Exelegent

01.

Threat Protection

3 Weeks engagement financially supported by Exelegent & Microsoft

ABOUT US

Exelegent is a professional services company

Exelegent is a premier East Coast cybersecurity and compliance company where efficiency is standard, and our customers are our partners. The Exelegent team leverages 10 years of professional experience serving the needs of healthcare providers, financial services, life sciences, aerospace and defense, insurance and so many more.

Over 100+ clients trusted our team of security experts to implement the best practices in security following industry standards in HIPAA, NIST, PCI-DSS, etc.

10,356

Worry-free end users supported

100%

Customer retention rate

$20 MLN+

Saved for our customers

200+

Clients worked with us

PRACTICES

Products & Services

Digital Workplace

aimed at fostering secure collaboration and ensuring seamless operations in the modern work landscape.

Security and Compliance

dedicated to fortifying organizations against evolving cyber threats and ensuring robust data governance..

Data & AI

offering a comprehensive suite of services to enhance operations and drive transformative outcomes.

BPO

bring efficiency, innovation, and scalability to organizations seeking streamlined processes and enhanced productivity

Value-Added Reseller

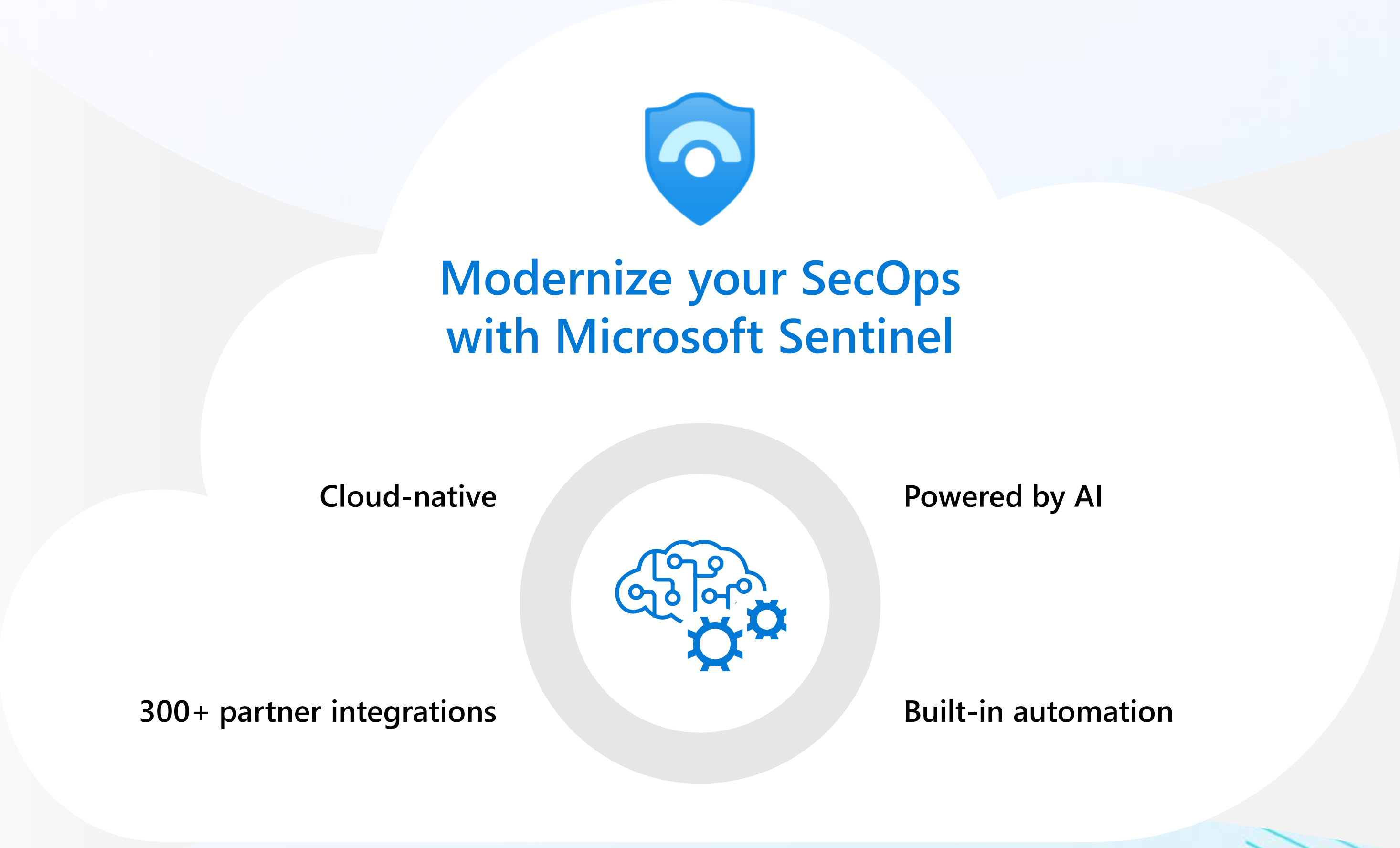
comprehensive solutions for Licenses & Consumption and Software and Hardware Procurement, catering to the diverse needs of businesses seeking technology solutions.

TrustElements.com

Automated cyber risk quantification and management platform

Move faster with simplified threat detection and response

- Infrastructure
- Devices
- Users
- Applications



Modernize your SecOps with Microsoft Sentinel

Across multicloud, multiplatform

Powered by community + backed by Microsoft security experts

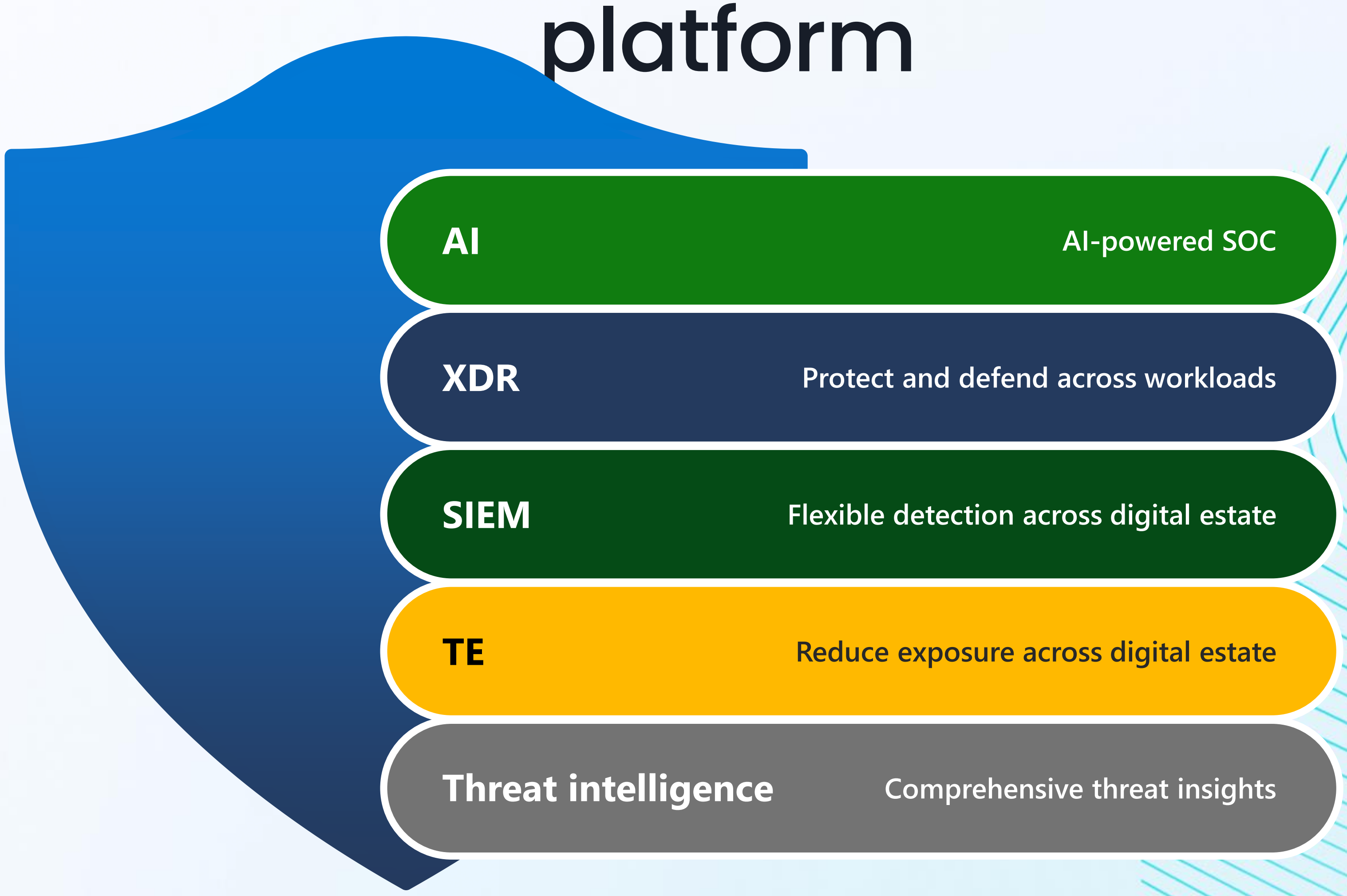
Detection
Correlate alerts into actionable incidents using machine learning

Investigation
Visualize the full scope of an attack

Response
Act immediately with built-in automation

Threat hunting
Hunt across all data with powerful search and query tools

It’s time for a unified security operations platform



AI — AI-powered SOC

XDR — Protect and defend across workloads

SIEM — Flexible detection across digital estate

TE — Reduce exposure across digital estate

Threat intelligence — Comprehensive threat insights

Optimized analyst experience | Targeted assistance | Automated protection and remediation

Objectives

Discover threats

Gain visibility into threats to your Microsoft 365 cloud and on-premises environments across email, identity, endpoints and data to better understand, prioritize and mitigate potential vectors of cyberattacks against your organization.

Discover vulnerabilities

Gain visibility into vulnerabilities to your Microsoft 365 cloud and on-premises environments to better understand, prioritize and address vulnerabilities and misconfigurations across your organization.

Define next steps

As part of the engagement, we will work together to define a list of next steps based on your needs, objectives, and results from the Threat Protection Engagement.

What we’ll do during the engagement

Analyze your priorities and requirements for deployment of Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) systems.

Define scope & deploy Microsoft Sentinel and Microsoft Defender XDR in production environment, integrating them with Microsoft and 3rd party solutions.

Discover threats to cloud and on-premises and across email, identity, endpoints and data and demonstrate how to automate responses.

Experience TrustElements - discover and prioritize vulnerabilities and misconfigurations across your organization.

Plan next steps on how we can work together.

Phases and activities

Kick Off Call

- Introductions
- Engagement walk-through
- Engagement Questionnaire
- Expectations
- Requirements

Engagement Setup

- Define and document deployment scope
- Setup trial licenses & subscription
- Configure engagement tools
  - Microsoft 365 Security Configuration
  - Microsoft Sentinel Configuration
- TrustElements Onboarding

Threat and Vulnerabilities Exploration

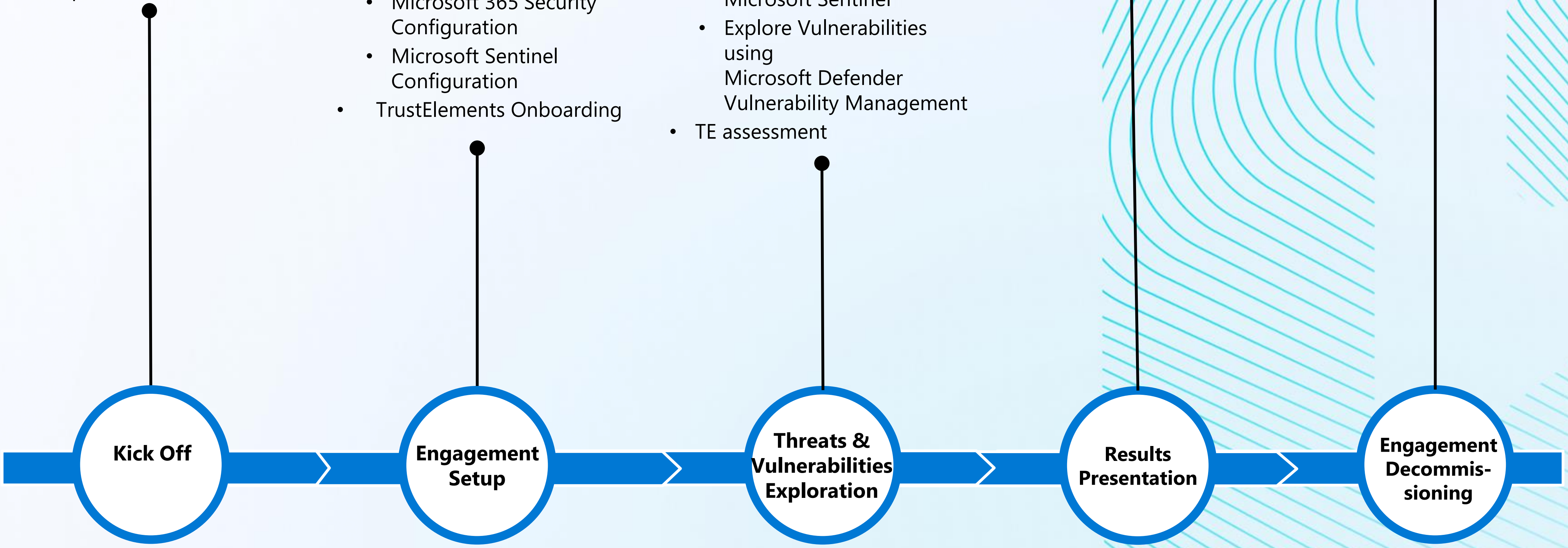
- Threats and Vulnerabilities Exploration
  - Explore threats using Microsoft Defender XDR
  - Explore threats using Microsoft Sentinel
  - Explore Vulnerabilities using Microsoft Defender Vulnerability Management
- TE assessment

Results Presentation

- Results presentation
- Next Steps discussion

Engagement Decommissioning

- Remove configuration changes
- Deactivate trial licenses/subscription



Kick Off

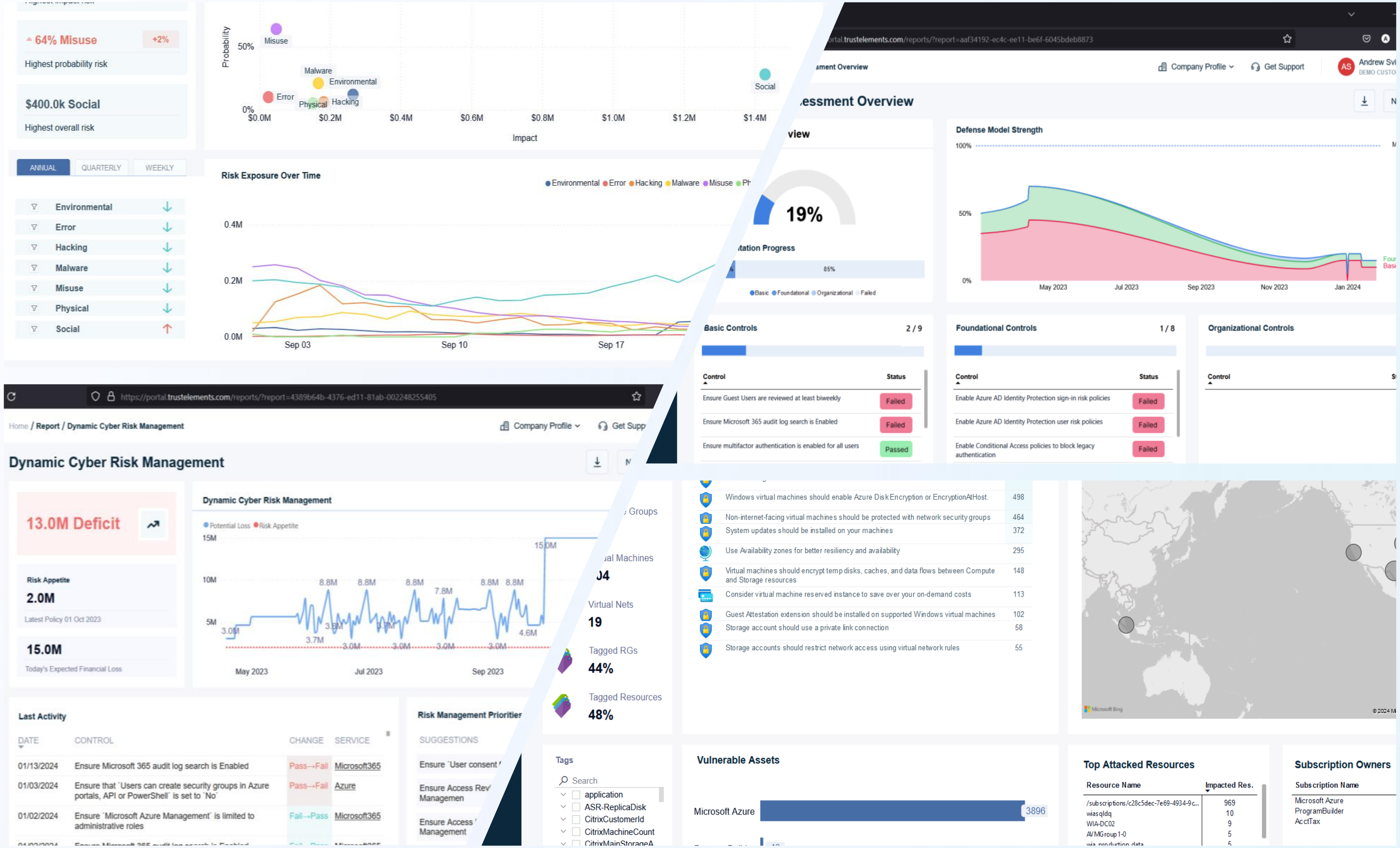
Engagement Setup

Threats & Vulnerabilities Exploration

Results Presentation

Engagement Decommis-sioning

TrustElements



Basic Controls 2 / 9

Control	Status
Ensure Guest Users are reviewed at least biweekly	Failed
Ensure Microsoft 365 audit log search is Enabled	Failed
Ensure multifactor authentication is enabled for all users	Passed

Foundational Controls 1 / 8

Control	Status
Enable Azure AD Identity Protection sign-in risk policies	Failed
Enable Azure AD Identity Protection user risk policies	Failed
Enable Conditional Access policies to block legacy authentication	Failed

Organizational Controls

Control	S

Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost.	498
Non-internet-facing virtual machines should be protected with network security groups	464
System updates should be installed on your machines	372
Use Availability zones for better resiliency and availability	295
Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources	148
Consider virtual machine reserved instance to save over your on-demand costs	113
Guest Attestation extension should be installed on supported Windows virtual machines	102
Storage account should use a private link connection	58
Storage accounts should restrict network access using virtual network rules	55

Last Activity

DATE	CONTROL	CHANGE	SERVICE
01/13/2024	Ensure Microsoft 365 audit log search is Enabled	Pass→Fail	Microsoft365
01/03/2024	Ensure that `Users can create security groups in Azure portals, API or PowerShell` is set to `No`	Pass→Fail	Azure
01/02/2024	Ensure `Microsoft Azure Management` is limited to administrative roles	Fail→Pass	Microsoft365

Risk Management Priorities

SUGGESTIONS

- Ensure `User consent f
- Ensure Access Rev Managemen
- Ensure Access Management

Tags

- □ application
- □ ASR-ReplicaDisk
- □ CitrixCustomerId
- □ CitrixMachineCount
- □ CitrixMainStorageA

Top Attacked Resources

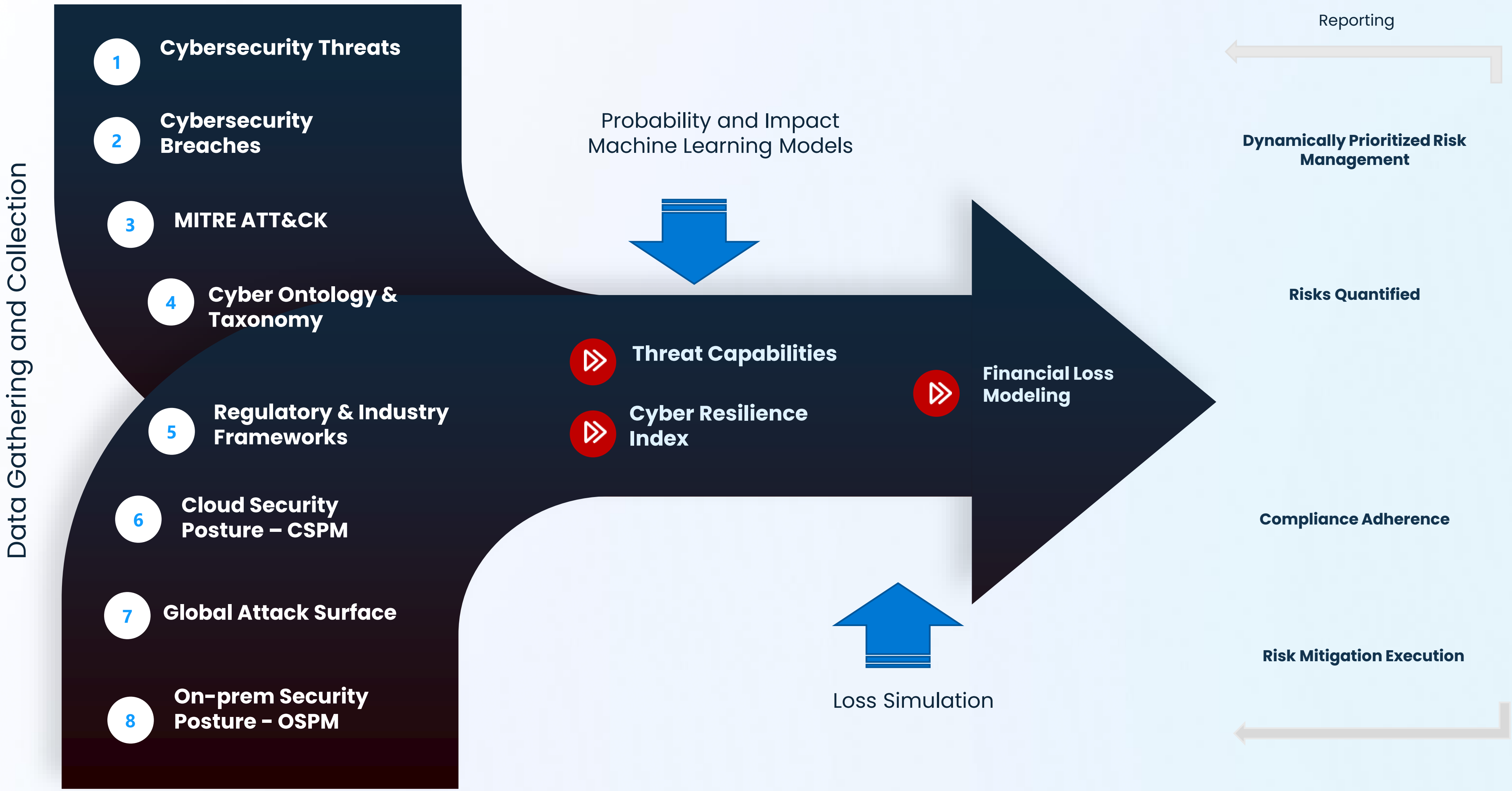
Resource Name	Impacted Res.
/subscriptions/c28c5dec-7e69-4934-9c...	969
wiasqldq	10
WIA-DC02	9
AVMGroup1-0	5

Subscription Owners

Subscription Name
Microsoft Azure
ProgramBuilder
AcctTax

APPROACH

TrustElements



Data Gathering and Collection

1 Cybersecurity Threats

2 Cybersecurity Breaches

3 MITRE ATT&CK

4 Cyber Ontology & Taxonomy

5 Regulatory & Industry Frameworks

6 Cloud Security Posture – CSPM

7 Global Attack Surface

8 On-prem Security Posture - OSPM

Probability and Impact Machine Learning Models

Threat Capabilities

Cyber Resilience Index

Financial Loss Modeling

Loss Simulation

Reporting

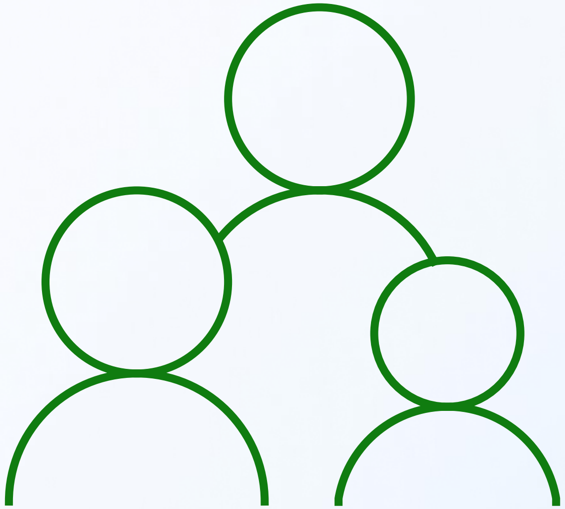
Dynamically Prioritized Risk Management

Risks Quantified

Compliance Adherence

Risk Mitigation Execution

Customer responsibilities



Access to key participants

Multiple activities require the attendance of selected members of security or cloud infrastructure teams.

Provide stakeholder/sponsor oversight

A stakeholder/sponsor is required to oversee and own the process from the customer side.

Access to the tenant

Provide access to the tenant to set up Microsoft security products used in the engagement and produce necessary reports from them.

After the Threat Protection Engagement, you'll…

- ✓ Better understand, prioritize, and mitigate potential threats.
- ✓ Better understand, prioritize, and address vulnerabilities.
- ✓ Accelerate your security journey with Microsoft.
- ✓ Have defined next steps based on your needs and objectives.