DXC Cybersecurity

Na ceste k Agentic SOC

November 2025

© 2025 DXC Technology Company. All rights reserved.

DXC Public

DXC Security by the numbers

3,200+
cybersecurity professionals

450+
Global clients

13
security operations centers

200+
Threat intel & responder experts

30+
strategic alliances & partnerships

6 Global Languages
English, Spanish, Italian, French, Japanese , Chinese

+25
customer delivery centers

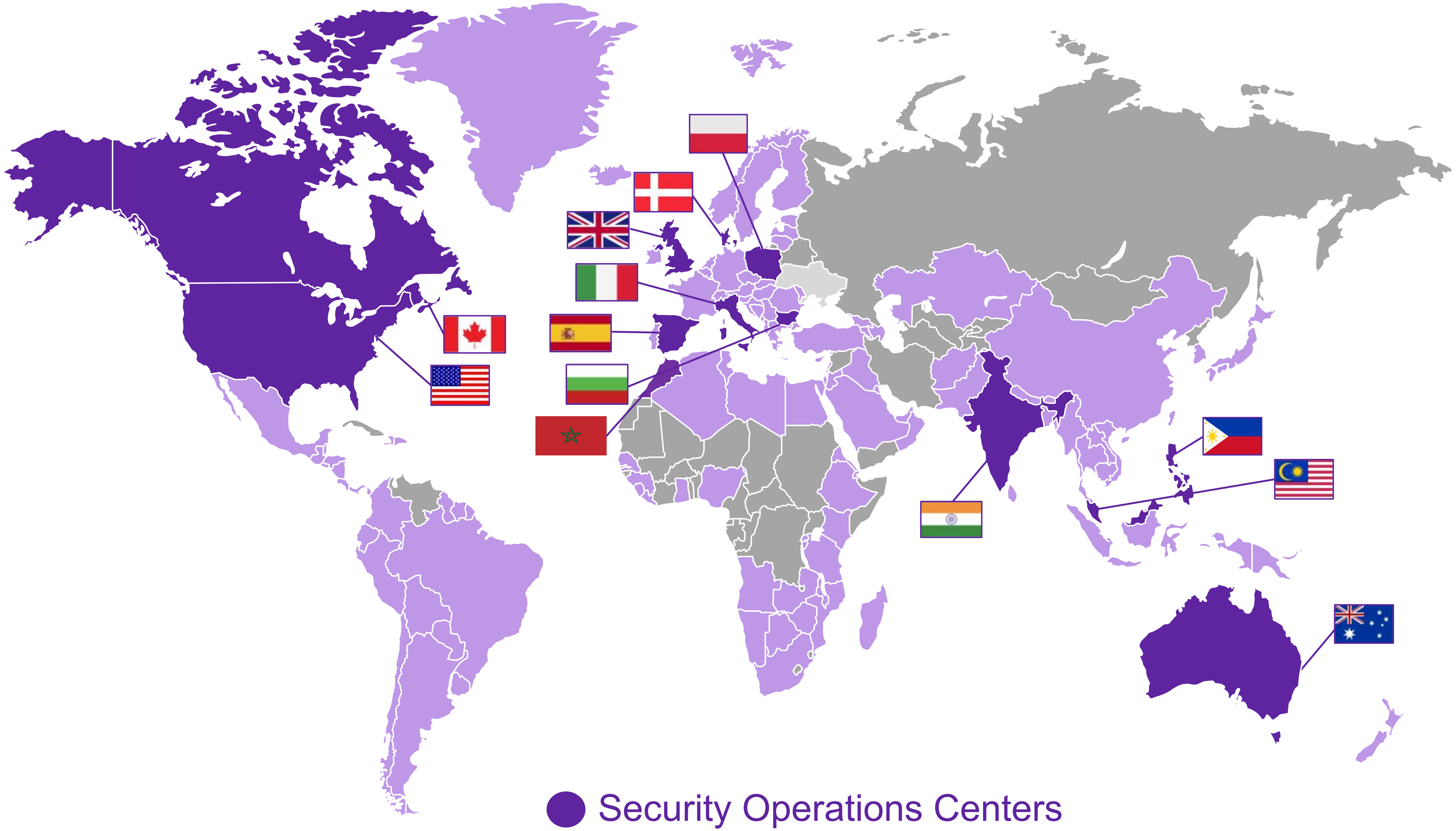
10+
Security offerings

Restricted
*

© 2025 DXC Technology Company. All rights reserved.

Global coverage

Three main regions: Americas, Europe, and APJMEA



● Security Operations Centers

500+
security professionals

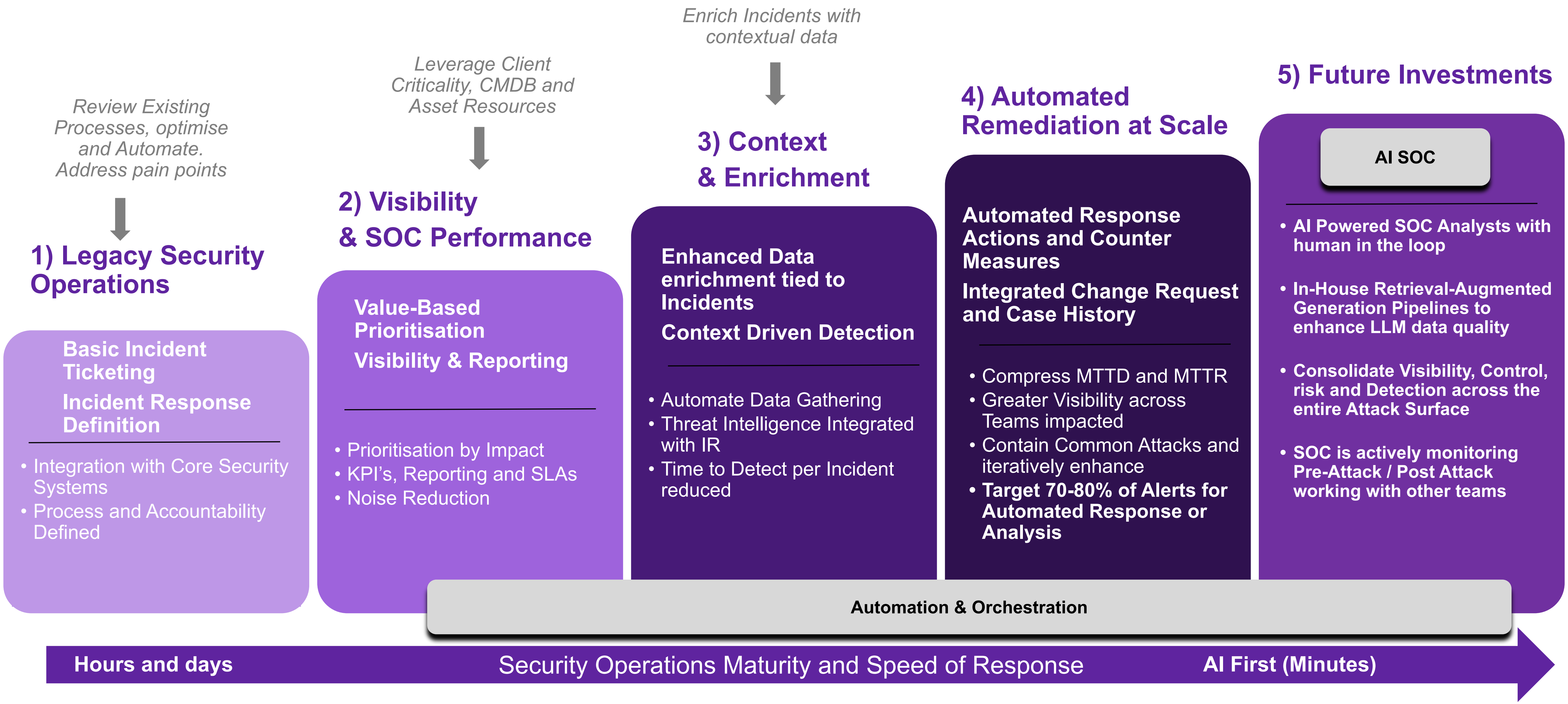
13
global security operations centers

24x7x365
security operations

© 2025 DXC Technology Company. All rights reserved.

DXC Confidential

Security Operations – Maturity Levels



Review Existing Processes, optimise and Automate. Address pain points

1) Legacy Security Operations

Basic Incident Ticketing

Incident Response Definition

- Integration with Core Security Systems
- Process and Accountability Defined

Leverage Client Criticality, CMDB and Asset Resources

2) Visibility & SOC Performance

Value-Based Prioritisation

Visibility & Reporting

- Prioritisation by Impact
- KPI’s, Reporting and SLAs
- Noise Reduction

Enrich Incidents with contextual data

3) Context & Enrichment

Enhanced Data enrichment tied to Incidents

Context Driven Detection

- Automate Data Gathering
- Threat Intelligence Integrated with IR
- Time to Detect per Incident reduced

4) Automated Remediation at Scale

Automated Response Actions and Counter Measures

Integrated Change Request and Case History

- Compress MTTD and MTTR
- Greater Visibility across Teams impacted
- Contain Common Attacks and iteratively enhance
- **Target 70-80% of Alerts for Automated Response or Analysis**

5) Future Investments

AI SOC

- **AI Powered SOC Analysts with human in the loop**
- **In-House Retrieval-Augmented Generation Pipelines to enhance LLM data quality**
- **Consolidate Visibility, Control, risk and Detection across the entire Attack Surface**
- **SOC is actively monitoring Pre-Attack / Post Attack working with other teams**

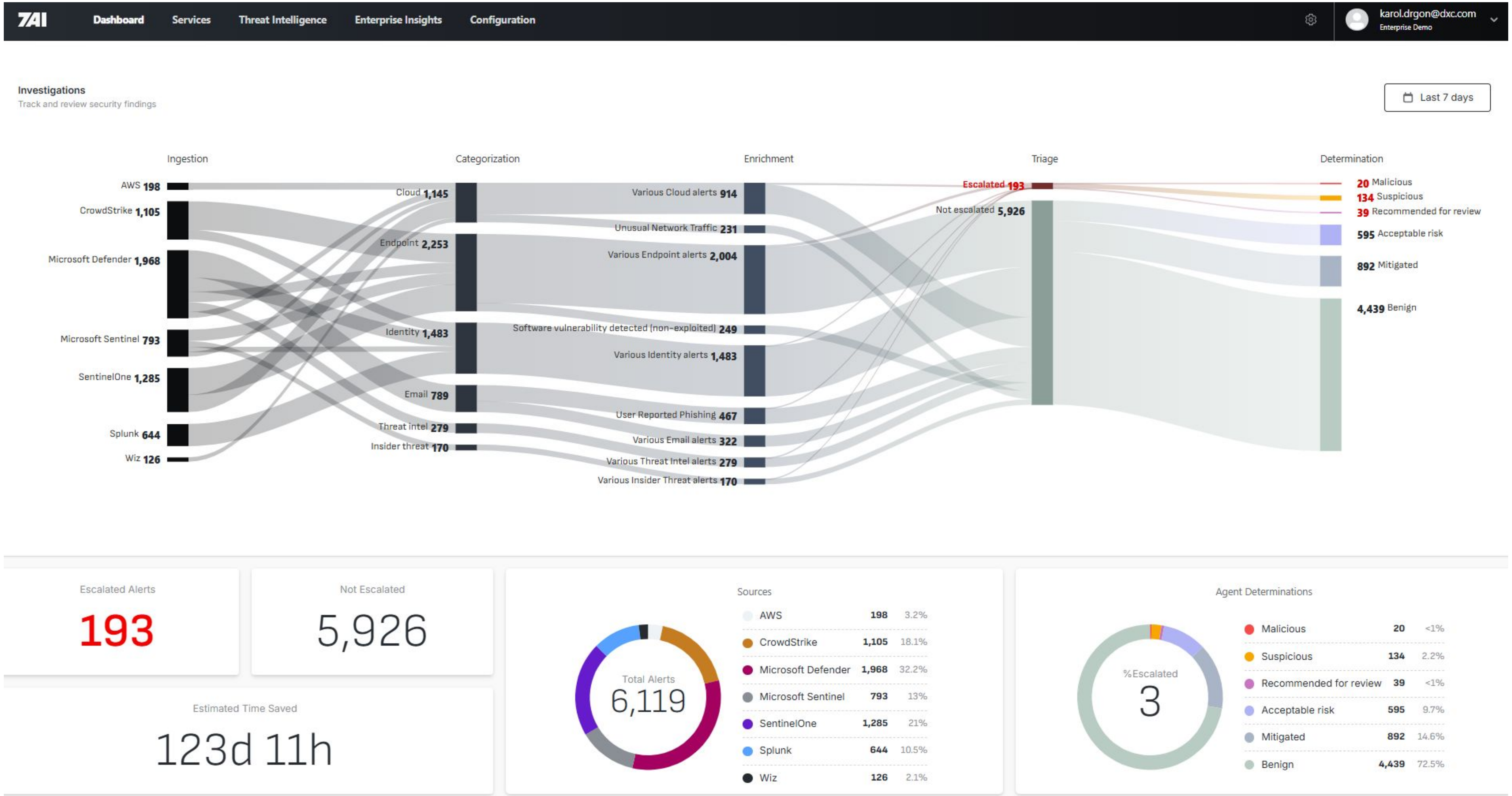
Automation & Orchestration

Hours and days Security Operations Maturity and Speed of Response **AI First (Minutes)**

© 2025 DXC Technology Company. All rights reserved.

DXC Confidential

DXC / 7AI Agentic SOC



Investigations

Track and review security findings

Escalated Alerts

193

Not Escalated

5,926

Estimated Time Saved

123d 11h

Sources

○ AWS	198	3.2%
● CrowdStrike	1,105	18.1%
● Microsoft Defender	1,968	32.2%
● Microsoft Sentinel	793	13%
● SentinelOne	1,285	21%
● Splunk	644	10.5%
● Wiz	126	2.1%

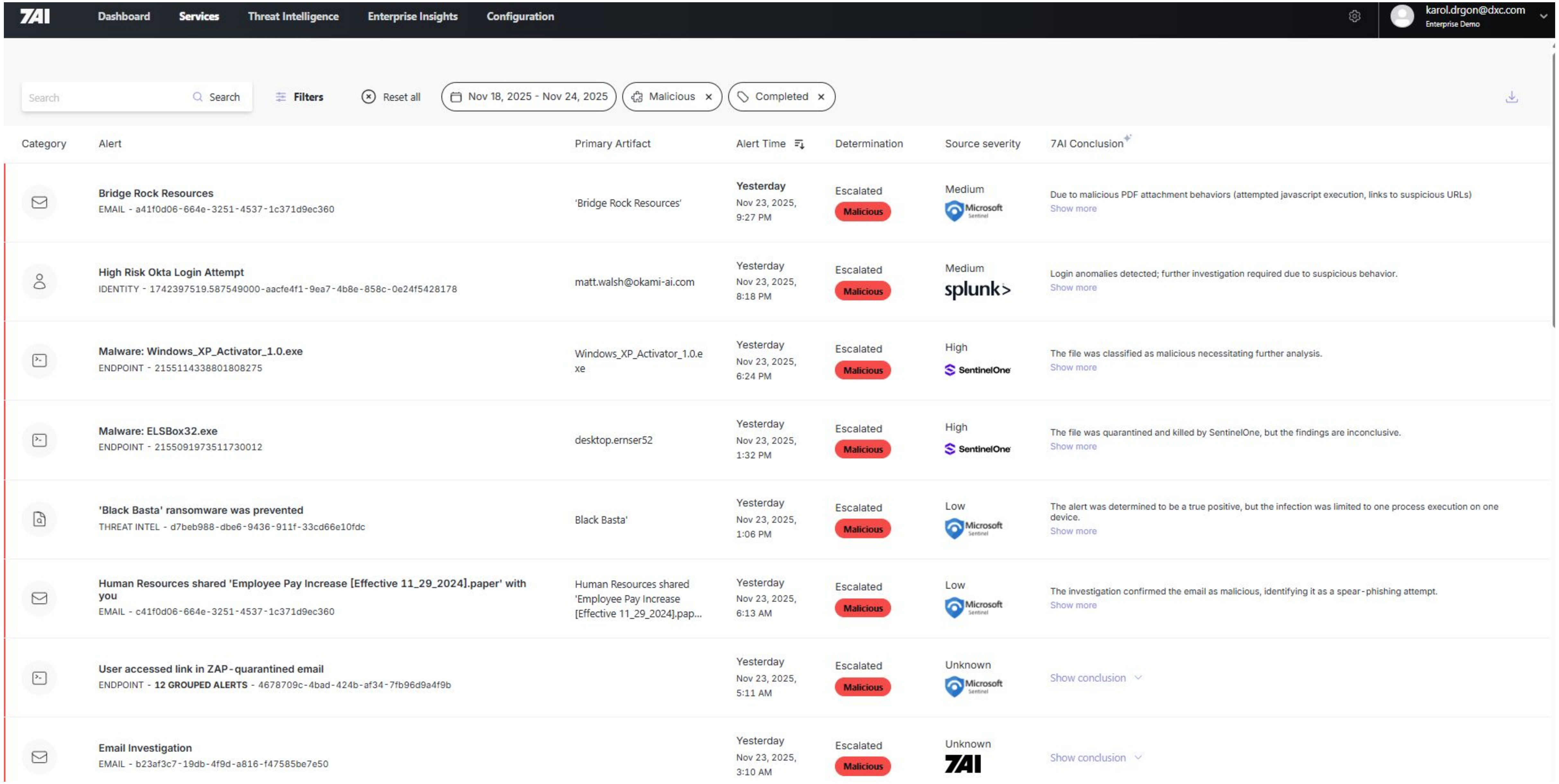
Agent Determinations

● Malicious	20	<1%
● Suspicious	134	2.2%
● Recommended for review	39	<1%
● Acceptable risk	595	9.7%
● Mitigated	892	14.6%
● Benign	4,439	72.5%

© 2025 DXC Technology Company. All rights reserved.

DXC Confidential

Incident view

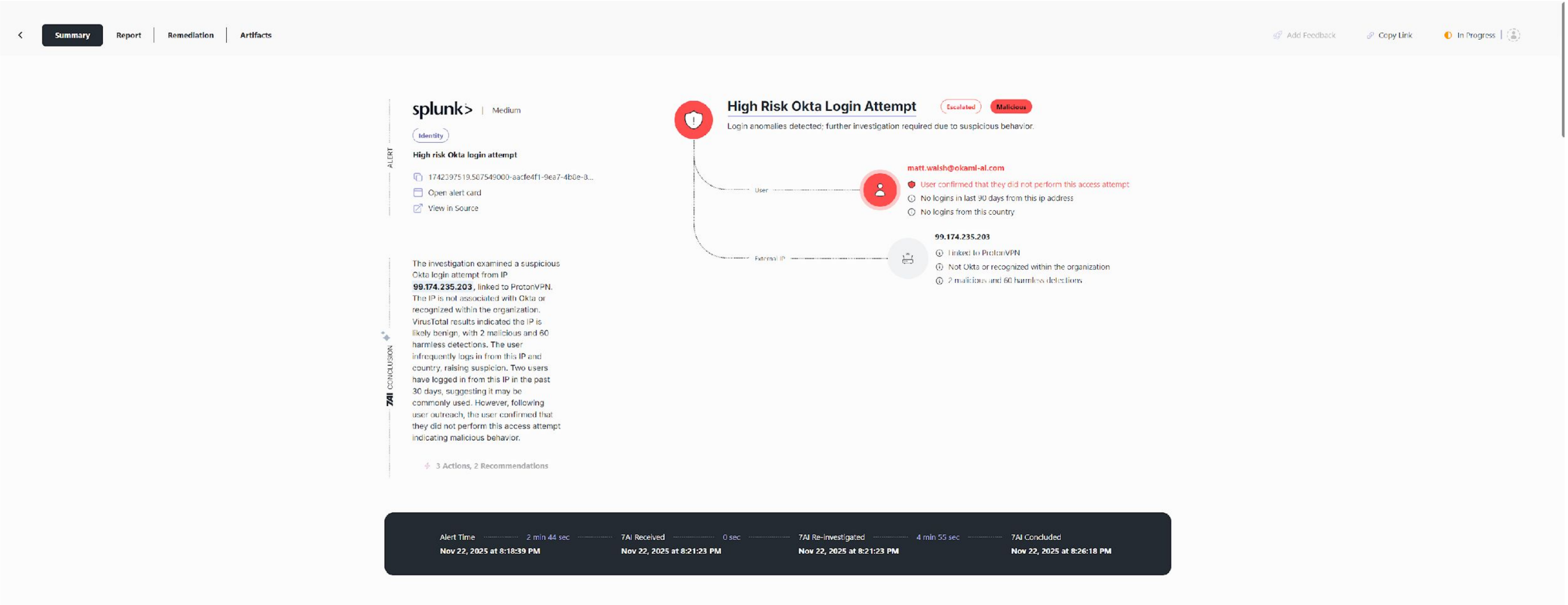


Category	Alert	Primary Artifact	Alert Time	Determination	Source severity	7AI Conclusion
✉	**Bridge Rock Resources** EMAIL - a41f0d06-664e-3251-4537-1c371d9ec360	'Bridge Rock Resources'	**Yesterday** Nov 23, 2025, 9:27 PM	Escalated Malicious	Medium Microsoft Sentinel	Due to malicious PDF attachment behaviors (attempted javascript execution, links to suspicious URLs) Show more
👤	**High Risk Okta Login Attempt** IDENTITY - 1742397519.587549000-aacfe4f1-9ea7-4b8e-858c-0e24f5428178	matt.walsh@okami-ai.com	Yesterday Nov 23, 2025, 8:18 PM	Escalated Malicious	Medium splunk>	Login anomalies detected; further investigation required due to suspicious behavior. Show more
>_	**Malware: Windows_XP_Activator_1.0.exe** ENDPOINT - 2155114338801808275	Windows_XP_Activator_1.0.exe	Yesterday Nov 23, 2025, 6:24 PM	Escalated Malicious	High SentinelOne	The file was classified as malicious necessitating further analysis. Show more
>_	**Malware: ELSBox32.exe** ENDPOINT - 2155091973511730012	desktop.ernser52	Yesterday Nov 23, 2025, 1:32 PM	Escalated Malicious	High SentinelOne	The file was quarantined and killed by SentinelOne, but the findings are inconclusive. Show more
🗎	**'Black Basta' ransomware was prevented** THREAT INTEL - d7beb988-dbe6-9436-911f-33cd66e10fdc	Black Basta'	Yesterday Nov 23, 2025, 1:06 PM	Escalated Malicious	Low Microsoft Sentinel	The alert was determined to be a true positive, but the infection was limited to one process execution on one device. Show more
✉	**Human Resources shared 'Employee Pay Increase [Effective 11_29_2024].paper' with you** EMAIL - c41f0d06-664e-3251-4537-1c371d9ec360	Human Resources shared 'Employee Pay Increase [Effective 11_29_2024].pap...	Yesterday Nov 23, 2025, 6:13 AM	Escalated Malicious	Low Microsoft Sentinel	The investigation confirmed the email as malicious, identifying it as a spear-phishing attempt. Show more
>_	**User accessed link in ZAP-quarantined email** ENDPOINT - **12 GROUPED ALERTS** - 4678709c-4bad-424b-af34-7fb96d9a4f9b		Yesterday Nov 23, 2025, 5:11 AM	Escalated Malicious	Unknown Microsoft Sentinel	Show conclusion
✉	**Email Investigation** EMAIL - b23af3c7-19db-4f9d-a816-f47585be7e50		Yesterday Nov 23, 2025, 3:10 AM	Escalated Malicious	Unknown 7AI	Show conclusion

© 2025 DXC Technology Company. All rights reserved.

DXC Confidential

7AI Investigation summary



splunk> | Medium

Identity

High risk Okta login attempt

1742397519.587549000-aacfe4f1-9ea7-4b8e-8...

Open alert card

View in Source

The investigation examined a suspicious Okta login attempt from IP **99.174.235.203**, linked to ProtonVPN. The IP is not associated with Okta or recognized within the organization. VirusTotal results indicated the IP is likely benign, with 2 malicious and 60 harmless detections. The user infrequently logs in from this IP and country, raising suspicion. Two users have logged in from this IP in the past 30 days, suggesting it may be commonly used. However, following user outreach, the user confirmed that they did not perform this access attempt indicating malicious behavior.

3 Actions, 2 Recommendations

High Risk Okta Login Attempt

Escalated Malicious

Login anomalies detected; further investigation required due to suspicious behavior.

matt.walsh@okami-ai.com

- User confirmed that they did not perform this access attempt
- No logins in last 90 days from this ip address
- No logins from this country

99.174.235.203

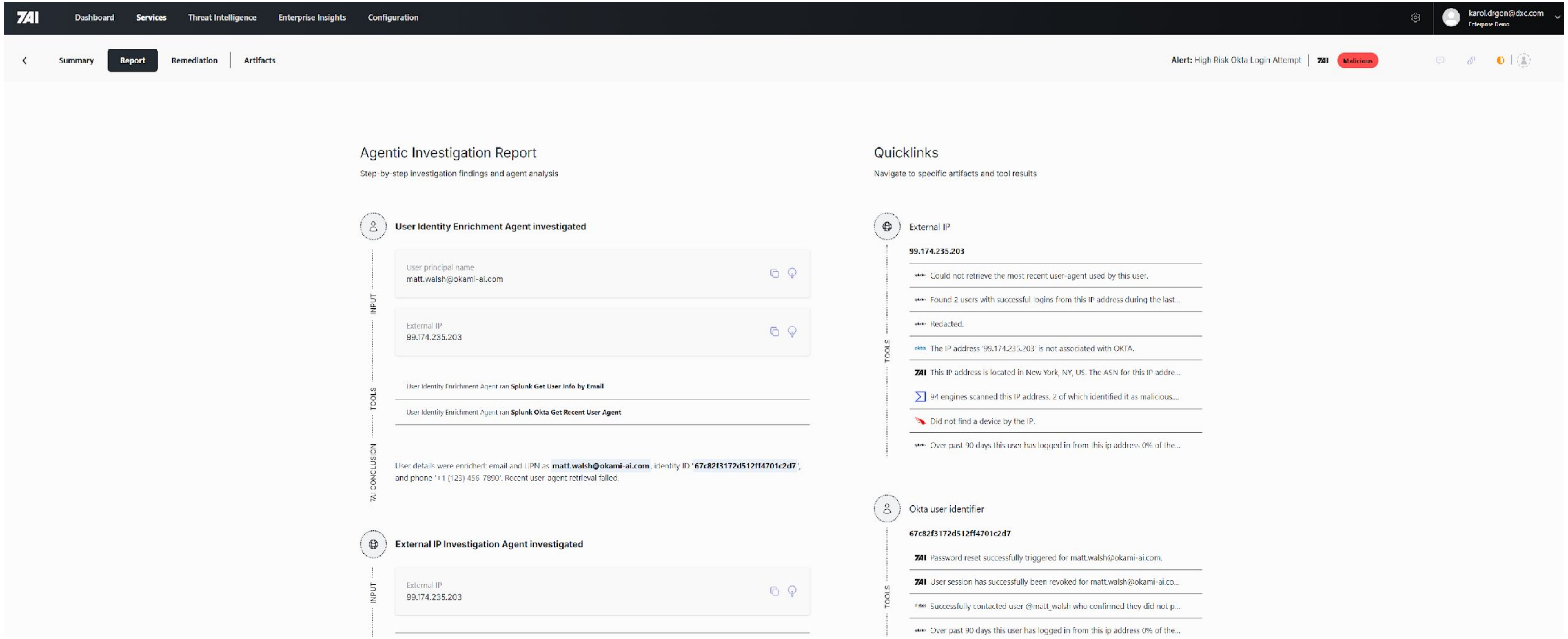
- Linked to ProtonVPN
- Not Okta or recognized within the organization
- 2 malicious and 60 harmless detections

Alert Time ········ 2 min 44 sec ········ 7AI Received ········ 0 sec ········ 7AI Re-investigated ········ 4 min 55 sec ········ 7AI Concluded

Nov 22, 2025 at 8:18:39 PM **Nov 22, 2025 at 8:21:23 PM** **Nov 22, 2025 at 8:21:23 PM** **Nov 22, 2025 at 8:26:18 PM**

© 2025 DXC Technology Company. All rights reserved.

Investigation report



Alert: High Risk Okta Login Attempt | 7AI Malicious

Agentic Investigation Report

Step-by-step investigation findings and agent analysis

User Identity Enrichment Agent investigated

User principal name
matt.walsh@okami-ai.com

External IP
99.174.235.203

User Identity Enrichment Agent ran **Splunk Get User Info by Email**

User Identity Enrichment Agent ran **Splunk Okta Get Recent User Agent**

User details were enriched: email and UPN as **matt.walsh@okami-ai.com**, identity ID '**67c82f3172d512ff4701c2d7**', and phone '+1 (123) 456 7890'. Recent user agent retrieval failed.

External IP Investigation Agent investigated

External IP
99.174.235.203

Quicklinks

Navigate to specific artifacts and tool results

External IP

99.174.235.203

- Could not retrieve the most recent user-agent used by this user.
- Found 2 users with successful logins from this IP address during the last...
- Redacted.
- The IP address '99.174.235.203' is not associated with OKTA.
- This IP address is located in New York, NY, US. The ASN for this IP addre...
- 94 engines scanned this IP address. 2 of which identified it as malicious....
- Did not find a device by the IP.
- Over past 90 days this user has logged in from this ip address 0% of the...

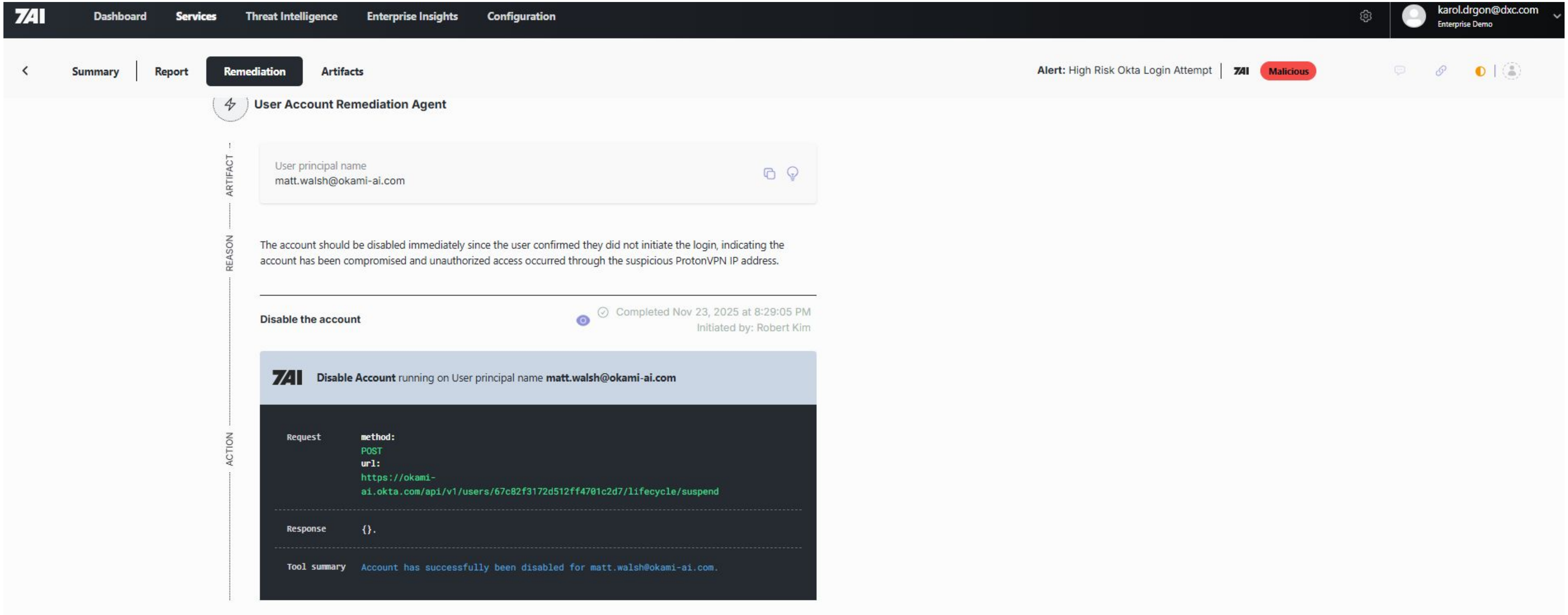
Okta user identifier

67c82f3172d512ff4701c2d7

- Password reset successfully triggered for matt.walsh@okami-ai.com.
- User session has successfully been revoked for matt.walsh@okami-ai.co...
- Successfully contacted user @matt_walsh who confirmed they did not p...
- Over past 90 days this user has logged in from this ip address 0% of the...

© 2025 DXC Technology Company. All rights reserved.

Incident remediation



Alert: High Risk Okta Login Attempt

User Account Remediation Agent

User principal name
matt.walsh@okami-ai.com

The account should be disabled immediately since the user confirmed they did not initiate the login, indicating the account has been compromised and unauthorized access occurred through the suspicious ProtonVPN IP address.

Disable the account

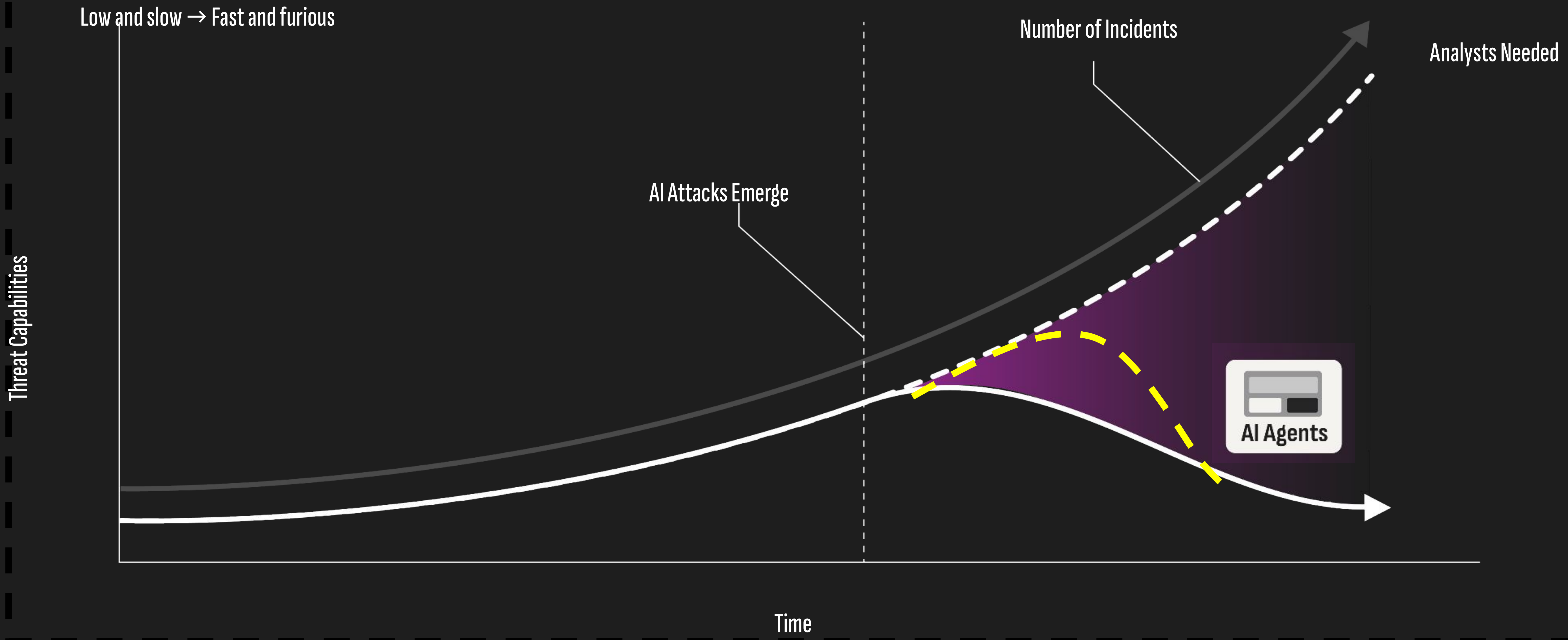
Completed Nov 23, 2025 at 8:29:05 PM
Initiated by: Robert Kim

Disable Account running on User principal name **matt.walsh@okami-ai.com**

```
Request       method:
              POST
              url:
              https://okami-
              ai.okta.com/api/v1/users/67c82f3172d512ff4701c2d7/lifecycle/suspend
-----------------------------------------------------------------------------
Response      {}.
-----------------------------------------------------------------------------
Tool summary  Account has successfully been disabled for matt.walsh@okami-ai.com.
```

© 2025 DXC Technology Company. All rights reserved.

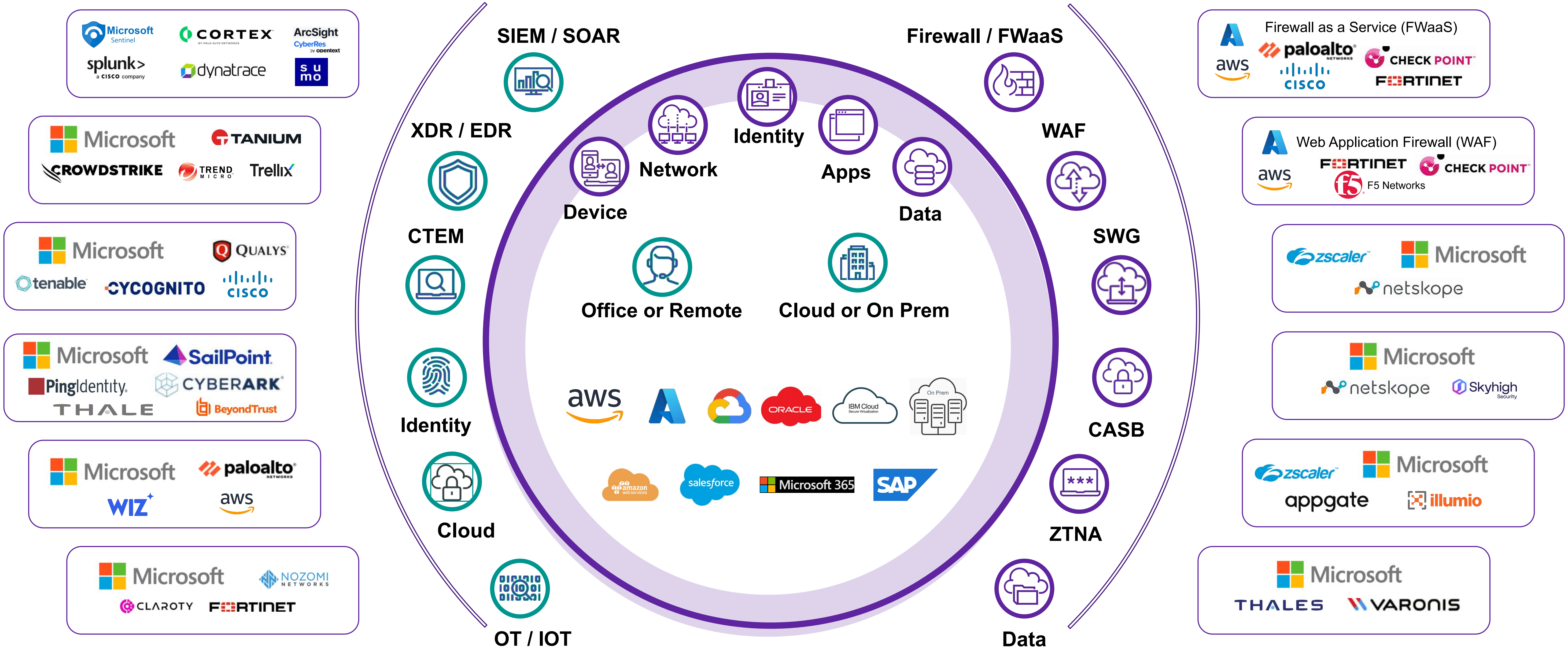
A DECADES-OLD PROBLEM GETTING EXPONENTIALLY WORSE.



© 2025 DXC Technology Company. All rights reserved.

DXC Confidential

DXC Cybersecurity Partners



SIEM / SOAR: Microsoft Sentinel, Cortex by Palo Alto Networks, ArcSight CyberRes by opentext, splunk> a cisco company, dynatrace, sumo

XDR / EDR: Microsoft, Tanium, CrowdStrike, Trend Micro, Trellix

CTEM: Microsoft, Qualys, tenable, CyCognito, cisco

Identity: Microsoft, SailPoint, PingIdentity, CyberArk, Thales, BeyondTrust

Cloud: Microsoft, paloalto networks, wiz, aws

OT / IOT: Microsoft, Nozomi Networks, Claroty, Fortinet

Firewall / FWaaS: Firewall as a Service (FWaaS) – aws, paloalto networks, cisco, Check Point, Fortinet

WAF: Web Application Firewall (WAF) – aws, Fortinet, Check Point, F5 Networks

SWG: zscaler, Microsoft, netskope

CASB: Microsoft, netskope, Skyhigh Security

ZTNA: zscaler, Microsoft, appgate, illumio

Data: Microsoft, Thales, Varonis

Identity, Network, Apps, Device, Data

Office or Remote

Cloud or On Prem

aws, Oracle, IBM Cloud Secure Virtualization, On Prem, amazon webservices, salesforce, Microsoft 365, SAP

DXC TECHNOLOGY

© 2025 DXC Technology Company. All rights reserved.

DXC Confidential

DXC Cybersecurity

Karol Drgon

GTCO Cyber Defense / SOC

karol.drgon@dxc.com

© 2025 DXC Technology Company. All rights reserved.

DXC Confidential