Microsoft

happiest minds
The Mindful IT Company
Born Digital . Born Agile

POWERING YOUR NEXT GEN SOC WITH Microsoft Sentinel

About Happiest Minds

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Next Generation Digital Transformation, Infrastructure, Security and Product Engineering Services Company

IPO
In September 2020

- 100 % digitally executed IPO
- Heavily oversubscribed with healthy listing gains

Reflects
- Our growth and profitability
- Management Team & Corporate governance

97%
Digital

94%
Agile

'Born Digital. Born Agile'

173+
Active clients

46 Fortune2000 / Forbes200 / Billion $ corporations

87%+ of repeat business

31.2%
RoCE[1]

29.8%
RoE

Mission Statement
Happiest People. Happiest Customers

SMILES Values
Sharing, Mindful, Integrity, Learning, Excellence, Social Responsibility

3,228+
Happiest Minds
across 7 Countries

Great Place To Work
- Ranked #4 - IT Services
- Top 50 India's Best Workplaces for Women
- Top 100 India's Best Workplaces
- Top 75 India's Best Workplaces for IT/IT-BPM

4.3
rating
on **Glassdoor**
#2 for Indian IT Services

Promoter

Ashok Soota

Great Place To Work. Certified APR 2020-MAR 2021 INDIA

RED HERRING ASIA 100 WINNER 2019

zinnov ZONES
Leaders – ER&D Services
Leaders - Education

PEOPLE FIRST IT'S ABOUT YOU!

HR Excellence Awards 2020

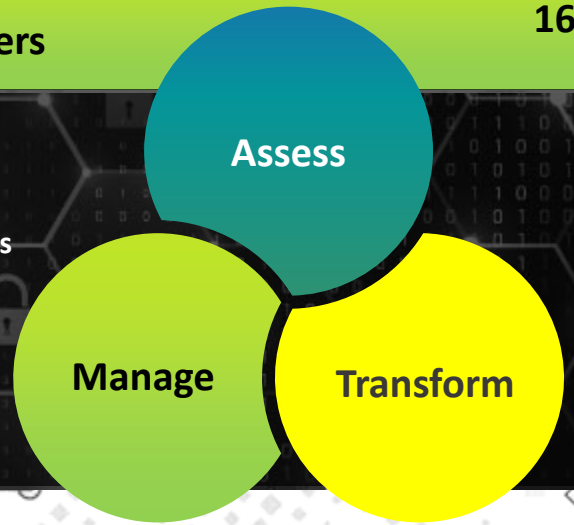
*All logos are properties of their respective owners Note 1 : ROCE / ROE is half year annualized

SECURITY SERVICES OVERVIEW

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Born Digital . Born Agile

300+ Smart minds | **60+ Customers** | **20+ Partners** | **16 Cities** | **8 Countries** | **Vendor Agnostic**



- Governance, risk & compliance Bcp/dr
- Infra security- Managed security Services (cloud and on prem)
- Identity & access management
- Advanced threat management (Security assurance)
- Managed detection and response (Edr, ndr, soc)
- Data & information security

NIST | SANS | COSO | COBIT 5 | ISO | MITRE ATT&CK | CREST | ITIL

Workstations | **Mobiles** | **DC Services** | **Networks** | **Cloud** | **IoT**

BFSI | **Retail** | **CPG** | **HiTech** | **Mfg/Industrial** | **Travel & Hosp.**

SECURITY SERVICES PORTFOLIO

happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

GOVERNANCE, RISK & COMPLIANCE

- IS policy Review /Remediation
- Compliance Consulting - ISO27001, ISMS, PCI-DSS, SOXITGC, SWIFT
- Risk assessment consulting - Cyber Risk, TPR, ASD, NESA, NIST
- Professional Services – Archer, Metric Stream, Galvanize, SNOW
- BCP/DR Consulting, Security Awareness Programs

MANAGED DETECTION RESPONSE

- Managed detection and respond (MDR)
- Managed Endpoint detection and response.
- OT/IT integrated security monitoring
- Cyber/Risk Analytics (UBA, NBA)
- End Point Threat Detection
- TI & Brand Monitoring as a service
- SOC operations & Incident management – 24*7, 8*5, dedicated / hybrid / shared

IDENTITY & ACCESS MANAGEMENT

- IDAM Consulting, Implementation, Ops Support
- Privilege Access-Implementation &Support
- Identity of Things(IOT)
- Cloud Access Security
- Multi-factor Authentication
- Identity Vigil (IDaaS) platform
- IDAM managed services (L1, L2)

ADVANCED THREAT MANAGEMENT

- Application Security Services
- Security Code Review
- Mobile Security Testing
- Network Security Assessment / VAPT
- Vulnerability Management
- IOT Security Testing
- Device Configuration Review
- Phishing simulation

DIGITAL RISK & DATA SECURITY

- Data Classification
- Data Leak Prevention
- Payment/Transaction Security
- PKI Management Services
- Encryption Services
- Secure File Transfer
- GDPR Remediation Services

INFRASTRUCTURE & CLOUD SECURITY

- Endpoint Security
- Network security
- Cloud infrastructure security
- Cloud compliance and workload protection
- Cloud based MDR services
- Security Baselining Consulting
- Cloud Security Assessment

OUR MDR SERVICES

happiest minds
The Mindful IT Company
Born Digital . Born Agile

HAPPIEST MINDS MDR AS A SERVICE

Consulting & engineering

- SOC 2.0 based maturity assessment and heat map.
- SOC 2.0 services design and implementation services
- SOC migration services.
- SOC services standardization
- Automation services – SOAR
- Automation use case definition and development
- Existing platform automation support

SOC as a Service

- SIEM based security correlation
- External threat intelligence integration
- Threat Intelligence & Brand Monitoring as a Service
- Orchestration and Automation as a Service
- Threat Intelligence; advisories; digital risk management.
- Deception techniques
- Red ream automation
- Threat hunting and Forensics
- Incident response and remediation

Security Automation as a Services

- Use case classification, grouping and qualification for Automation.
- Workflow and collaboration – Operational standardization
- Orchestration and Automation
- Threat Intelligence management.
- Overall security incident ticketing and case management.

EDR as a Service

- NGAV ,Anti Ransomware
- EDR with AI –ML based detection
- Threat hunting and Forensics
- Support containment and remediation of incidents qualified by your SOC
- Forensics investigation with breach impact analysis .
- Support Incident response automation

NDR/UEBA as a Service

- User and Entity Behavioral Analytics
- Network behavioral analytics
- Malicious network activities
- Phishing attack detection
- Command and control communications
- Threat hunting and Forensics
- Incident Detection and remediation services

CORTEX XSOAR · Microsoft · IBM Radar · RAPID7 · splunk> · FORTINET · Microsoft · FIREEYE · DARKTRACE · splunk> · SIEMPLIFY · McAfee · Recorded Future · Resilient · Cymulate · Carbon Black. · CROWDSTRIKE · Microsoft · SECURONIX

AZURE SENTINEL SERVICES

- Solution value proposition to Customers
- Proof of Concept (PoC)
- Existing estate Maturity Assessment

.

- Technical Solution Design:
- Implementation/Rollout of services
- Existing Environment Enhancements
- Security monitoring Gap assessments:

- Security monitoring services rollout
- Security Incident response, reporting and remediation.
- Ongoing Platform engineering:

SOC 2.0 – WITH AZURE SECURITY

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Knowledge base
SIRT training templates

Experts at work
24*7 Incident detection and response experts Threat hunting

- Passive TI
- External Threat advisories

Proactive

Deception tools
User Awareness

TI Feeds;
Dark web

Security Testing
Prioritization

Predictive

SOAR

Azure Sentinel

SIEM

Adaptive

UEBA

EDR

NDR

- Azure Sentinel
- **BYOML**

- Azure Defender

- Azure ATA
- Azure ATP

- MISP/Open CTI
- Commercial TIP

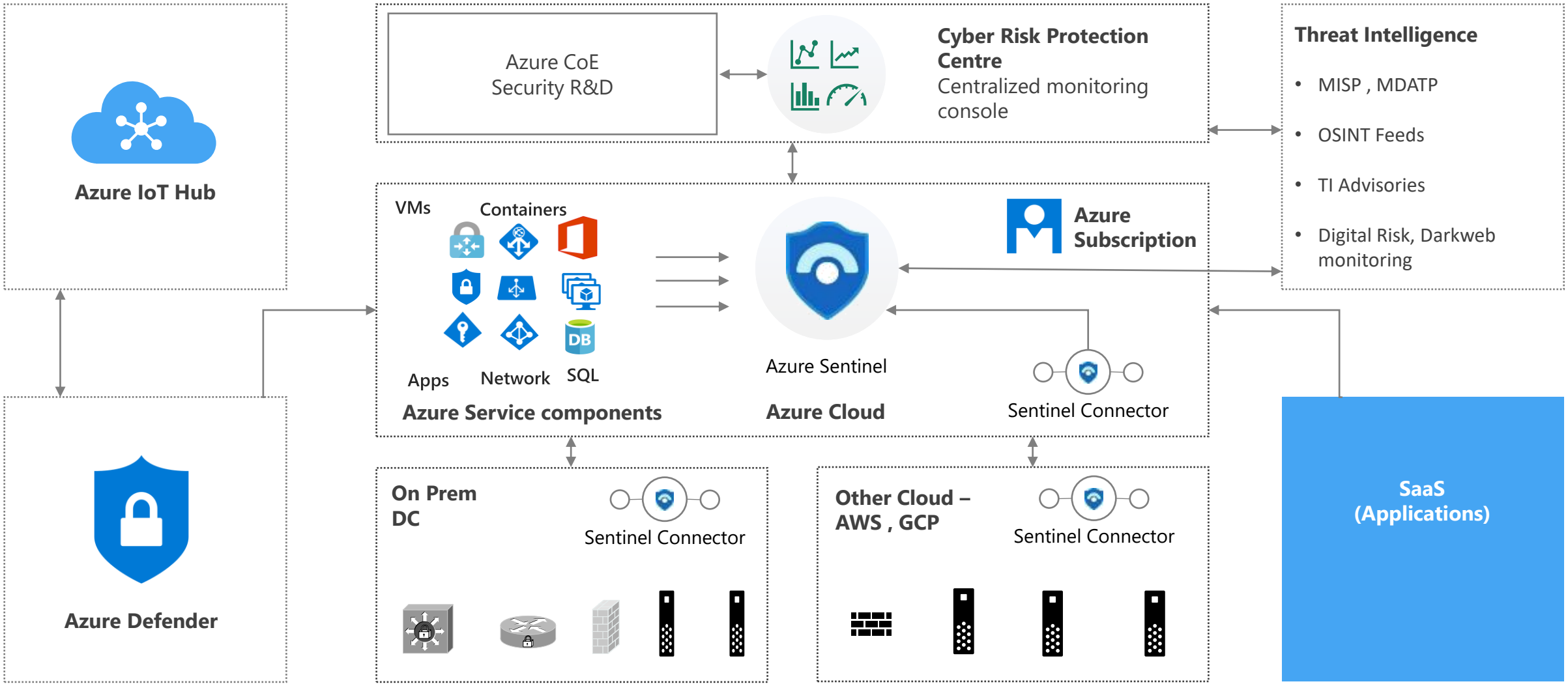
- AZ Secure Devops Kit

- Defender TVM
- Attack Surface reduction
- Vulnerability prioritizatio

Windows & Unix | Firewalls/WAF | AV,EDR, | O365 | Vulnerability DB

IAM/PAM | Web/Email gateways | DNS, DHCP, AD | SaaS applications | Azure components

SENTINEL SOC ARCHITECTURE



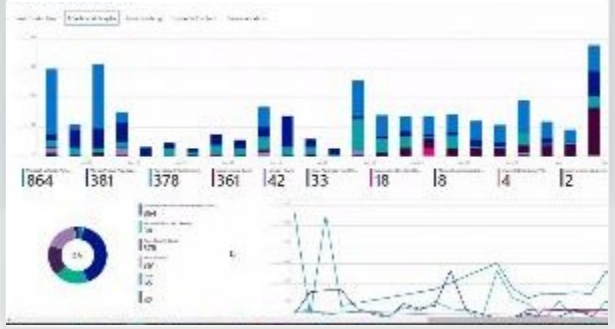
VISIBILITY

Incident overview

- Incident overview
- Threat Visualization

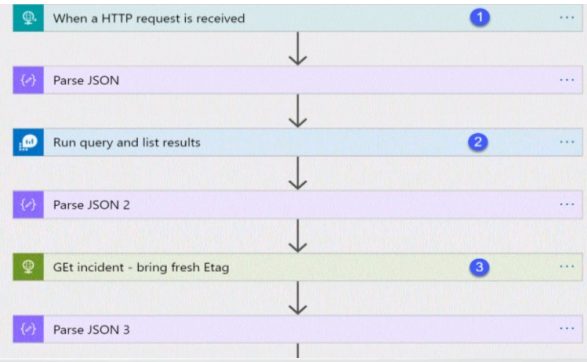
Workbooks

- 106 Built in workbooks
- Customer specific workbooks
- Customized visibility

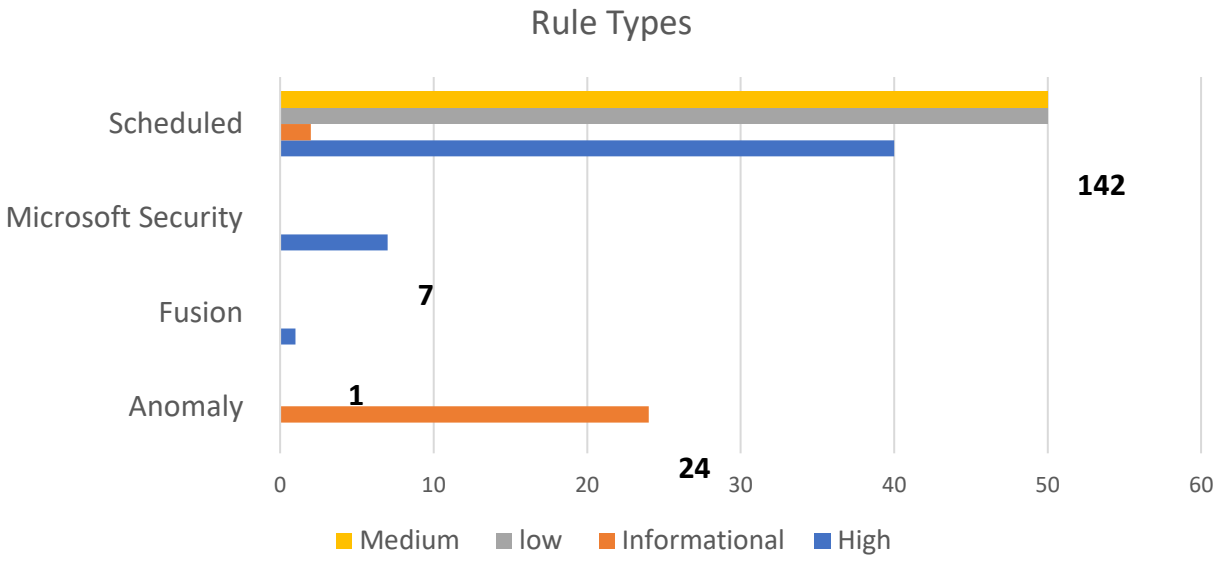


Incident handling - ITSM

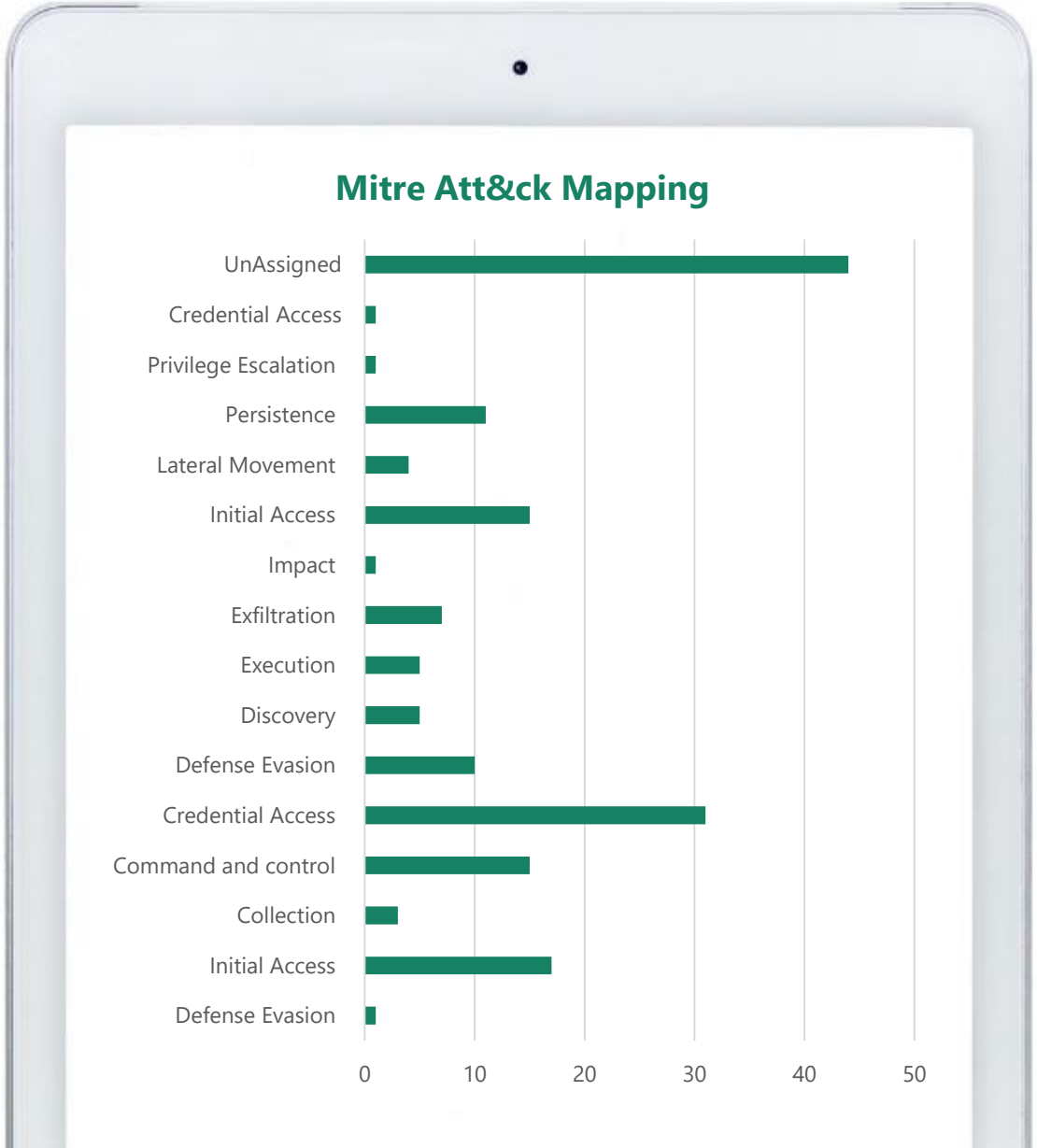
- SNOW integration
- Bidirectional sync through logic Apps



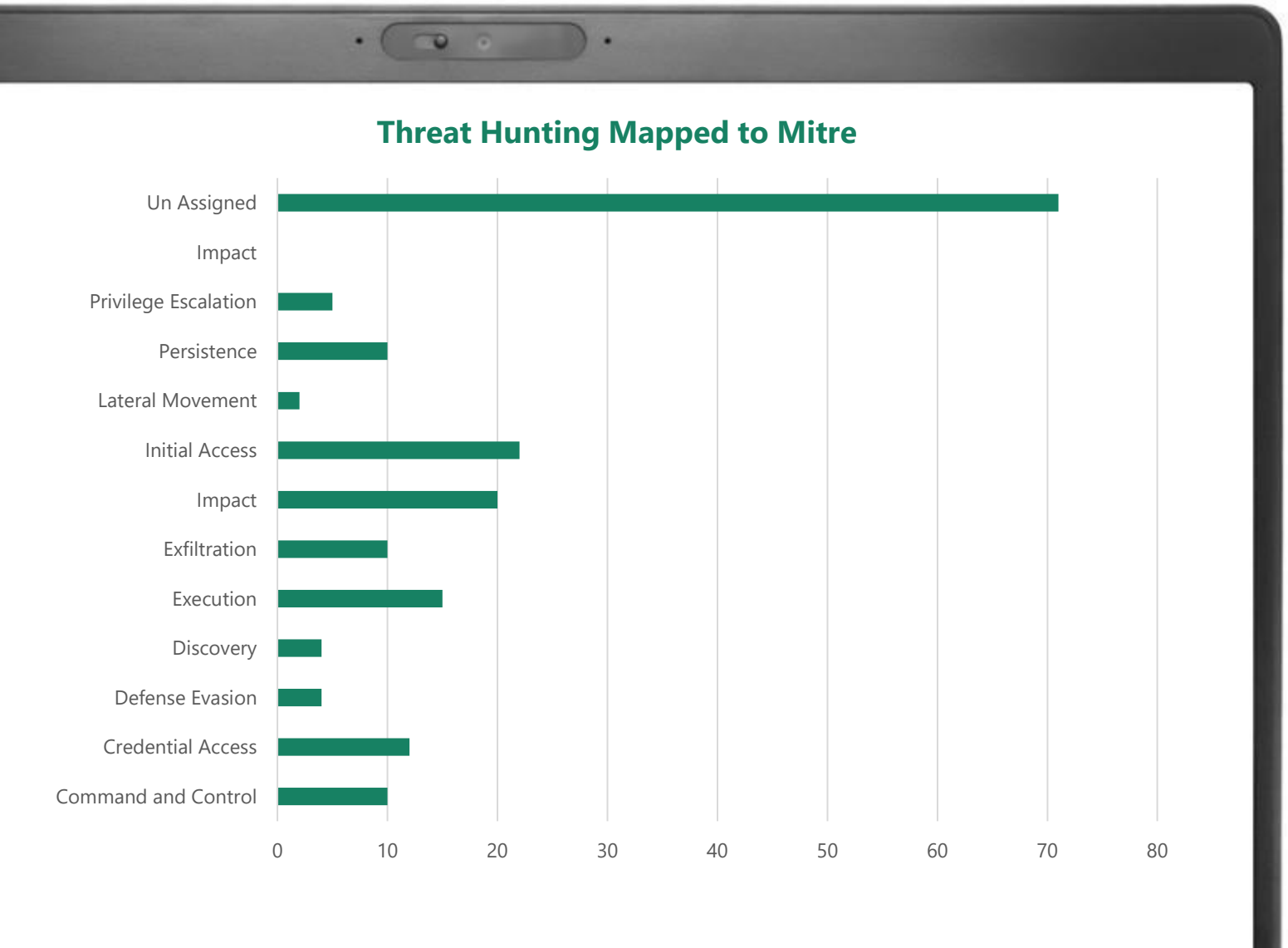
DETECTION- ANALYTICAL RULES



- ✓ Customer specific rule activation
- ✓ Fine tuning of rules based on customer data sources
- ✓ Customization based on 150+ MSSP rulesets built on Mitre TTPs
- ✓ Customer specific rules, ML



DETECTION – THREAT HUNTING

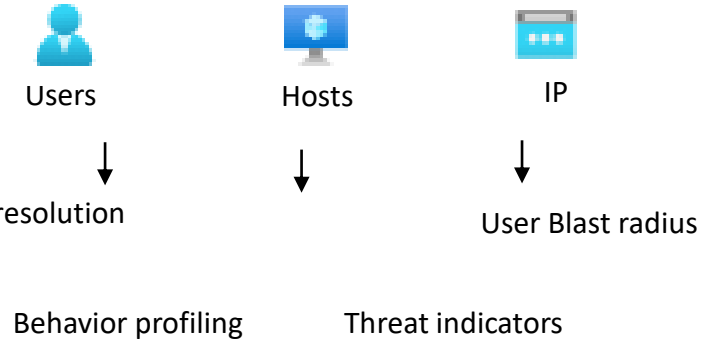


- Hypothesis Driven - Related TTP's and IOCs analysis using MITRE Att&ck and Framework
- Situational awareness - Crown Jewel analysis (identification of an organization's critical assets)
- Intelligence Driven - Threat intelligence feeds, advisories

DETECTION – AI & ML

Built In

- ✓ Analytics built on ML
- ✓ UEBA



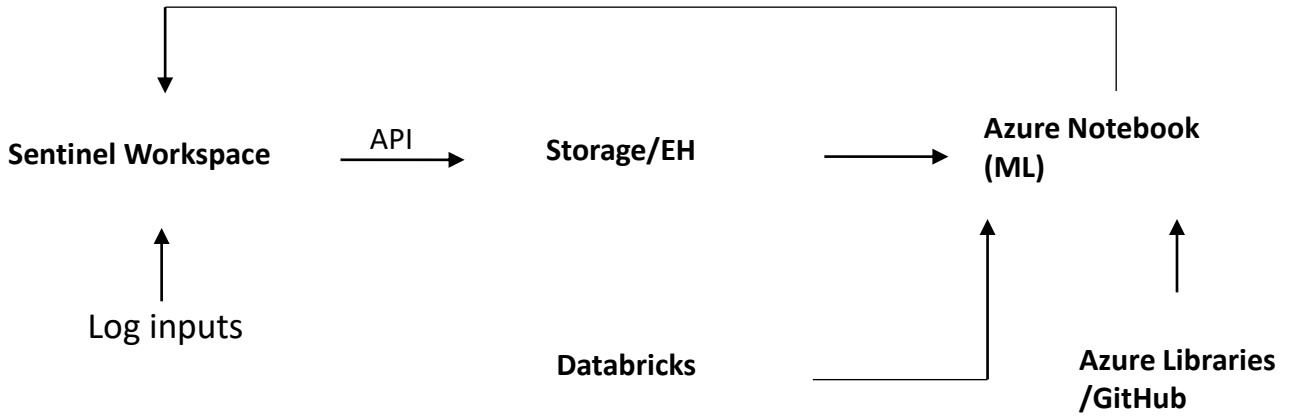
ML For SOC Analysts

- ✓ Security Triaging, Visualizations
- ✓ External data references

BYOML

Data Scientists

- ✓ Custom data sets and analytics
- ✓ Business driven security analytics



RESPOND - AUTOMATION

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Phase wise approach for optimum Security Automation

Identify

- ✓ Identify and classify alerts
- ✓ Qualify alerts for automation

Use case Category 1- Critical	Use case Category 2- Volume	Use case Category 3- Time consumed
Compromise: Account Added to Admin Group	AIE: Office 365: Unique Users Authenticated from Single IP	Threat hunting- IOC IP
Palo Alto: Network Scan Detected	AIE: Proxy : Phishing URL Detected	Threat hunting- IOC File
AIE: NetApp: Insufficient Disk	McAfee: Malware Outbreak	Threat hunting- IOC URL

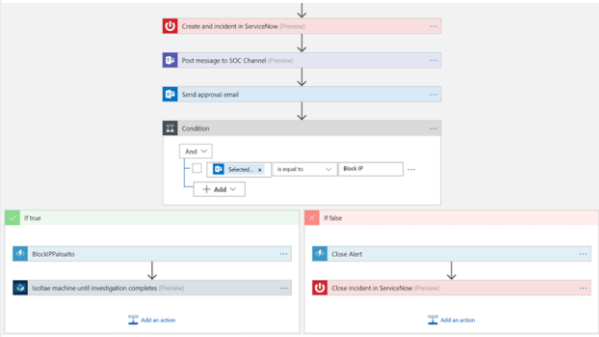
Define

- ✓ Define Data Sources
- ✓ Define actions and workflow

Use case	Action	Dependency
Compromise: Account Added to Admin Group	Extract user name from raw logs	SIEM smart response
	Condition	SIEM smart response
	Email notification	Email gateway
	Query to run search on user in SIEM	SIEM smart response
	Disable user from AD	Active directory
Network External scan	Extract IP's , ports	SIEM smart response
	Query to run search for alerts on IP in SIEM	SIEM smart response
	Query to check history of IP in SIEM	SIEM smart response
	Query for outbound traffic	SIEM smart response
	IP reputation check	Threat intel
	IP block with approval	Palo alto firewall
	Extracting IP's, ports, host	SIEM smart response

Execute

- ✓ Execute automation
- ✓ Test automation
- ✓ Finetune



METHODOLOGY AND TIMELINE

Assess	Define	Implement	Normalize	Monitor
1 Weeks	1 Weeks	4 to 6 Weeks	2 to 4 Weeks	Ongoing process
• Understand Existing Architecture and Setup. • Understand existing security monitoring setup • Understand existing security incident response process • Understand secure connectivity details	• Design Architecture • Define Project plan • Define plan to integrate Azure Native and On-prem devices • Define Data connectors' mapping against Log Sources • Identify Analytics Rules	• Connect Log Sources using in-built Data Connectors, develop custom Data Connectors (if required), parsing (if required) • Develop custom use cases by KQL and enable in-built use cases • Implement Playbook to take automatic actions	• Observation phase – Normal functioning • Fine tuning of watchlist & Filter. • Response automation testing • Reports and dashboards	• Alert Notification • Newsletter • Trending malware & ransomware • Weekly, Monthly & Quarterly Reports • Prioritized vulnerability patching list. • Periodic reporting and review • Governance Review Meeting
CUSTOMER RESPONSIBILITY				
• Provide understanding of Existing architecture • Provide Existing SOC environment and Process details	• Review and signoff submitted doc • Acceptance of the In-Scope Devices	• Change approval • Underlying infrastructure provisioning • Support remote agent deployment. • Secure Connectivity initiation	• SOC Integration coordination	• Review reporting and feedback

SOC 2.0 SERVICES -SENTINEL

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Security Incident monitoring response & Remediation

- Incident monitoring
- Remediation support
- Threat Hunting
- Response Automation
- Threat Intelligence
- Digital risk/Dark web monitoring

Predictive

- SIEM - Sentinel
- SOAR – Built in
- Event source integration

Proactive

- Deception tools
- Red teaming
- Vulnerability Prioritization – MS ATP
- Threat intelligence – MISP, MSATP
- User awareness training
- Digital risk/Dark web monitoring Platform

Adaptive

- EDR – MS ATP
- NDR – MS ATA
- UEBA - Azure

Event Sources

- Windows & Unix
- Firewalls/WAF
- AV,EDR,
- O365
- Vulnerability DB
- IAM/PAM
- Web/Email gateways
- DNS, DHCP, AD
- SaaS applications
- Azure components

Support Services

24*7 Monitoring, triaging analysis and reporting.

SLA based monitoring and tracking

Threat Hunting

Periodic reporting.

Forensics and IR retainer

Response Automation

- Logs forwarded to SOC platforms

Happiest Minds Services using Azure security solutions

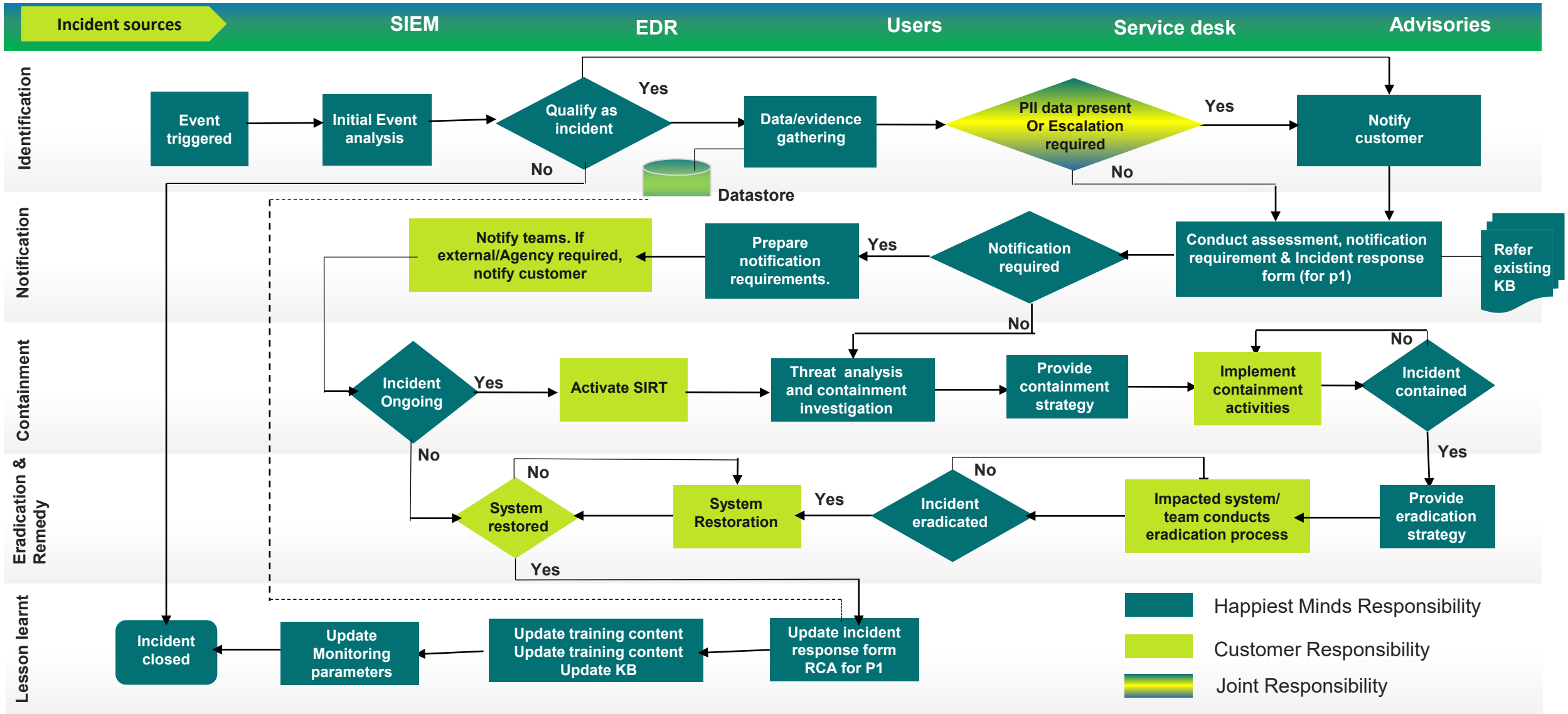
Happiest Minds Services addon using Third-party security solutions

Typical Log Sources

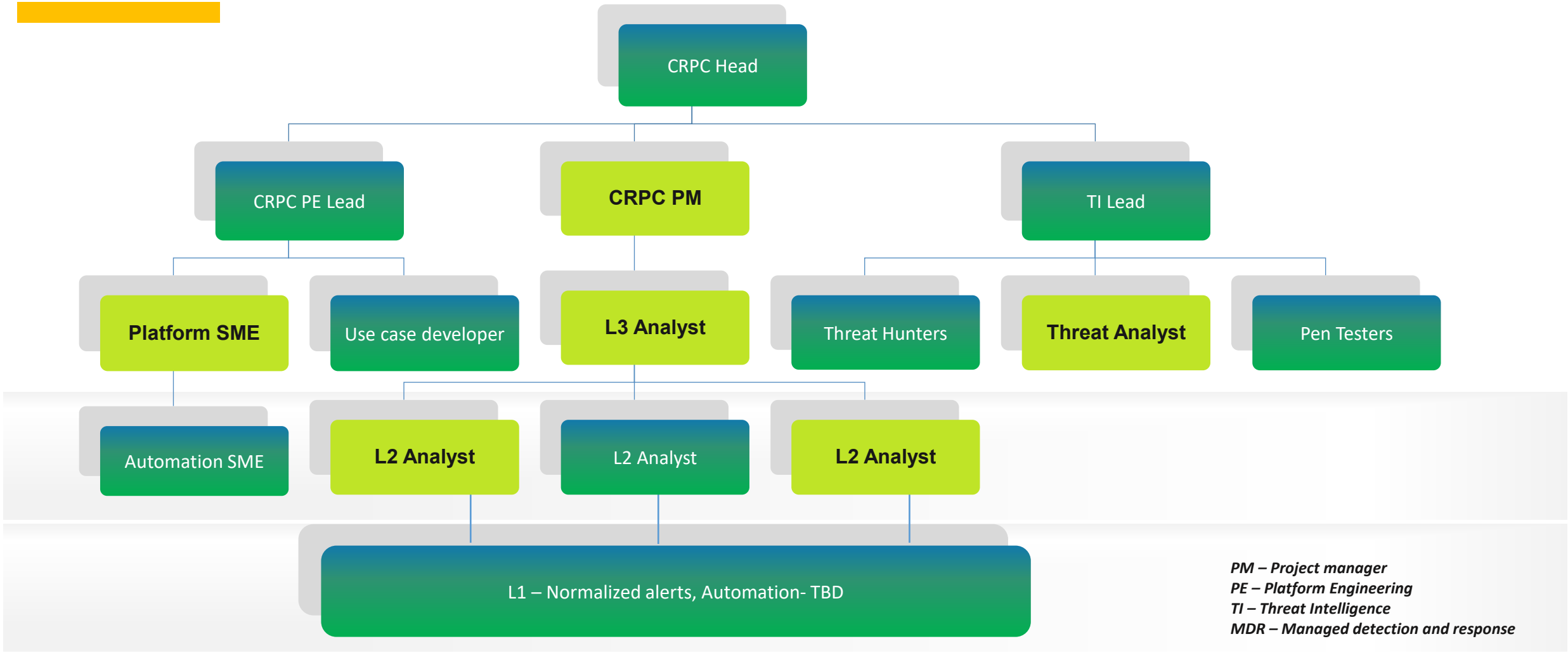
INDICATIVE SLA

Critical Service Level Category	Response Time	Expected Service Level	Remarks
Steady State 24/7 Security Monitoring and Management Services			• P1 – Successful Attack, compromise, Virus outbreak etc. • P2 – High Priority Alert from integrated devices, Policy Violations, multiple scans • P3-Low Priority Alerts from integrated devices, limited scan, recon, infections etc.
Service outage notification (P1)	30 Mins	99.00%	
P1 Incident detection case creation	15 Mins	99.00%	
P1 Incident remediation case up-dation	45 Mins	99.00%	
P2 Incident detection case creation	1 Hrs	96.00%	
P2 Incident remediation case update	4 Hrs	96.00%	
P3 Incident detection case creation	4 Hrs	94.00%	
P3 Incident remediation case update	8 Hrs	94.00%	

INDICATIVE SLA



CRPC TEAM STRUCTURE



PM – Project manager
PE – Platform Engineering
TI – Threat Intelligence
MDR – Managed detection and response

PROJECT MANAGEMENT AND GOVERANCE

happiest minds
The Mindful IT Company
Born Digital . Born Agile

- Strategic Review – Quarterly
- Relationship Management
- Business Continuity
- Go/No-go for initiatives

- Program Review – Monthly
- Service Delivery Improvement
- Program Prioritization
- Discuss risks / issues
- Take corrective actions

- Project Review – Weekly Execution
- Daily incident reports
- Reporting

- Transition Review – Weekly Status
- People, Process, Tool mapping
- Reporting

Customer	Happiest Minds
Business Executive PMO Business Sponsor	Global Del.Head / GEO Delivery Head, Account Executive
Program Manager	Off. Delivery Head Account Delivery Mgr.
Project Leads Program Manager	Tower Leads Project Manager
Transition Manager Service Manager	Transition Manager Account Delivery Manager Project Manager

MANAGED AZURE SENTINEL SERVICES

Azure Sentinel Managed Service offerings			
Services	**Silver**	**Gold**	**Platinum**
▪ Service Window	8*5	24*7	24*7
▪ Environment Assessment	√	√	√
▪ Design and Implementation	√	√	√
▪ Out-of-Box Integration and Analytics Rules	√	√	√
▪ Enabling Default Analytics and Playbooks	√	√	√
▪ Out of the box Automation use cases	√	√	√
▪ Out of the box Dashboards	√	√	√
▪ Recommendations to Remediate	√	√	√
▪ Out of the box reports	√	√	√
▪ Custom Log Sources integration	Up to 2	Up to 3	Up to 5
▪ Custom Workbooks and Automation use cases	None	Upto 5	Upto 10
▪ Weekly / Monthly Service review	√	√	√
▪ Quarterly Governance review with leadership	X	X	√
▪ Customized Reports	X	X	√
▪ Threat Hunting with In-Built Queries and HM Native Tools	X	X	√
▪ Custom Analytics Rules based on MITRE Framework	X	X	√
▪ Remediation support	X	√	√

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Sample Case Studies

CASE STUDY

Azure Sentinel PoC Engagement

A Private Foundation in US

About Customer

One of the large NGO based company in US, with coverage across globe. Has offices in multiple countries in Africa, Americas and APAC

Strategy & Objectives

- Limited set of default integrations additional effort required for building API.
- Default correlation rules mostly around Microsoft solutions, and more customizations required.
- Dashboards are limited without drill down options
- Technical support resolution time is higher considering it being a new solution in the market.

Service Offered

Integration and Configuration of Azure Sentinel and associated use cases including

- **In scope device integration**: Cisco Meraki, Carbon black, Microsoft ATA, Crowdstrike, O365, MS cloud App Security, Domain controller, Cisco ISE, Cisco Umbrella and Okta.
- **Integration for unsupported devices:** Cisco Meraki, Carbon black, Crowdstrike, controller, Cisco Umbrella and Okta
- **Custom Parser creation:** Cisco Umbrella, Crowdstrike, Carbon black and Okta

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Digital Security Delivered

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

Detect previously undetected threats, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft

Respond to incidents rapidly with built-in orchestration and automation of common tasks

CASE STUDY

Azure Sentinel Optimization

A Leading energy and multi-technical service provider

About Customer

Company operates in three main service and utility areas traditionally managed by public authorities – water and waste management and energy services

Strategy & Objectives

- Limited set of integrations Additional effort required for building API.
- Correlation rules are mostly around Microsoft solutions, more customizations required.
- Dashboards are limited without drill down options
- Technical support resolution is higher considering its time in the market

Service Offered

Integration and Configuration of Azure Sentinel and associated use cases including

- **In scope device integration**: Office365 – Audit Logs and MessageTraceLogs, Azure Active Directory, Security Events, Windows Logs, Fortinet Firewall Logs, NSG Logs, Azure Blob Storage Logs
- **Integration for unsupported devices:** MessageTraceLogs, NSG logs, Azure Blob Storage Logs, PowerShell scripting
- **Custom Parser created for:** MessageTraceLogs

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Digital Security Delivered

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

Detect previously undetected threats, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft

Respond to incidents rapidly with built-in orchestration and automation of common tasks