Exelegent

01.

Cybersecurity Assessment

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

Automated cyber risk quantification and management platform

INDUSTRY

Top Ransomware & Data Risk Concerns

Organizations struggle with maintaining basic cybersecurity hygiene

98% of ransomware attacks can be traced to common configuration errors in software and devices.[1]

Ransomware attacks have been steadily increasing

37% of all businesses and organizations were hit by ransomware in 2021.[2]

Recovering from a ransomware attack is costly

$1.85M Recovering from a ransomware attack cost businesses $1.85 million on average in 2021.[3]

[1] Digital Defense Report 2022, Microsoft

[2] Ransomware Statistics, Trends and Facts for 2023 and Beyond

[3] Ransomware Statistics, Trends and Facts for 2023 and Beyond

Data security incidents are widespread

83% of organizations experience more than one data breach in their lifetime[1]

Malicious insiders account for 20% of data breaches, adding to costs

$15.4M Total average cost of activities to resolve insider threats over 12 month period[2]

Organizations are struggling with fragmented landscape

80% of decision makers purchased multiple products to meet compliance and data protection needs[3]

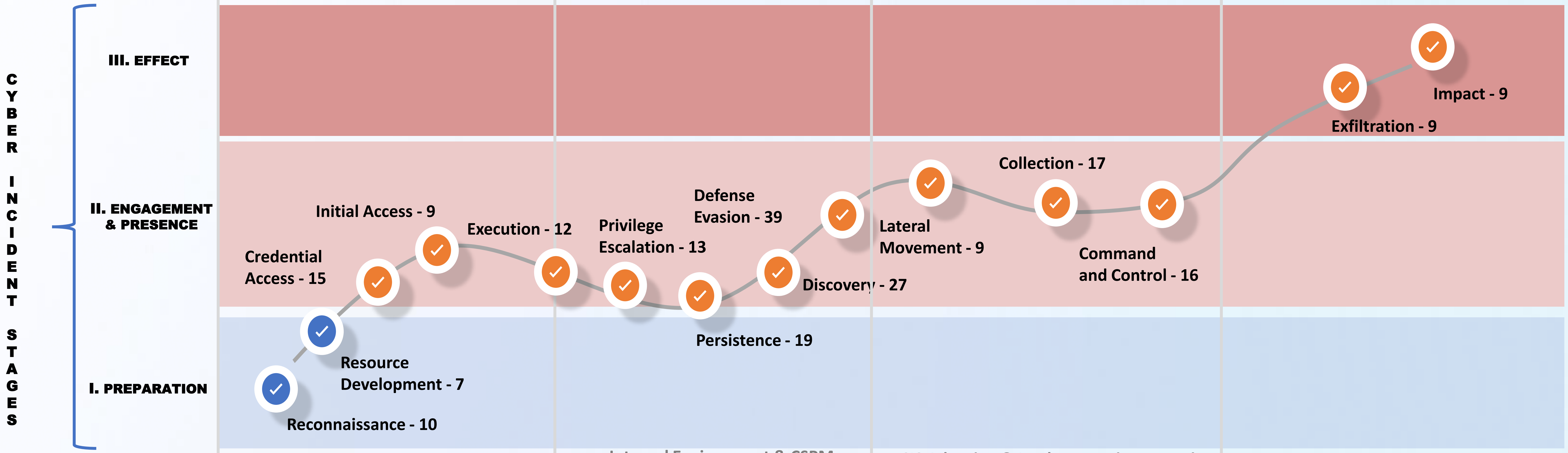
[1] Cost of a Data Breach Report 2022, IBM

[2] Cost of Insider Threats Global Report 2022, Ponemon Institute

[3] February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees,
n=100 1000+ employees)
commissioned by Microsoft with MDC Research

Cyber Resilience vs Attack Vectors

CYBER RESILIENCE	ANTICIPATE	WITHSTAND	RECOVER	ADAPT
NIST 800-53	CA; CP; IR; PM; RA; SA; SI; AC; AU; CM; PE; SC; CA; IA; PL	IA; SP; SI; SR; AC; AU; CP; IA; PL; SA; CM; RA; MA	CP; PE; SP; AC; AU; CM; IA; PE; SP; SI	SP; SI; CM; PM; SA; SP



Global Attack Surface

- External Perimeter: ports, services, vulnerabilities, SSL certificates
- Email Infrastructure Review
- Business Email Compromise

Internal Environment & CSPM

- Identity & Access Management
- Patching Cadence
- Internal Environment VA
- Cloud Security Posture

CIS Adoption & Implementation Maturity

- Organization’s Maturity
- Safeguards Implementation Heatmap
- Safeguards Implementation Roadmap and Priorities

Cyber Resilience & Cyber Risk Modeling

- Cyber Resilience Index
- Cyber Risk Quantification
- Cyber Investment Priorities

GOALS

Objectives and Approach

Discover Vulnerabilities

Gain visibility into vulnerabilities within your Microsoft 365 cloud environment.

Discover and analyze vulnerabilities to servers and endpoints using Microsoft Defender Vulnerability Management.

Explore and Evaluate sensitive information and potential insider risk

Gain visibility into sensitive information discovered by Microsoft Purview Information Protection.

Explore potentially risky data handling activities identified by Microsoft Purview Insider Risk Management Analytics.

TrustElements

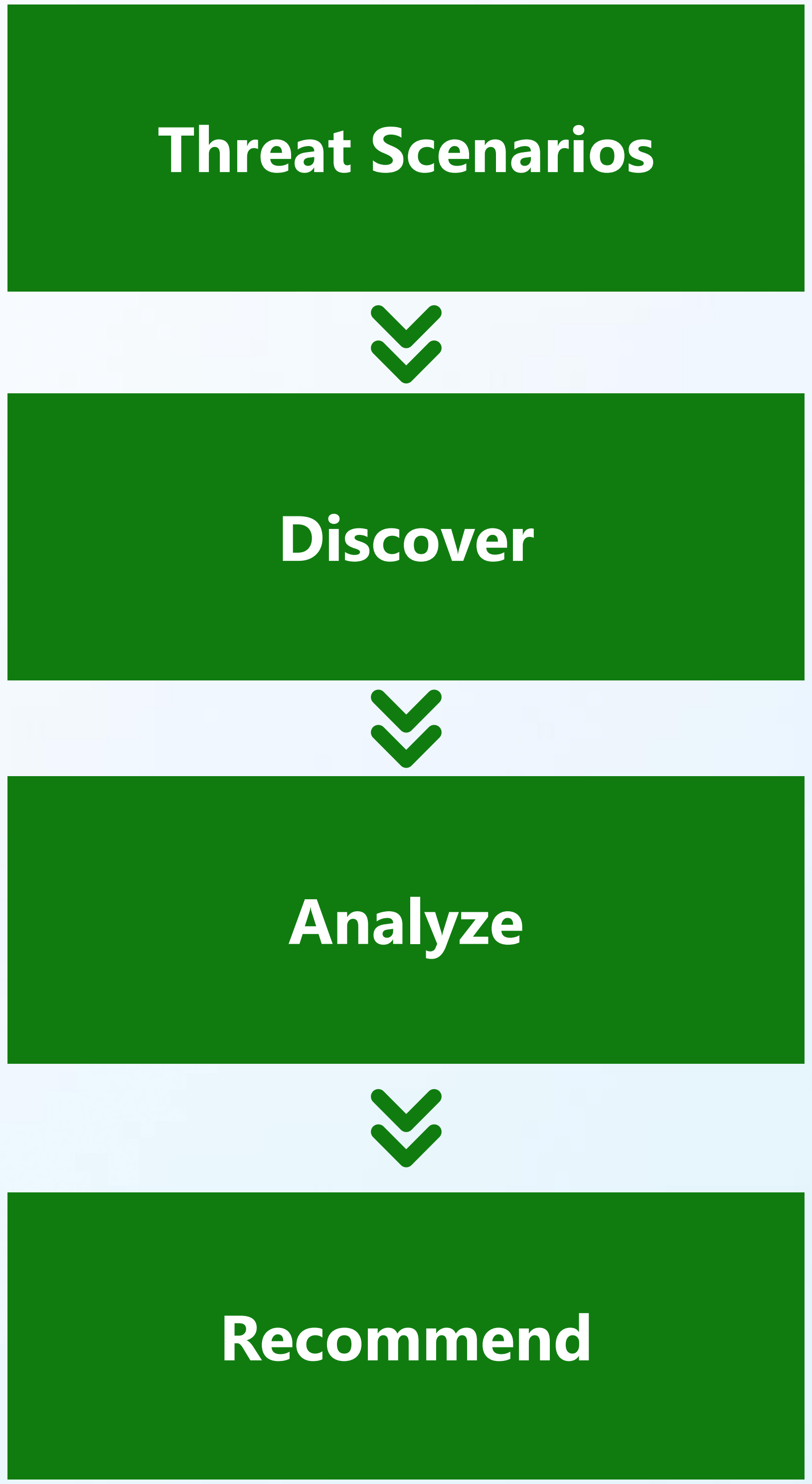
Evaluate cyber risks through Industry standard value at risk models

Visualize cyber risks and potential financial impacts.

Model real-time changes to emerging cyber security threats and enterprise environments

Define next steps

List of next steps based on organization’s needs, objectives, and results from the Cybersecurity Assessment.



Threat Scenarios

Discover

Analyze

Recommend

METHOD

Engagement Methodology

The engagement **covers commonly seen threat scenarios**:

- Ransomware
- Data Security risks

Using the engagement tools, **discover vulnerabilities within the environment** across cloud, servers and endpoints.

The vulnerabilities and risks are analyzed and prioritized to show how prepared the organization's defenses are against the threat scenarios.

Prepare detailed recommendations to help the organization to prioritize the improvements to their cybersecurity posture.

OUTLINE

What we’ll do during the engagement

Analyze your environment and current cybersecurity maturity level based on v8 of the CIS Critical Security Controls.

Define scope & deploy Microsoft Defender Vulnerability Management and Insider Risk Analytics in your production environment.

Experience Trust Elements and understand your cloud security posture enhanced through the use of quantification and dynamic management of risk

Perform a data security assessment, discover and evaluate sensitive information and potential insider risks in your organization.

Plan next steps on how to improve your cyber and data security posture and how we can work together.

ACTIVITIES

Phases and Activities

Kick Off Call

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

Engagement Setup

- Engagement scope and design decisions

General Configuration

– 0.5 hour

- Setup trial licenses & subscription
- Setup pre-requisites for engagement tools

Microsoft Defender Vulnerability Management Configuration

- Configure Microsoft Defender Vulnerability Management

Insider Risk Management Analytics Configuration

- Configure Microsoft Purview Insider Risk Management

Vulnerabilities Exploration

- Explore vulnerabilities in:
  - Microsoft Defender Vulnerability Management
  - Microsoft Secure Score

Data Security Exploration

- Explore data security risks from company insiders.

TrustElements Assessment

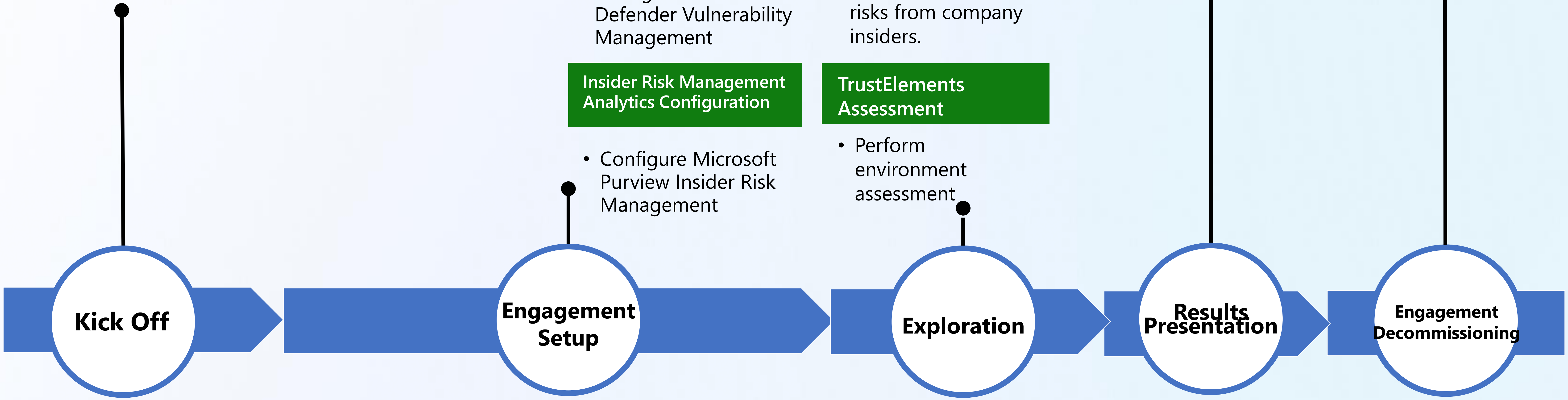
- Perform environment assessment

Results Presentation

- Results presentation and Next Steps discussion.

Engagement Decommissioning

- Remove configuration changes
- Deactivate trial licenses



Kick Off

Engagement Setup

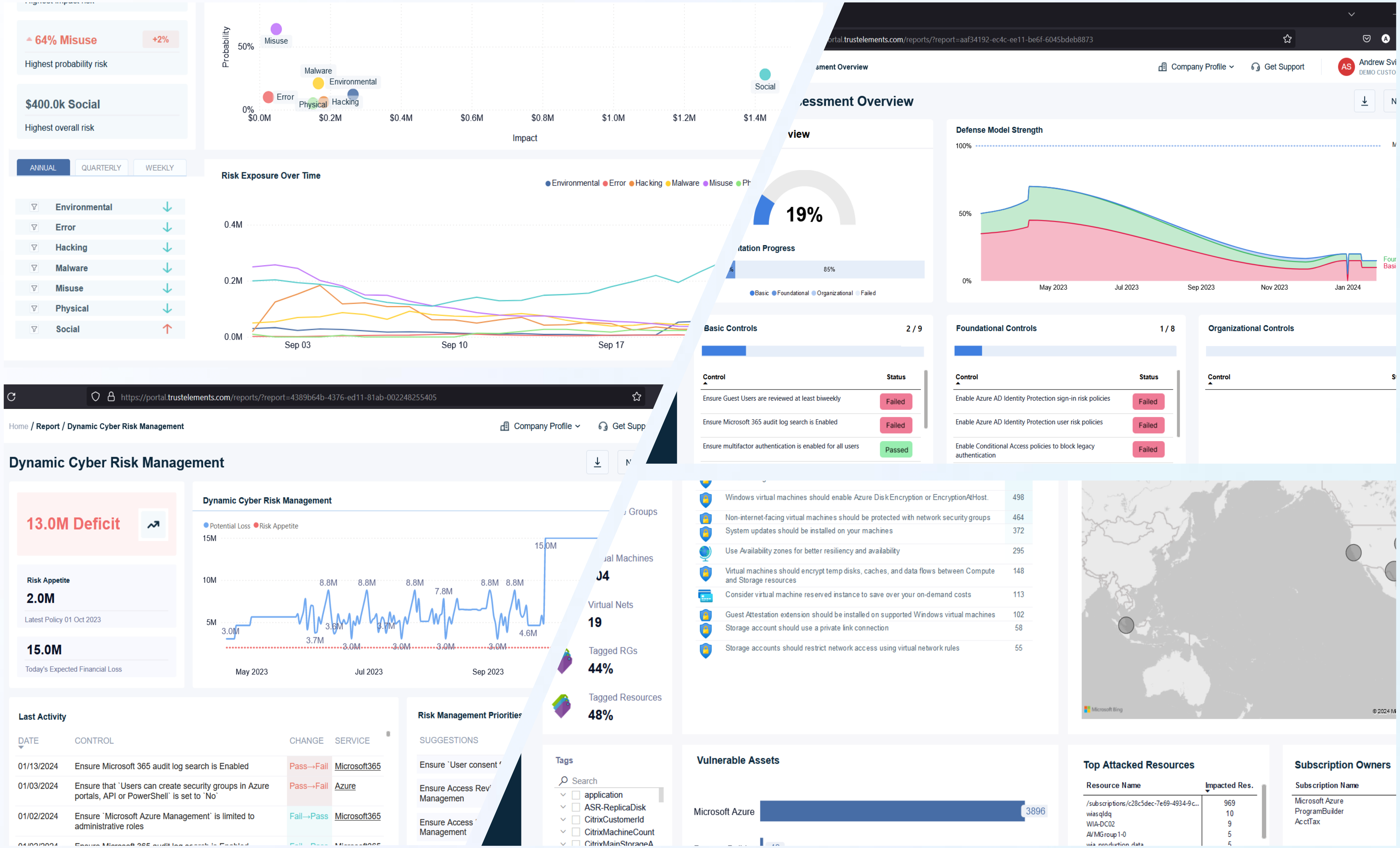
Exploration

Results Presentation

Engagement Decommissioning

DELIVERABLES

TrustElements



64% Misuse +2%

Highest probability risk

$400.0k Social

Highest overall risk

ANNUAL | QUARTERLY | WEEKLY

Environmental	↓
Error	↓
Hacking	↓
Malware	↓
Misuse	↓
Physical	↓
Social	↑

Risk Exposure Over Time

ortal.trustelements.com/reports/?report=aaf34192-ec4c-ee11-be6f-6045bdeb8873

sment Overview

Company Profile | Get Support | AS Andrew Svi DEMO CUSTO

essment Overview

view

19%

tation Progress

Defense Model Strength

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

https://portal.trustelements.com/reports/?report=4389b64b-4376-ed11-81ab-002248255405

Home / Report / Dynamic Cyber Risk Management

Company Profile | Get Supp

Dynamic Cyber Risk Management

13.0M Deficit

Risk Appetite

2.0M

Latest Policy 01 Oct 2023

15.0M

Today's Expected Financial Loss

Dynamic Cyber Risk Management

Groups

ual Machines

04

Virtual Nets

19

Tagged RGs

44%

Tagged Resources

48%

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
- Ensure Access Rev Managemen
- Ensure Access Management

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

Tags

Search

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

Vulnerable Assets

Top Attacked Resources

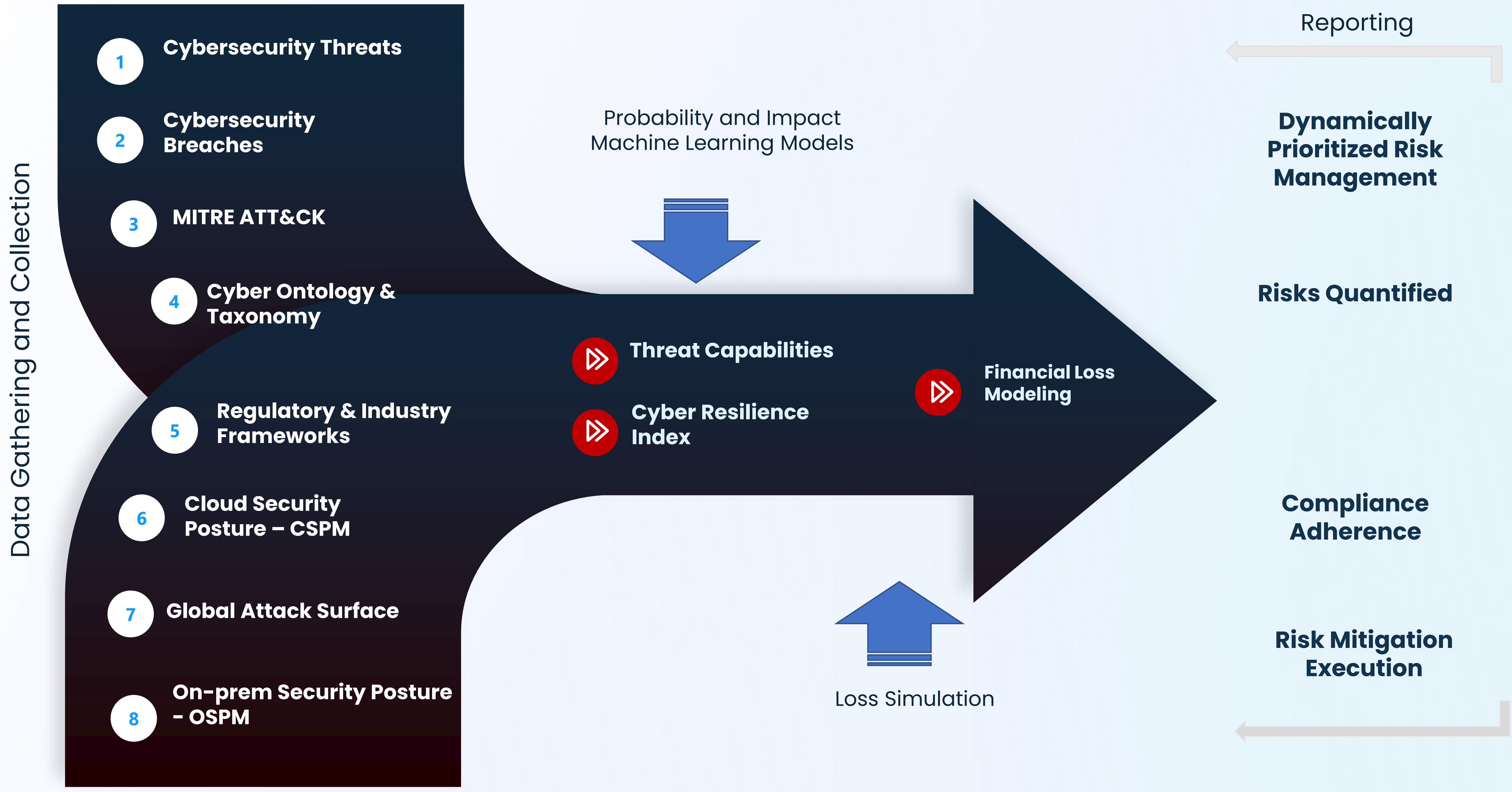
Resource Name	Impacted Res.
/subscriptions/c28c5dec-7e69-4934-9c...	969
wiasqldq	10
WIA-DC02	9
AVMGroup1-0	5
wia-production-data	5

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

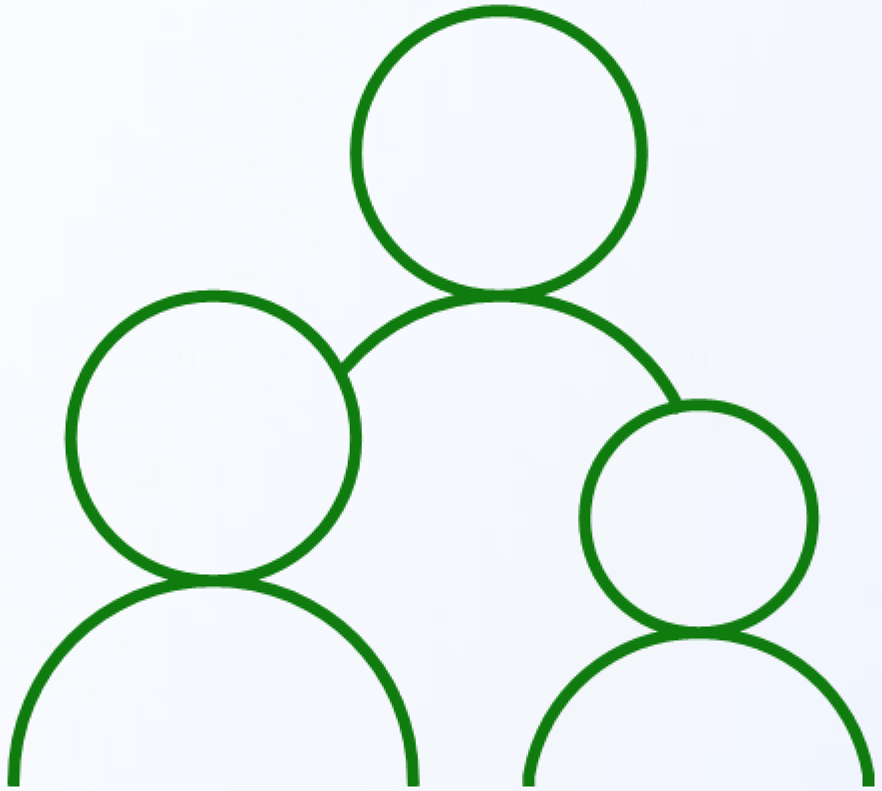
Risks Quantified

Compliance Adherence

Risk Mitigation Execution

REQUIREMENTS

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.

Provision a physical or virtual machine
Provision and provide access to a machine which will be used to scan for vulnerabilities during the engagement.