AZURE SENTINEL – POC IN A WEEK WITH DELPHI CONSULTING

BUILD YOUR FORT-KNOX

Microsoft Partner
Microsoft

Gold Communications
Gold Cloud Platform
Gold Cloud Productivity
Gold Enterprise Mobility Management
Gold Windows and Devices

DELPHI
IT STRATEGY | CONSULTING | SUPPORT

AZURE SENTINEL – WHY THIS PROOF OF CONCEPT? AND HOW WE AIM TO HELP

DELPHI
IT STRATEGY | CONSULTING | SUPPORT

Delphi Consulting will help you get started with Azure Sentinel with its Proof of Concept offering and the program running over 4-5 days. We aim to provide you a definite understanding of how Azure Sentinel can contribute to your business from securing the enterprise to saving the infrastructure cost.

Solution Onboarding & Integration

- Perform native Integration of selected M365 products
- Set-up Syslog Collector & integrate selected on-prem log sources

Content & Dashboard Creation

- Create selected analytics rules from built-in templates
- Create selected customized workbooks

Automated Playbooks

- Create selected automated playbooks demonstrating the auto-investigation, alerting and response

AZURE SENTINEL-PROOF OF CONCEPT-OUR DELIVERABLES

- Delphi Consulting provides an Azure Sentinel Proof of Concept Service to help your organization trial and test Microsoft's powerful next generation SIEM+ SOAR solution.
- Delphi Consulting will help you to deploy a concept Sentinel instance and provide a demonstration of how the solution works driving intelligent security analytics and threat intelligence across the enterprise.

Scope of work

- Initial Discovery Assessment – Understanding customer's need around security challenges
- Introduction to Azure Sentinel, its capabilities and how it can help improving security posture
- Technical enablement
  - ➢ Set up Azure Sentinel Workspace & Syslog Log Collector
  - ➢ Enabling three native M365 Security Components
  - ➢ Demonstrate onboarding of a windows server (Domain Controller)
  - ➢ Demonstrate onboarding of two security log sources
- Configure Built-in Analytics Rules (10-15), customize and create two workbooks
- Demonstrate creation of two automation playbooks
- Provide Technical & Operational Guidance

Customer Key Take-aways

- Get a complete overview of Azure Sentinel
- gain an understanding of your security challenges and infrastructure
- A workshop report and recommendations for next steps
- Get a high-level solution plan, roadmap and next steps
- Get Pricing Details for Azure Sentinel
- Get a high-level Sentinel Architecture Diagram
- Focus on your core strengths - protecting your business
- Cut out the 'noise' and prioritizes incident response
- Enable rapid detection, investigation, and response
- Save on infrastructure and management overheads
- Harness the power of Machine Learning and AI

INDUSTRY WIDE CHALLENGES AROUND SECURITY & INFRASTRUCTURE

DELPHI
IT STRATEGY | CONSULTING | SUPPORT

Business networks are complex and so is security management for them. They include on-premises systems and cloud services.. New threats appear daily. Not everything fits a known threat signature, so protective software relies on behavioral patterns to catch zero-day threats. This approach is inevitably inexact. What's needed is enough intelligence to weed out the false alarms.

Challenges

- Disconnect between monitoring of On-Prem, Cloud-based infrastructure and other products.
- Investment challenges for infrastructure and scalability
- Limited threat intelligence capabilities
- Sophisticated Threats

Ideal Solution

- Single pane of glass
- Scalable Model
- Built-in Threat Intel
- Machine Learning with AI

Desired Outcome

- Integrated monitoring across both on-prem and cloud infrastructure.
- Unified console to monitor activity across various log sources.
- Outsourced Infrastructure with "Pay-as-you-go" scalability, built in redundancy.
- Intelligence concerning emerging threats

AZURE SENTINEL – PROOF OF CONCEPT

Get started with Azure Sentinel with our Proof-of-Concept Offering and gain a definite understanding on the features and capabilities of the Microsoft's next generation SIEM + SOAR solution

Refer to some of these exciting features of Sentinel before we begin:

Integration with Existing Technologies

- Azure Sentinel makes it easy to collect security data across your entire hybrid organization from devices, to users, to apps, to servers on any cloud.

Billion Strong Threat Intel feed from Microsoft

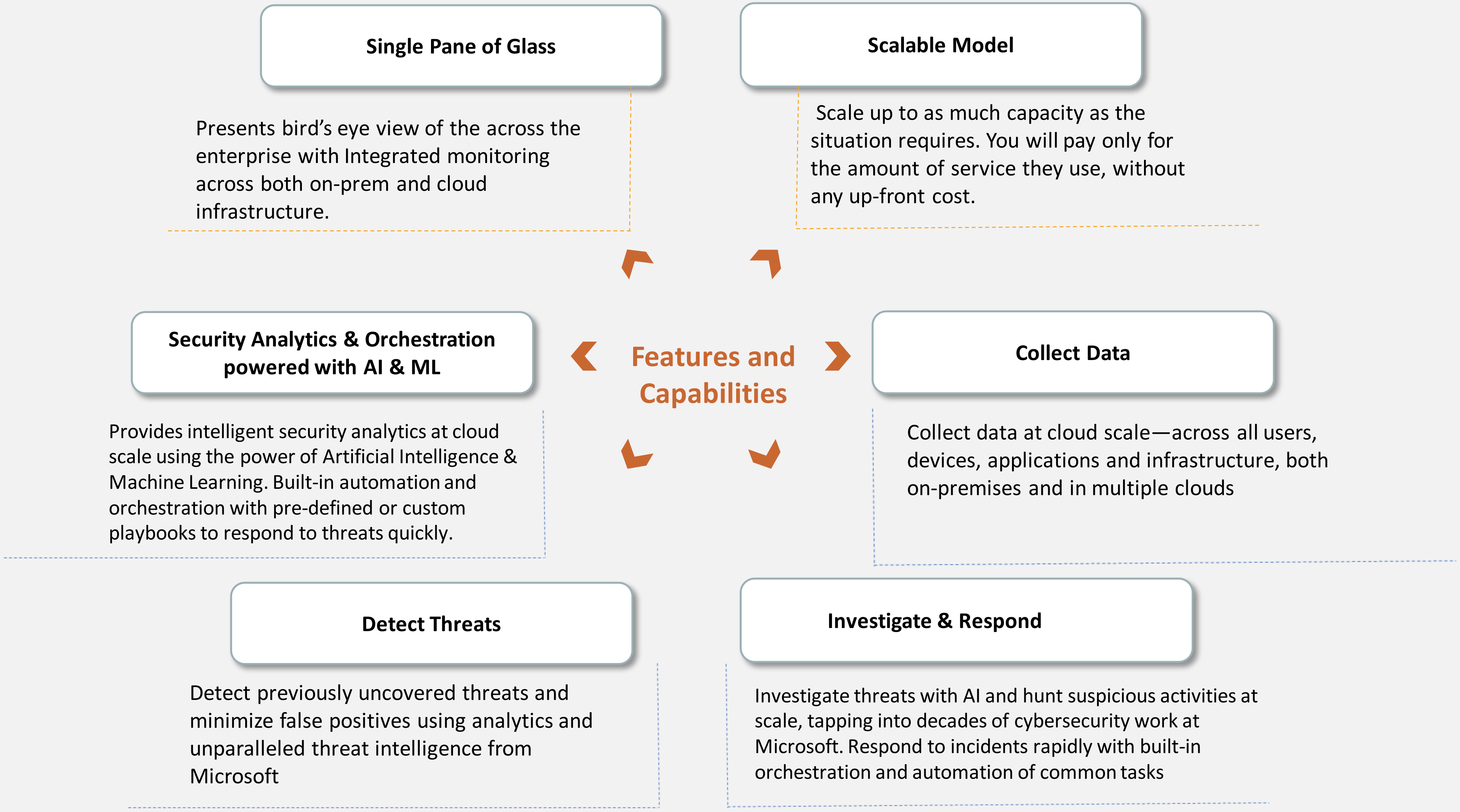
- Azure Sentinel can be integrated with Microsoft Graph Security API, which enables you to import your own threat intelligence feeds and customizing threat detection and alert rules.

Detection, Investigation, Automation & Response

- Azure Sentinel uses AI to detect real threats and provides built-in automation and orchestration with pre-defined or custom playbooks to solve repetitive tasks and to respond to threats quickly.

FEATURES AND CAPABILITIES OF AZURE SENTINEL

DELPHI
IT STRATEGY | CONSULTING | SUPPORT



Features and Capabilities

Single Pane of Glass

Presents bird's eye view of the across the enterprise with Integrated monitoring across both on-prem and cloud infrastructure.

Scalable Model

Scale up to as much capacity as the situation requires. You will pay only for the amount of service they use, without any up-front cost.

Security Analytics & Orchestration powered with AI & ML

Provides intelligent security analytics at cloud scale using the power of Artificial Intelligence & Machine Learning. Built-in automation and orchestration with pre-defined or custom playbooks to respond to threats quickly.

Collect Data

Collect data at cloud scale—across all users, devices, applications and infrastructure, both on-premises and in multiple clouds

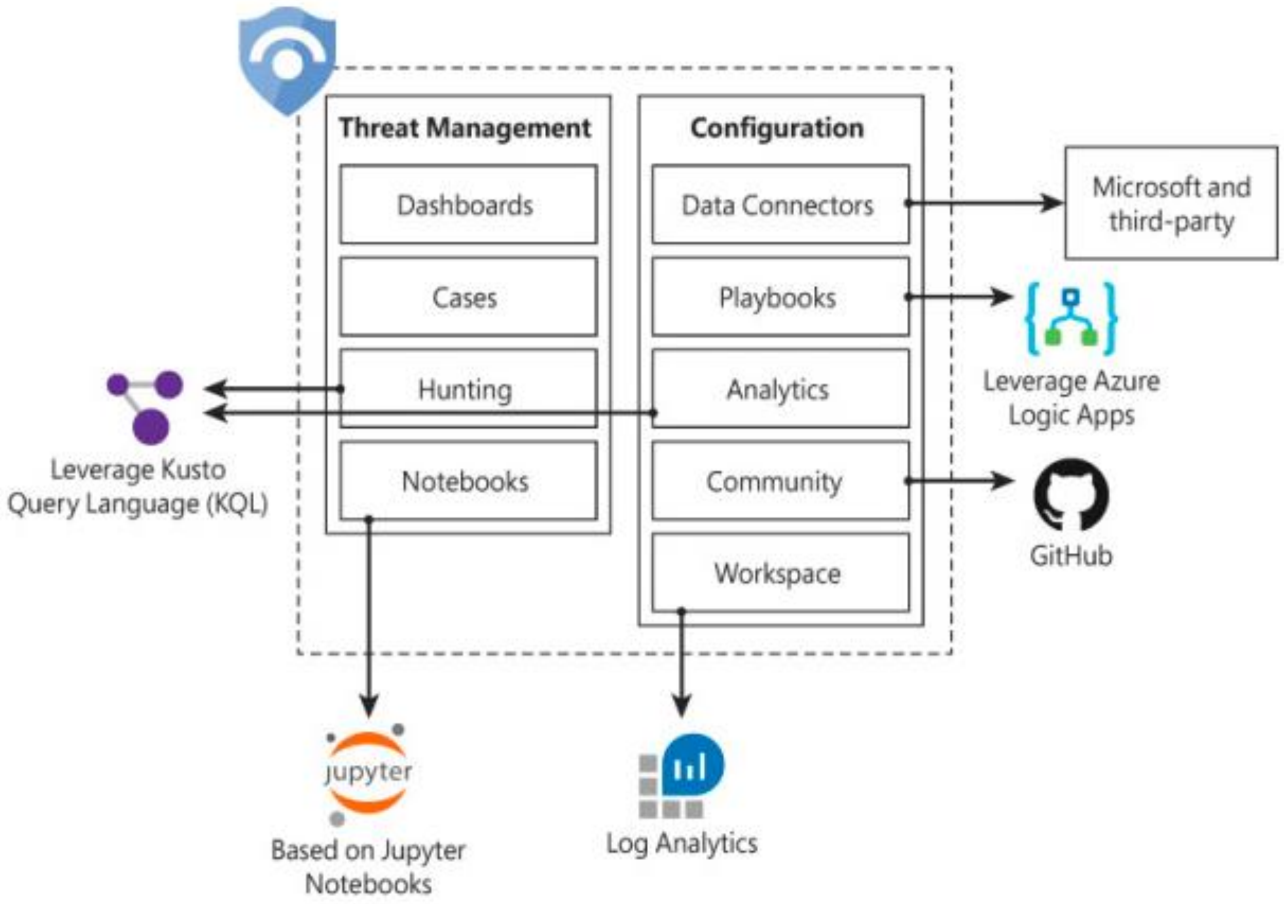
Detect Threats

Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft

Investigate & Respond

Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft. Respond to incidents rapidly with built-in orchestration and automation of common tasks

AZURE SENTINEL ARCHITECTURE



DELPHI
IT STRATEGY | CONSULTING | SUPPORT

CUSTOMER SUCCESS STORY:

ENHANCED THREAT PROTECTION FOR

THE FIRST GROUP

The First Group, Dubai's leading Properties & Real Estate Establishment, sought to gain deeper visibility with contextual insights into the existing threats across their organization.

Results:

- A unified approach to threat detection and response through Azure Sentinel.
- Complete visibility and continuous monitoring across the client's estate.
- Reduced false positives and alert 'noise' to focus on the real threats.

CONNECT WITH US TO KNOW MORE:

Get	Get a free trial: [delphime.com]
Call	Call for more information: [+971 56 253 1541]
Ask	Ask a Marketplace offer
Question	question via email: [security@delphime.com]
Learn	Learn more: [delphime.com]
Link	Link to your Microsoft Commercial (To be added)

DELPHI
IT STRATEGY | CONSULTING | SUPPORT