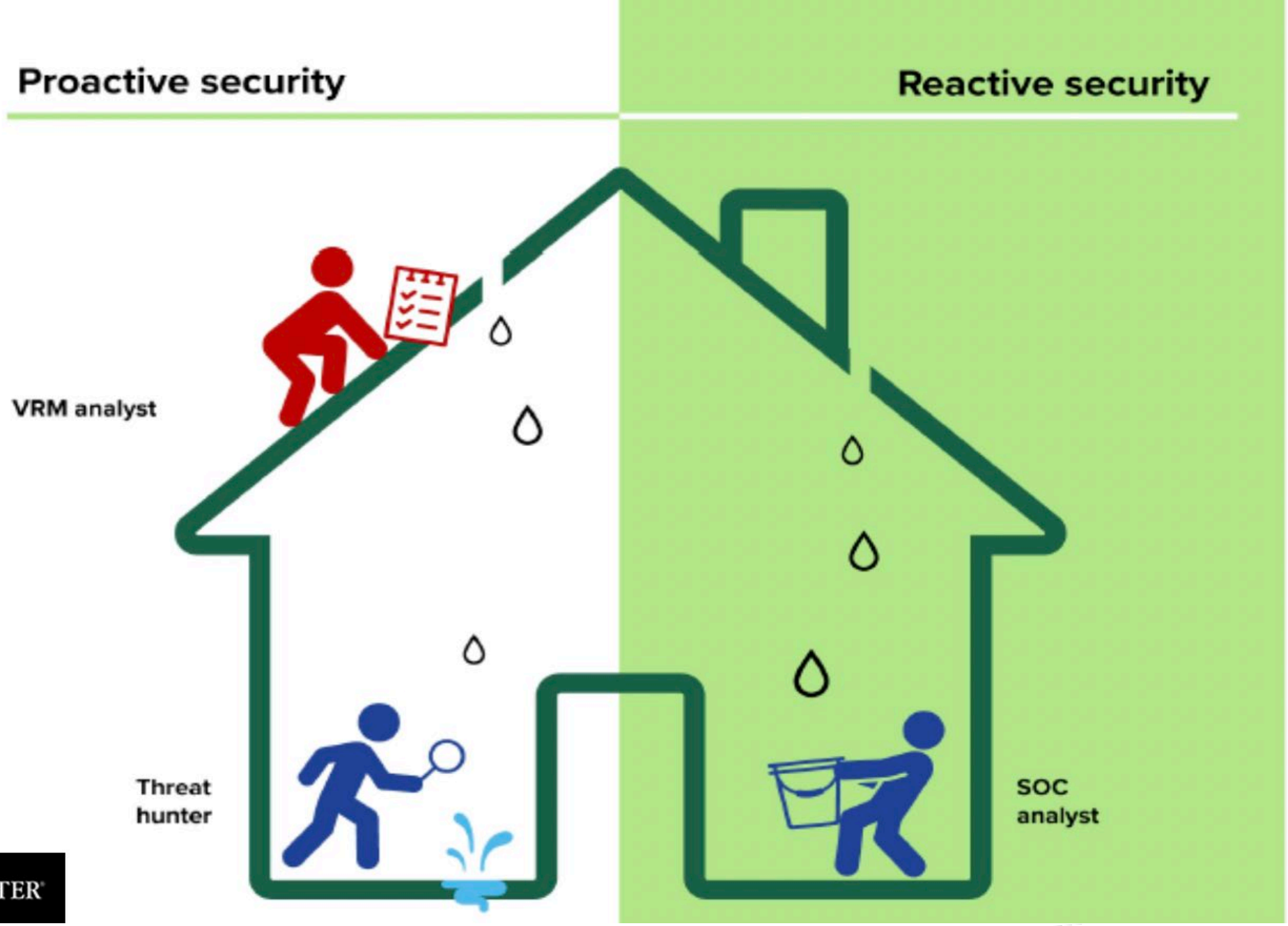
…a separate siloed view into network events,

SecOps

But You Can’t Defend What You Don’t Know About

69% of organizations have experienced some type of cyberattack in which the attack itself started through the exploit of an unknown, unmanaged, or poorly managed internet-facing asset





FORRESTER®

TREND MICRO™


Reactive
Proactive

TREND Vision One | Attack Surface Risk Management (ASRM)

Proactive

- Discovering All Assets
- Assessing Cyber Risk
- Prioritizing Risk Mitigation
- Mapping Relationships
- Classifying and Tagging Assets with AI
- Analyzing Compliance

TREND Vision One | Extended Detection and Response (XDR)

Responsive

- Correlating Attacks Cross-Layers
- Coordinating Response Cross-Vendors
- Sweeping with New Threat Intel
- Powerful Hunting and Forensic Tools
- Augmenting Staff with Companion AI
- Automating Security Response

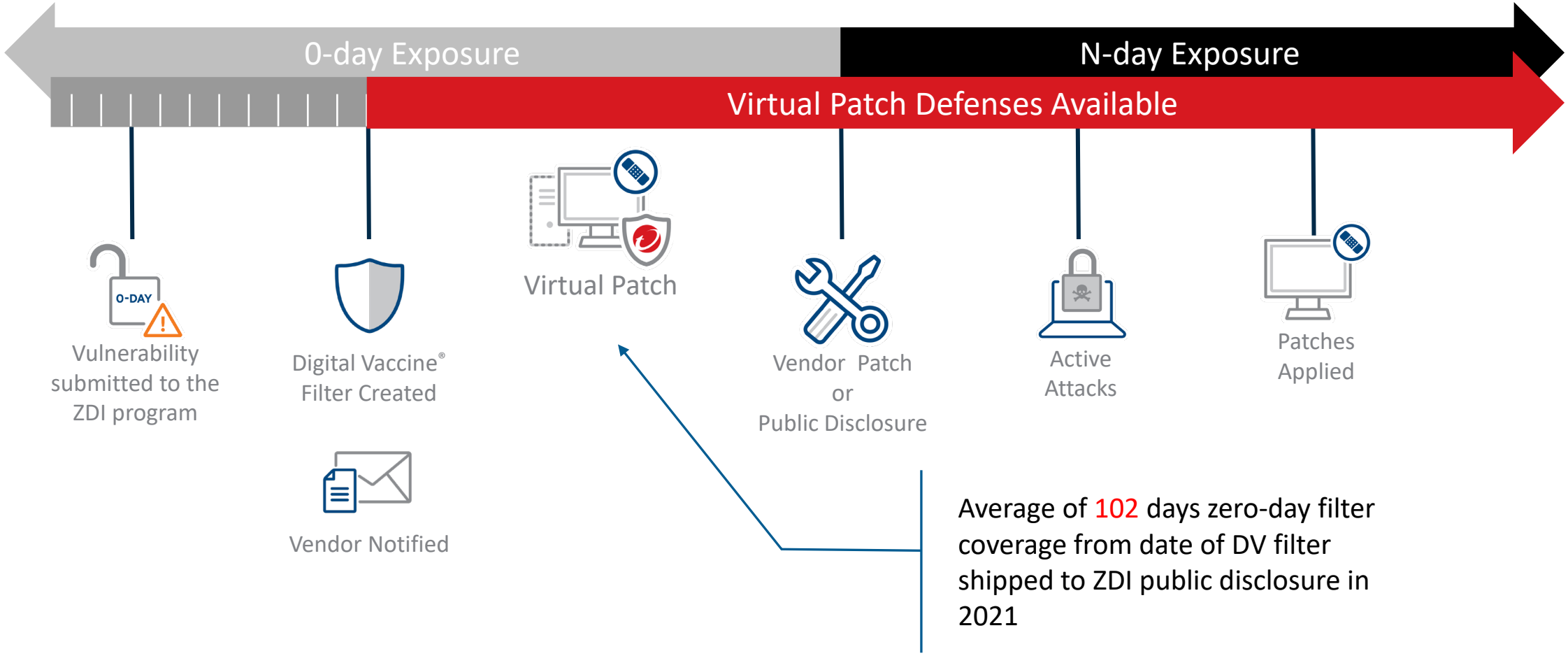
TREND Vision One | Data Lake

Detection Logs and Activity Data

Endpoint	Identity	Email	Cloud	Network	Data	OT	3rd Party
+ Protection	+ Protection	+ Protection	+ Protection	+ Protection	+ Protection	+ Protection	

Broadest Coverage with Native Sensors

Trend Micro's Unique Position with Vulnerabilities – Virtual Patching



Attack Surface Risk Management

- Complete attack surface visibility
- Compiled though third-party connections, security products, and network telemetry
- Automatically de-duplicates assets across multiple data sources
- Classifies and tags assets automatically, establishing criticality and a baseline
- Analyzes compliance

Why Extend XDR to Email?

98% of malware infection source

Detect: Are there compromised accounts sending internal phishing emails? Automatic sweeping of mailboxes

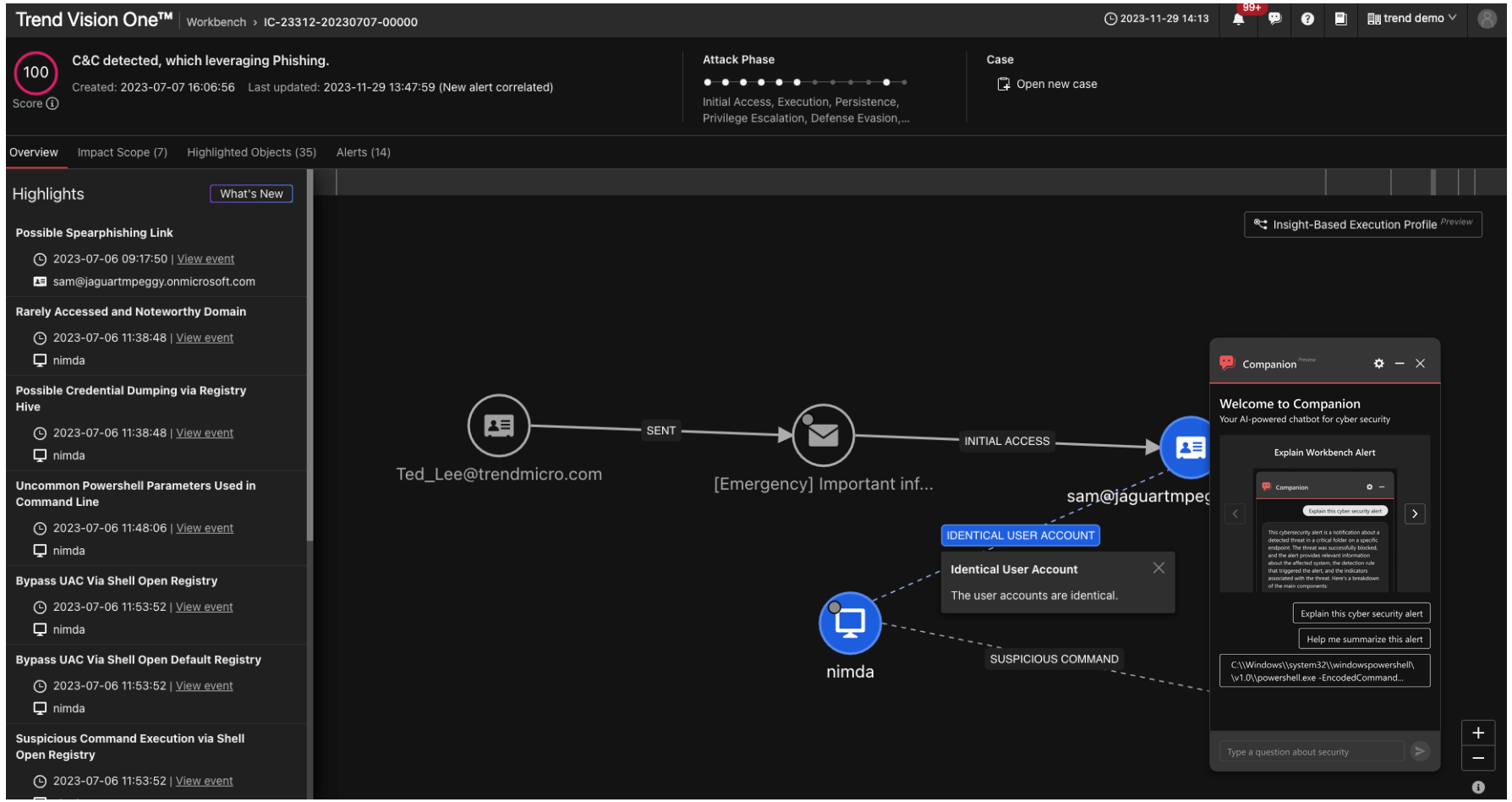
Investigate: Who else received this email / threat?

Respond Examples: Quarantine email, delete email, add to block list

Malware Infection Source

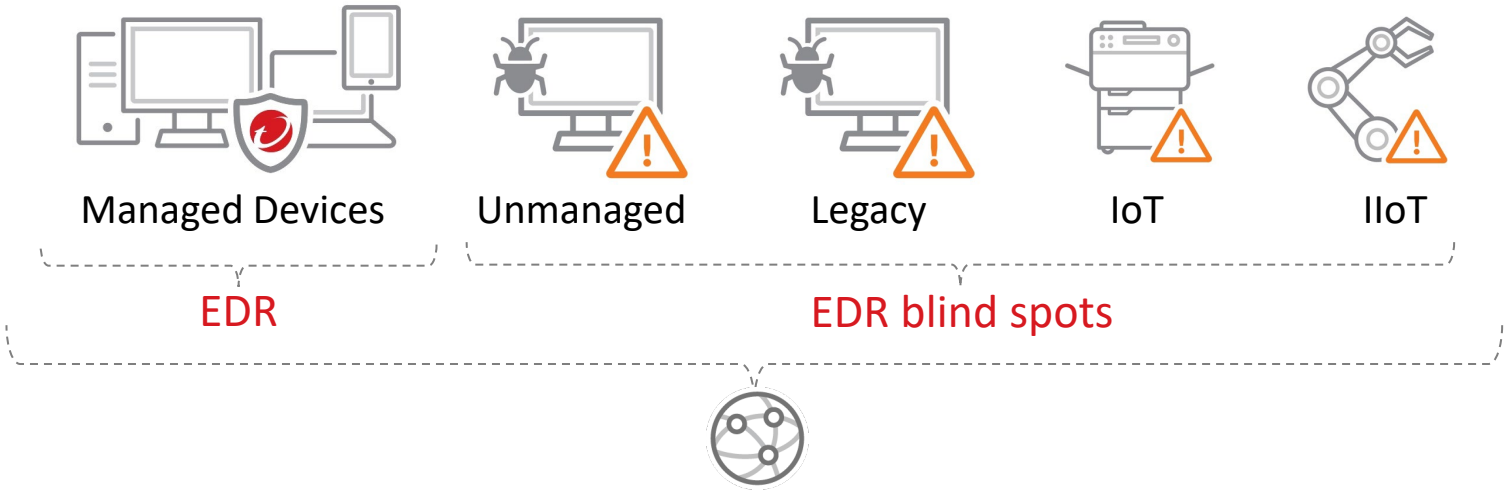
Source: Verizon Data Breach Investigations Report, 2023

Insight-based view



Better layout and more details to improve AX

Why Extend XDR to your Network?



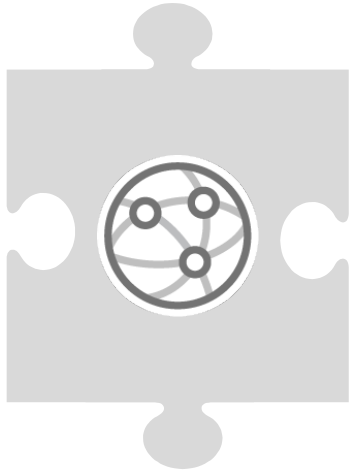
Activity Data:

- Traffic Flow
- Perimeter and Lateral Connections
- Suspicious Traffic Behaviors

Detect: See across the network including EDR blind spots. Analytics discover complex threats. IOC sweeping.

Investigate: How is a threat communicating? How is the attacker moving across the organization?

Respond Examples: Block host, block URL, disable account (Azure AD).



Use case – network forensic and hunting

See your network's unmanaged attack surface

Faster detection and response with network forensics

TREND MICRO™ Vision One

Single Platform

Centralized visibility and management with unified protection, detection, and response.

Extended Detection and Response (XDR)

User and Identity | Email | Endpoints and Servers | Cloud Infrastructure | Applications | Code Repository | Data | Network | 5G | ICS/OT

Email Security | **Endpoint** Security | **Cloud** Security | **Network** Security | **Data** Security | **Identity** Security

Risk Mitigation • IT Automation — **Orchestration and Automation** — Custom Playbooks • Case Management

Attack Surface Intelligence • Zero Day Initiative — **Global Threat Intelligence** — Threat Research • Big Data Analytics

AI Privacy and Ethics • AI Companion — **AI Native Foundation** — Generative AI • Custom LLM • Machine Learning

TREND MICRO™

Paris Kaskas

Cyber Security Consultant, Greece, Cyprus & Malta

Email: Paris_Kaskas@TrendMicro.com

Mobile: +30 6948661494

SCAN ME