Microsoft Sentinel Quick Start

Presentation to Client

January 22, 2023

edgile

a **wipro** company

Edgile

Established in 2001, Edgile is headquartered in Austin, TX and delivers technology-enabled security and privacy services.

Edgile has deep expertise with highly regulated clients in sectors like financial services, healthcare, and insurance.

In December of 2021, Edgile was acquired by Wipro and is now part of their 8000-person Cyber Security Practice.

Senior Team	Highly Specialized	Core Competencies
▪ Average of 10+ years in industry experience ▪ Nationwide firm with extensive Big Four experience	▪ Identity and Access Management ▪ Integrated Risk Management ▪ Cloud Security	▪ Advisory ▪ Strategy ▪ Implementation ▪ Managed Service

SAVIYNT

SailPoint Admiral
TOP DELIVERY PARTNER

SailPoint
Identity & Access

Accelerate Cloud Adoption with Risk and Compliance Insights

Accelerate Access Control Risk and Compliance Sustainment

edgile

Microsoft Azure
Cloud

Accelerate Access Control to Cloud and On-Premise Apps

servicenow
Integrated Risk Management

Microsoft Partner
2022 Partner of the Year Winner
Compliance Award
Microsoft

2020 MICROSOFT SECURITY SYSTEM INTEGRATOR OF THE YEAR

servicenow Partner
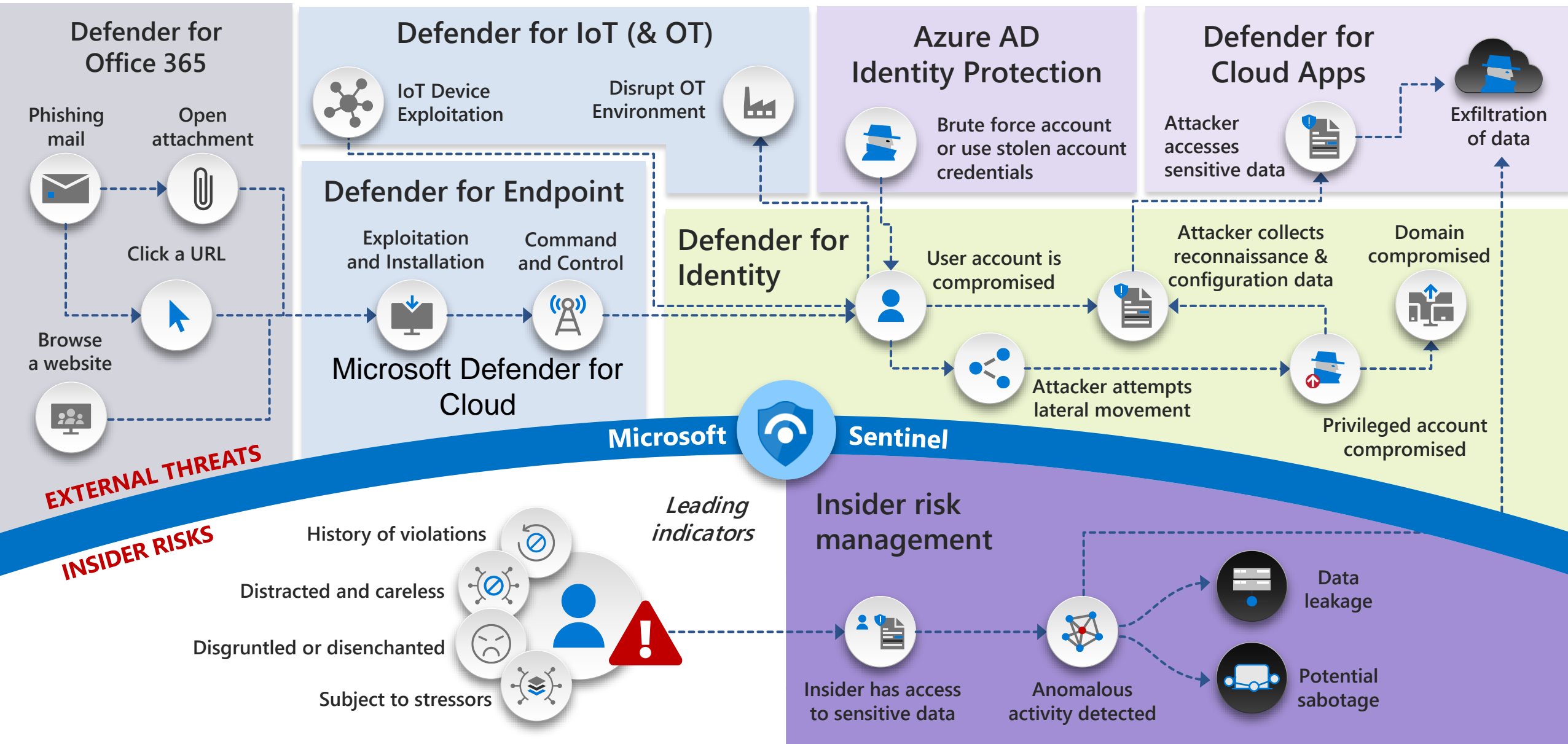Premier

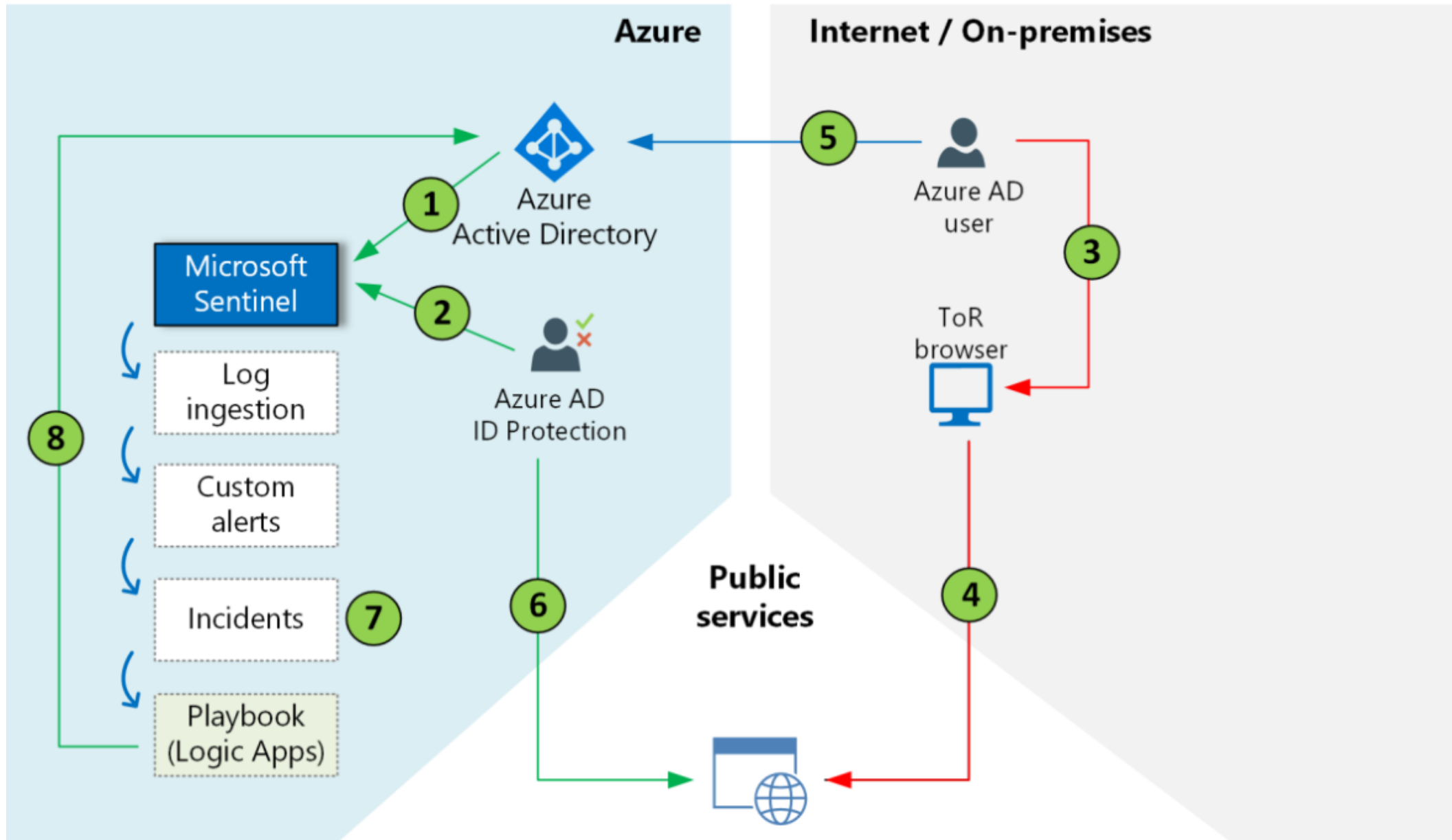# Microsoft Sentinel Quick Start

Workstream

Outcomes

1 **Discovery & Design**

Discovery and analysis of business process capture, identification and interview of priority stakeholders, and develop conceptual working sessions.

2 **Identify Data Connectors & Configuration**

Delivery of an initial configuration in production of data connectors with Microsoft Sentinel and the creation of workbooks and watchlist

3 **Identify & Configure Analytics Rules**

Delivery of an initial configuration in production of analytic rules configured within Microsoft Sentinel

4 **Automation**

Delivery of an initial configuration in production of Microsoft Sentinel playbooks with automation rules and hunting queries

5 **Knowledge Transfer**
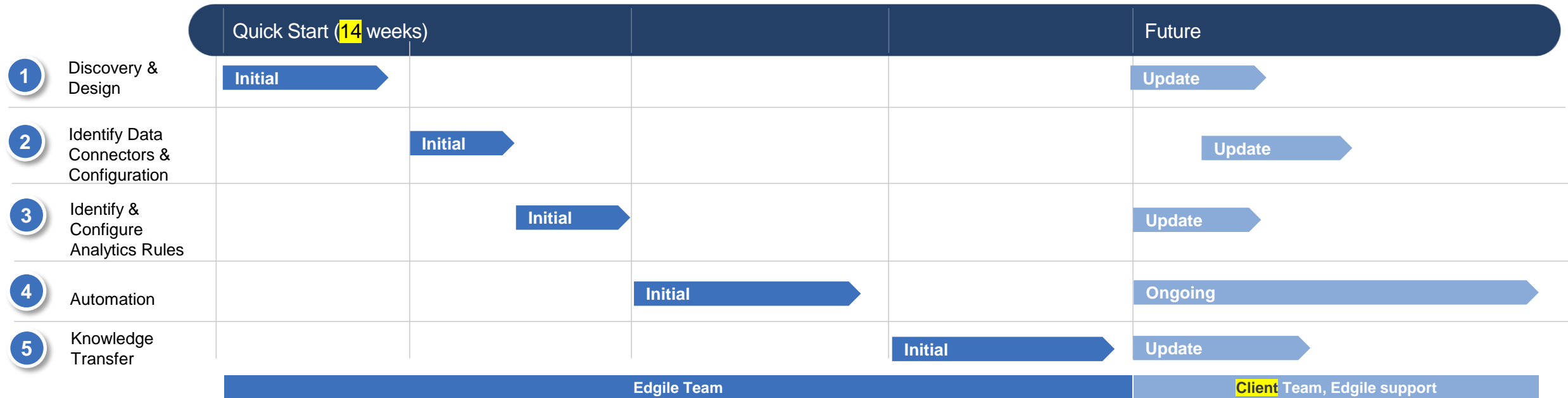
Ongoing knowledge transfer sessions (up to 8 hours total).

Defend across attack chains
Insider and external threats

Defender for Office 365

Phishing mail

Open attachment

Click a URL

Browse a website

Defender for IoT (& OT)

IoT Device Exploitation

Disrupt OT Environment

Defender for Endpoint

Exploitation and Installation

Command and Control

Microsoft Defender for Cloud

Azure AD Identity Protection

Brute force account or use stolen account credentials

Defender for Cloud Apps

Attacker accesses sensitive data

Exfiltration of data

Defender for Identity

User account is compromised

Attacker attempts lateral movement

Attacker collects reconnaissance & configuration data

Privileged account compromised

Domain compromised

Microsoft Sentinel

EXTERNAL THREATS

INSIDER RISKS

Leading indicators

History of violations

Distracted and careless

Disgruntled or disenchanted

Subject to stressors

Insider risk management

Insider has access to sensitive data

Anomalous activity detected

Data leakage

Potential sabotage

Timeline, Cost, and Projected Effort

		Quick Start (14 weeks)				Future
1	Discovery & Design	Initial				Update
2	Identify Data Connectors & Configuration		Initial			Update
3	Identify & Configure Analytics Rules		Initial			Update
4	Automation			Initial		Ongoing
5	Knowledge Transfer				Initial	Update
		Edgile Team				Client Team, Edgile support

Projected Quick Start Timeline: 14 Weeks

Edgile Resources
- 1 x Project Lead
- 1 x Sentinel Security Engineer
- 1 x Sentinel SME
- SMEs as required

Client Resources/ Support
- Project Manager
- Business Analyst
- M365 Administrators
- Change Mgmt. Support

Fixed Price: $350,000

In closing, Edgile offers…

- A **top-5 ranked security and compliance consulting** partner with Healthcare expertise

- **Unique and award-winning capabilities** that exactly match VSPs Data Governance needs

- A **cost-effective** consulting partner who understands VSP and is **committed to your success**

- **Objective recommendations** based on what is best for you

- A **leading expert** in GRC and **controls mapping to M365** solutions

- **Managed Services and relevant capabilities** that, if desired, can support your long-term vision

Thank you

Q&A

edgile
a wipro company

Driving Alignment Between Business and Security