



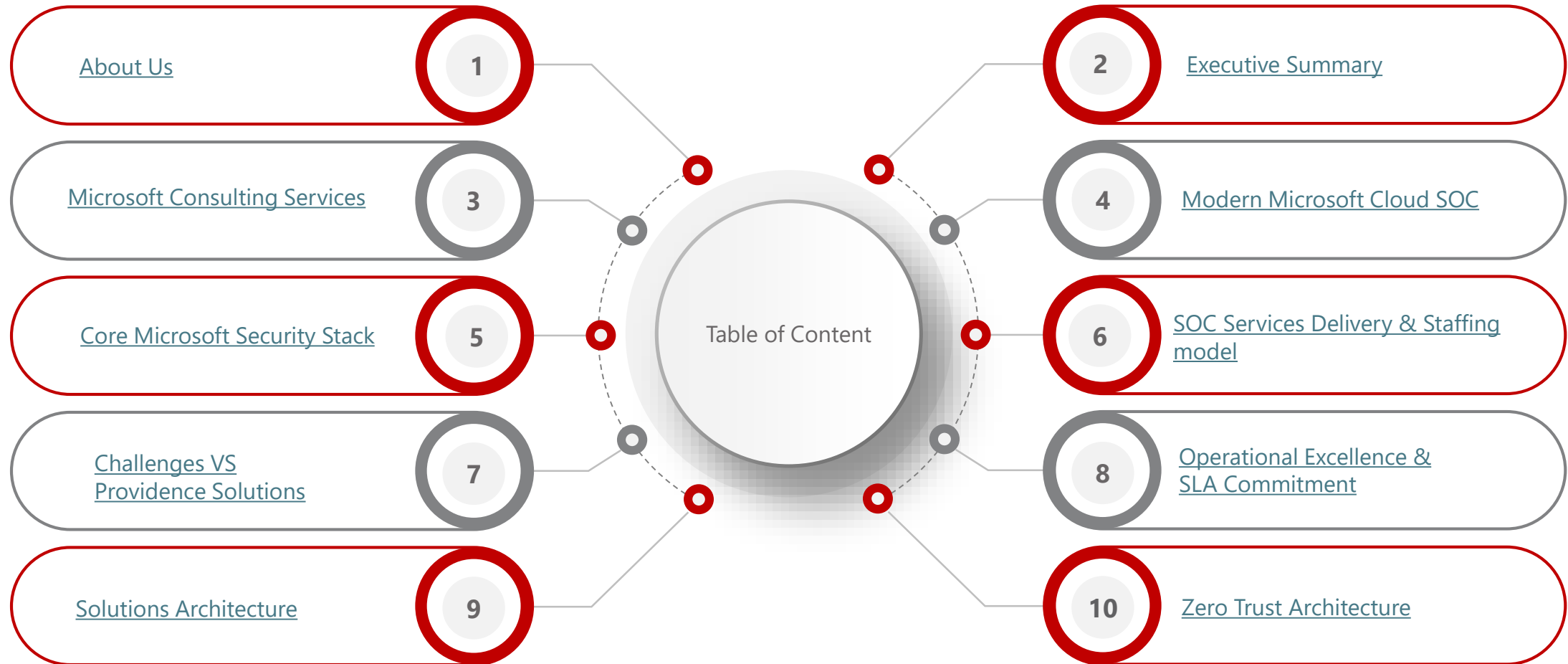
MICROSOFT SECURITY OPERATIONS CENTRE

AI-Driven Security Operations Centre (SOC)



Providence
Software Solutions

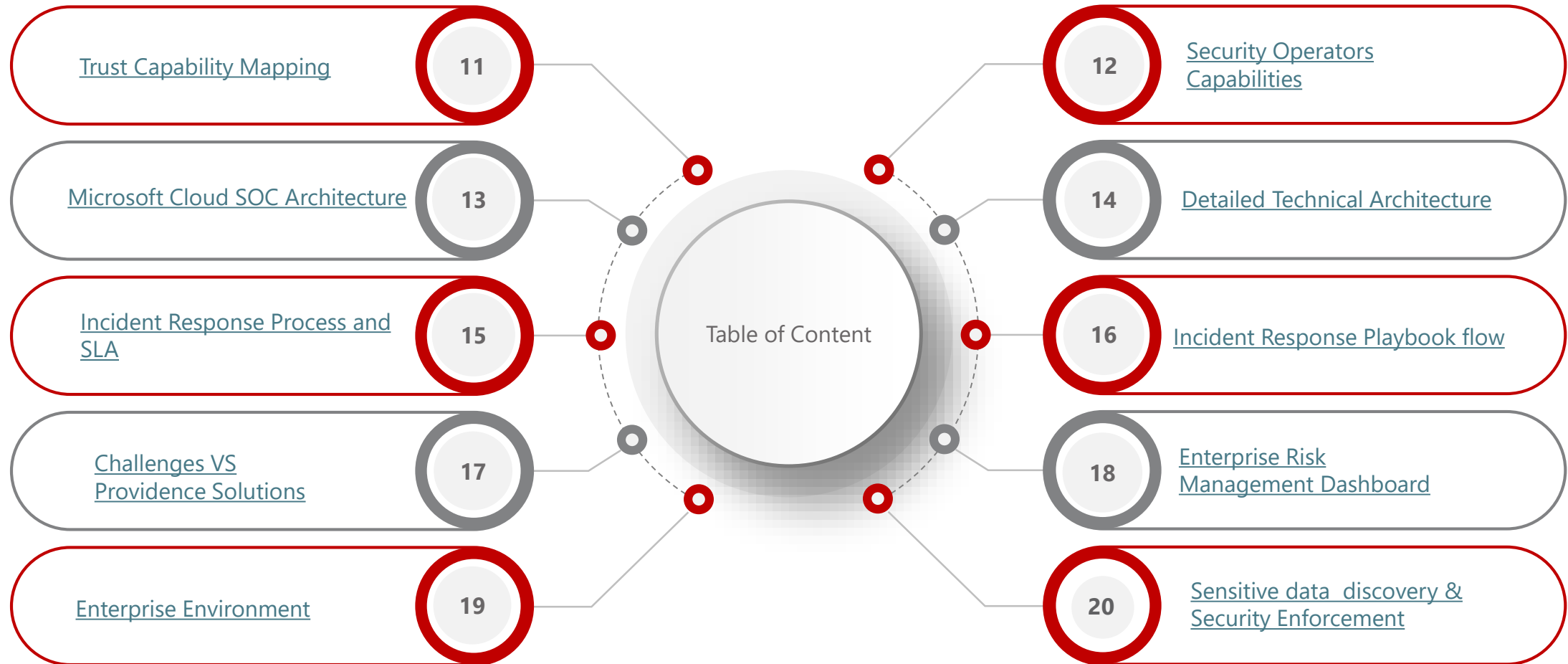
TABLE OF CONTENTS



The diagram features a central grey circle with the text "Table of Content". Ten lines radiate from this center to ten numbered circles (1-10) arranged in two columns. Each numbered circle is connected to a rounded rectangular box containing a page number and a title. Circles 1, 2, 5, 6, 9, and 10 have red borders, while circles 3, 4, 7, and 8 have grey borders. The boxes for 1, 2, 5, 6, 9, and 10 also have red borders, while the others have grey borders.

About Us	1	2	Executive Summary
Microsoft Consulting Services	3	4	Modern Microsoft Cloud SOC
Core Microsoft Security Stack	5	6	SOC Services Delivery & Staffing model
Challenges VS Providence Solutions	7	8	Operational Excellence & SLA Commitment
Solutions Architecture	9	10	Zero Trust Architecture

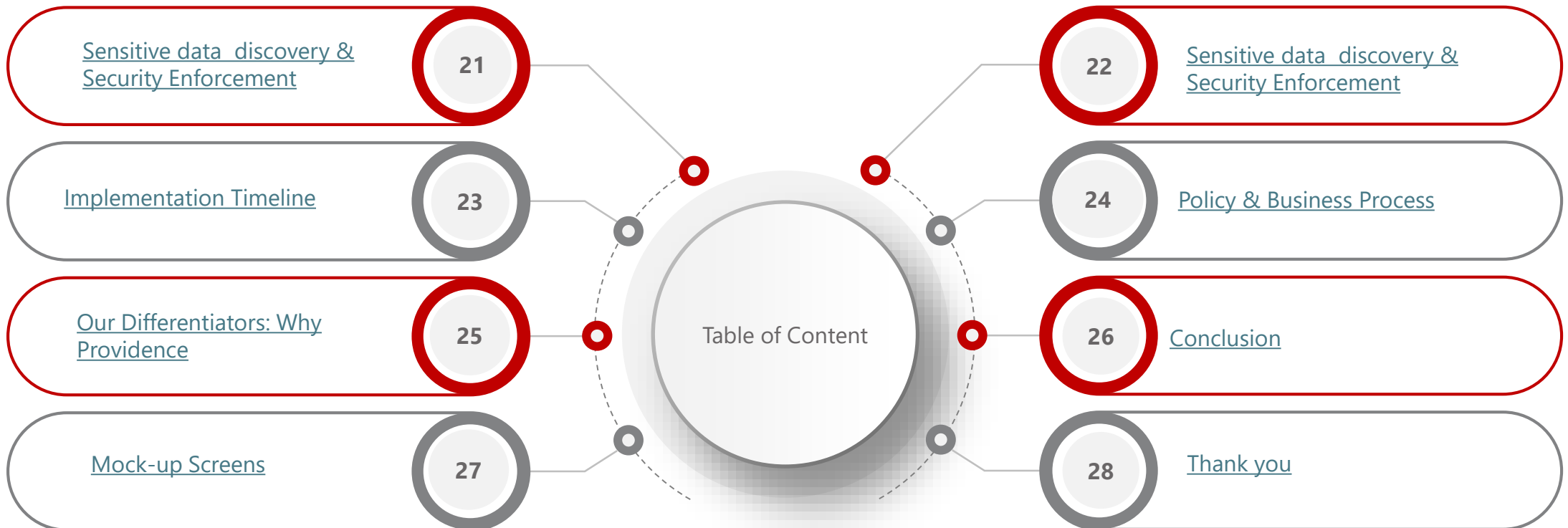
TABLE OF CONTENTS CONT...



The diagram features a central grey circle labeled "Table of Content". Ten lines radiate from this center to ten numbered circles (11-20) arranged in two columns. Each numbered circle is connected to a rounded rectangular box containing a title. Circles 11, 12, 15, 16, 19, and 20 have a thick red border, while circles 13, 14, 17, and 18 have a grey border. The titles are underlined in the original image.

Trust Capability Mapping	11	12	Security Operators Capabilities
Microsoft Cloud SOC Architecture	13	14	Detailed Technical Architecture
Incident Response Process and SLA	15	16	Incident Response Playbook flow
Challenges VS Providence Solutions	17	18	Enterprise Risk Management Dashboard
Enterprise Environment	19	20	Sensitive data discovery & Security Enforcement

TABLE OF CONTENTS CONT...



Sensitive data discovery & Security Enforcement	21	22	Sensitive data discovery & Security Enforcement
Implementation Timeline	23	24	Policy & Business Process
Our Differentiators: Why Providence	25	26	Conclusion
Mock-up Screens	27	28	Thank you

DISCLAIMER

The information shared in this presentation regarding the Microsoft Security Operations Center (SOC) is for informational purposes only. The content provided reflects the current capabilities, features, and potential benefits of the Microsoft Security Operations Center (SOC) as of the time of the presentation. While every effort has been made to ensure the accuracy, reliability, and relevance of the information, no guarantees are made regarding the completeness or timeliness of the data presented.

This presentation is not intended to be a comprehensive guide or definitive recommendation regarding Microsoft Security Operations Center (SOC). The views expressed herein are based on the present functionality and scope of the solution, which may evolve or change over time as it undergoes further development or updates. As such, features, capabilities, and pricing may be subject to revision.

The solution discussed is designed to address certain use cases within digital workplace environments, but its applicability to specific organizations or industries should be assessed independently. The effectiveness of the solution will depend on the specific needs, technological environment, and compliance requirements of each organization.

Providence Software Solutions and any associated parties make no representations or warranties regarding the future performance or suitability of Microsoft Security Operations Center (SOC) for any specific organization or industry. The information provided does not constitute legal, business, or professional advice, and attendees are encouraged to consult with experts in their respective fields before making any decisions based on the content presented.

Neither Providence Software Solutions nor any associated companies will be liable for any direct, indirect, or consequential damages resulting from the use or reliance on the information presented during this session. The implementation and integration of Microsoft Security Operations Center (SOC) should be done in consultation with qualified professionals to ensure compatibility, security, and compliance with applicable regulations.

By attending this presentation, you acknowledge that the information presented is subject to change and that Providence Software Solutions is not responsible for any errors, omissions, or misinterpretations in the content. It is recommended that organizations conduct a thorough evaluation of any Microsoft Security Operations Center (SOC) before implementation.

COMPANY INFORMATION

Business Name : Providence Software Solutions (Pty) Ltd
Company Registration Number : 2005/028399/07
VAT Number : 4580254615
Contact Person : Prabhakar Manikonda
Contact Number : +27 (0) 87-711-5555
E-mail Address : info@providencesoft.co.za
Mobile Number : +27 78 862 6506
Physical Address : 35 Western Service Road, Woodmead, Sandton,
Johannesburg, South Africa, 2148
Postal Address : PostNet Suite 201, Private Bag X23, Gallo Manor,
Sandton 2052



About Us — — —

WHY TRUST US

20+ YEARS INDUSTRY
EXPERIENCE

1000+ COMPLETED
PROJECTS

LEVEL 1 B-BBEE
COMPLIANCE

GRC DEDICATED
DEPARTMENT



About Us — — —

OUR SERVICES



CUSTOM SOFTWARE SOLUTIONS

We create tailored software solutions that innovate by leveraging cutting-edge technologies to drive efficiency, scalability, and competitive advantage



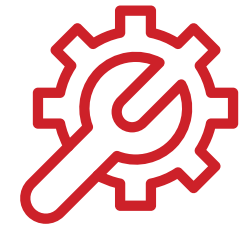
COMPLIANCE

Our GRC services ensure your operations meet industry standards while mitigating risks and safeguarding data integrity



INFRASTRUCTURE

We build and optimize secure, scalable IT infrastructure that future-proof your operations and ensure seamless performance, uptime, and disaster recovery.



MAINTENANCE & SUPPORT

Our support and maintenance team ensure your systems stay agile, secure and up-to-date, minimizing downtime and allowing your team to focus on innovation

“CUSTOMER SATISFACTION THROUGH PERFECTION”

Four words from which **PROVIDENCE** derives its soul

VISION

Providence aims to provide premier advisory services to its clients by shaping them to become industry leaders. This is done through providing them with a competitive edge in transformation, quality management systems, operational systems as well as risk management systems.

MISSION

Providence aims to achieve customer delight through excellence in all we do, by offering world class services in assisting our customers to create an IT environment that provides a stable platform to enable informed management decisions that drives business profitability.

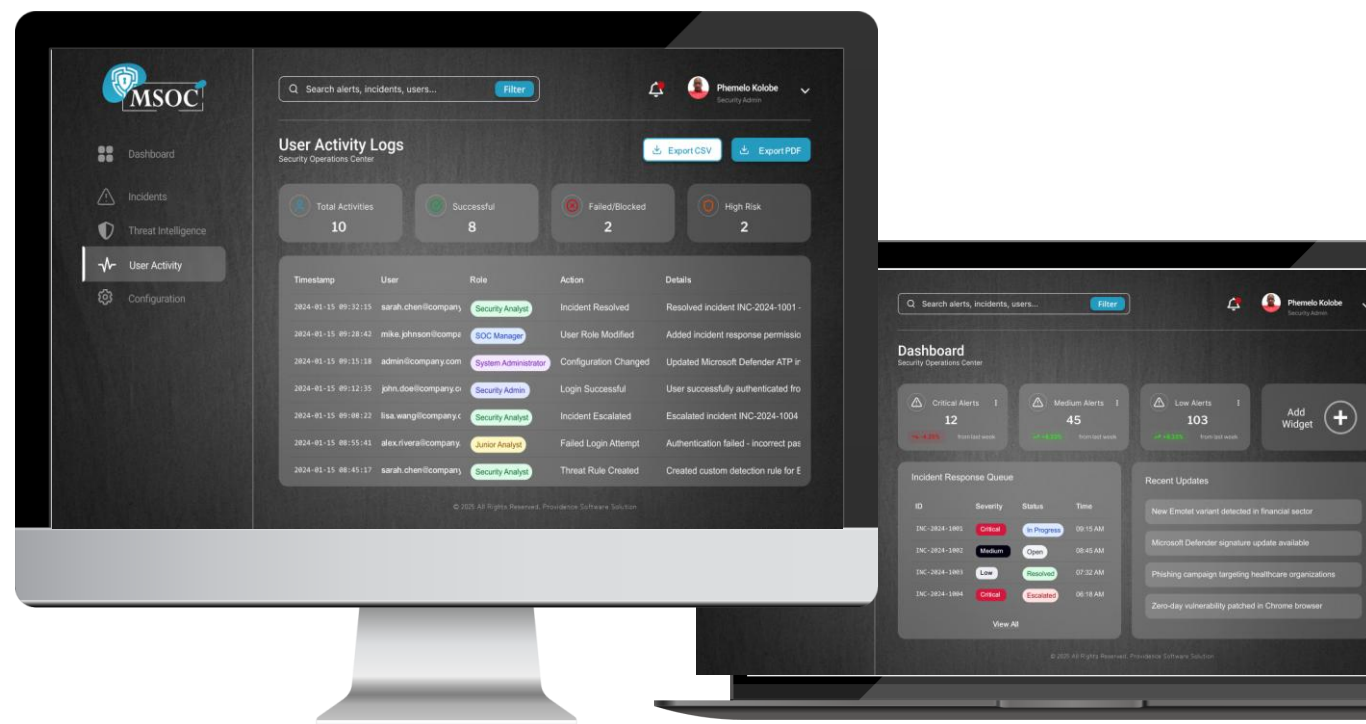
PROMISE

- Co-creation of innovative ideas and high impact results to our clients.
- Creation of lasting benefits in the societies and communities we live in.
- Ensure above market growth and value for our clients and stakeholders.
- Providing the highest standard of quality.
- Exemplary quality assurance practices providing seamless, worry-free control throughout the duration of a project and beyond.

EXECUTIVE SUMMARY

Providence Software Solutions proposes the implementation of a modern, AI-driven Security Operations Center (SOC) leveraging the Microsoft Cloud security stack. This solution is designed to protect your IT ecosystem from central data centers to every courtroom(s) providing 24/7 threat detection, automated response, and robust compliance with POPIA/GDPR, and ISO 27001: Information Security Management Systems (ISMS).

Our partnership model emphasizes skills transfer and co-management, ensuring we build internal capability while benefiting from our deep expertise as a Microsoft Gold Partner / Solutions Partner and ISO 27001-certified service provider. We align fully with the transformation goals, offering a solution that is not only secure but also socially and economically empowering.



A MODERN MICROSOFT CLOUD SOC

01

SIEM & SOAR : FUNCTION
Microsoft Sentinel : MICROSOFT TOOL
CLIENT-SPECIFIC APPLICATION :

Centralized log ingestion from all servers and apps.
AI-driven correlation and automated playbooks for incidents like ransomware containment or suspicious case file access.

02

Extended Detection & Response (XDR) : FUNCTION
Microsoft Defender XDR (Endpoint, Identity, Office 365, Cloud Apps) : MICROSOFT TOOL
CLIENT SPECIFIC APPLICATION:

Unified protection for endpoints in courts, identity/access management (preventing credential theft), and email security (blocking phishing targeting judicial staff).

03

Identity & Access : FUNCTION
Microsoft Entra ID P2 : MICROSOFT TOOL
CLIENT-SPECIFIC APPLICATION :

Enforces Zero-Trust principles with Multi-Factor Authentication (MFA) and conditional access, crucial for protecting privileged accounts.

04

Data Compliance & Protection : FUNCTION
Microsoft Purview : MICROSOFT TOOL
CLIENT-SPECIFIC APPLICATION :

POPIA/GDPR compliance: Discovers, classifies, and protects sensitive data across the estate. Manages Data Loss Prevention (DLP) policies.

Cloud Security Posture

Microsoft Defender for Cloud

Hardens the configuration of cloud workloads and provides vulnerability management.

05

Data Cloud Security Posture : FUNCTION
Microsoft Defender for Cloud : MICROSOFT TOOL
CLIENT-SPECIFIC APPLICATION :

Hardens the configuration of cloud workloads and provides vulnerability management.



CORE MICROSOFT SECURITY STACK

01 Microsoft Sentinel

Cloud-native SIEM correlating logs from 450+ servers and 120+ applications across all 696 courts

02 Defender XDR

Extended Detection & Response protecting endpoint, emails and cloud workload nationwide

03 Entre ID P2

Identity governance with MFA, Zero trust and privileged access management

04 Microsoft Purview

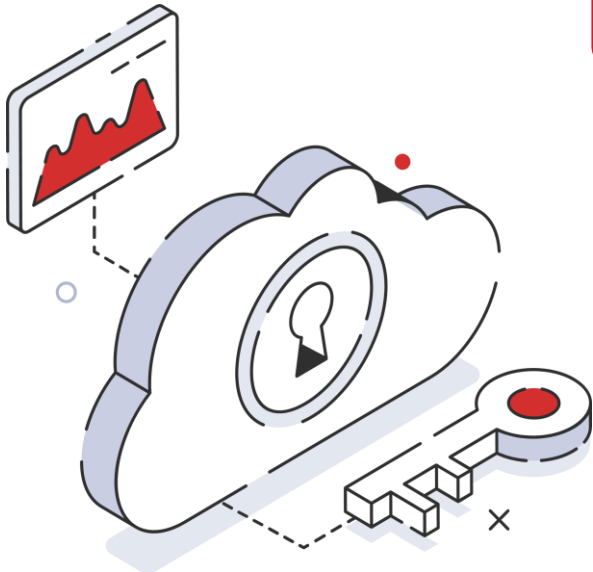
Data governance, classification, and POPIA compliance for sensitive judicial records

05 Sentinel Playbooks

Automated incident response for phishing, Ransomware, and insider threats

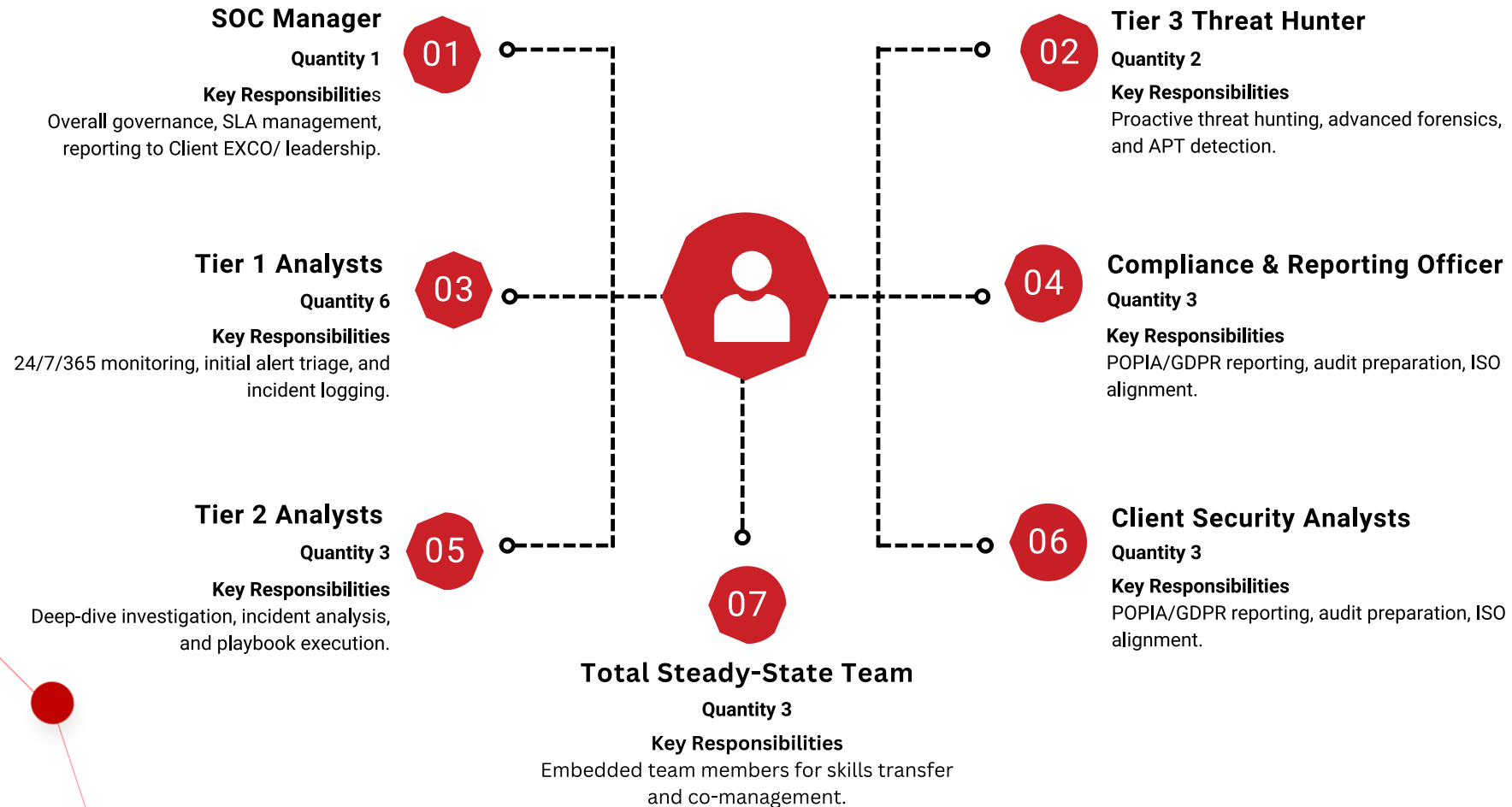
06 Defender for Cloud

Continuous security monitoring of cloud resources and workloads



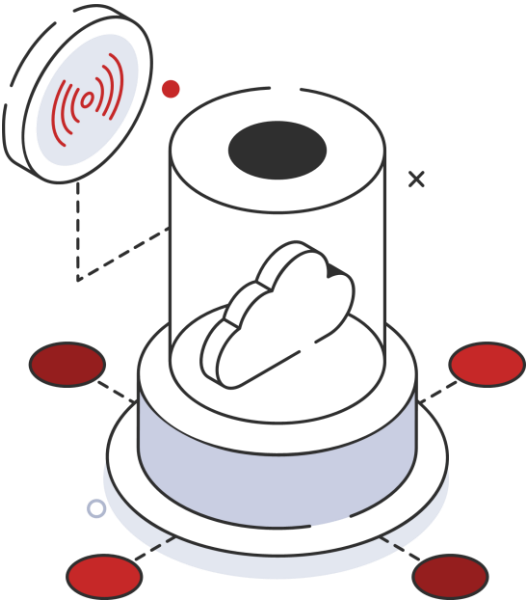
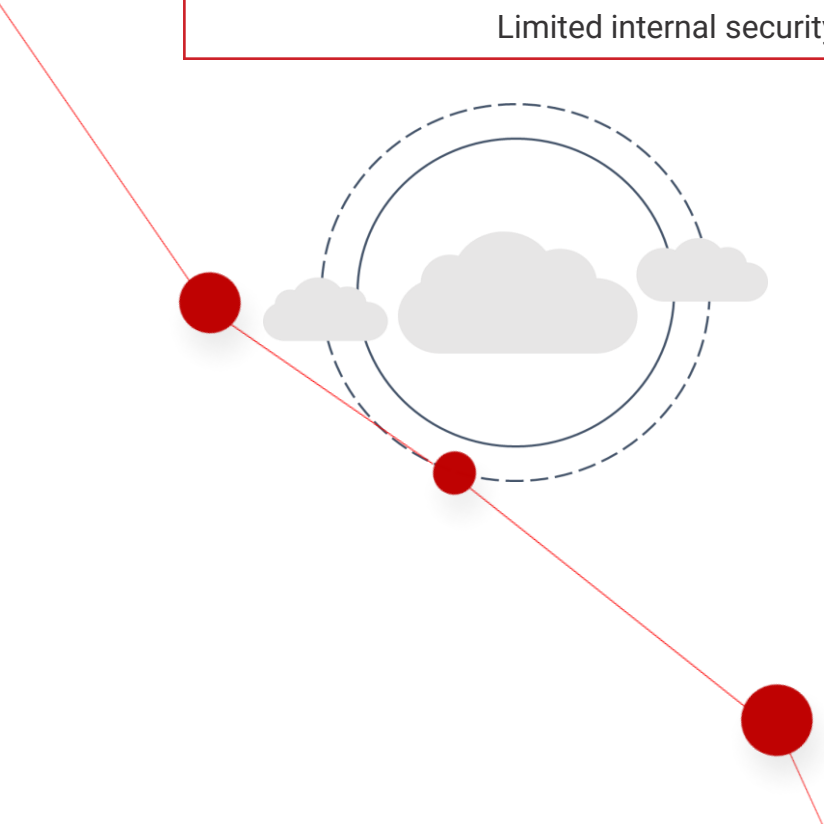
SOC SERVICE DELIVERY & STAFFING MODEL

We propose a Hybrid Co-Managed SOC model, blending Providence experts with Client staff to ensure long-term sustainability and skills transfer.



CHALLENGES VS PROVIDENCE SOLUTIONS

Client Challenge	Our Solution
Fragmented visibility across courts	Microsoft Sentinel centralized SIEM
Manual detection & slow remediation	AI + Automation via Defender XDR
Compliance risks (POPIA, GDPR)	Purview governance & DLP enforcement
Limited internal security expertise	Co-managed SOC with skills transfer



Metrics Block:

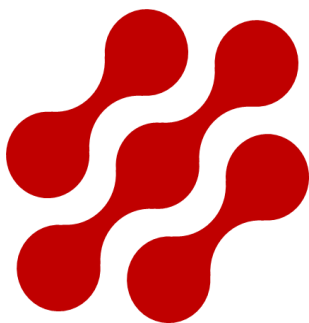
- First Expert Verdict: ≤15 mins
- Remediation Time: ≤2 hrs
- Uptime: 99.99%
- Frameworks: ISO 27001:2022 | NIST CSF |

OPERATIONAL EXCELLENCE & SLA COMMITMENTS

Purpose: Define measurable, outcome-based service levels.

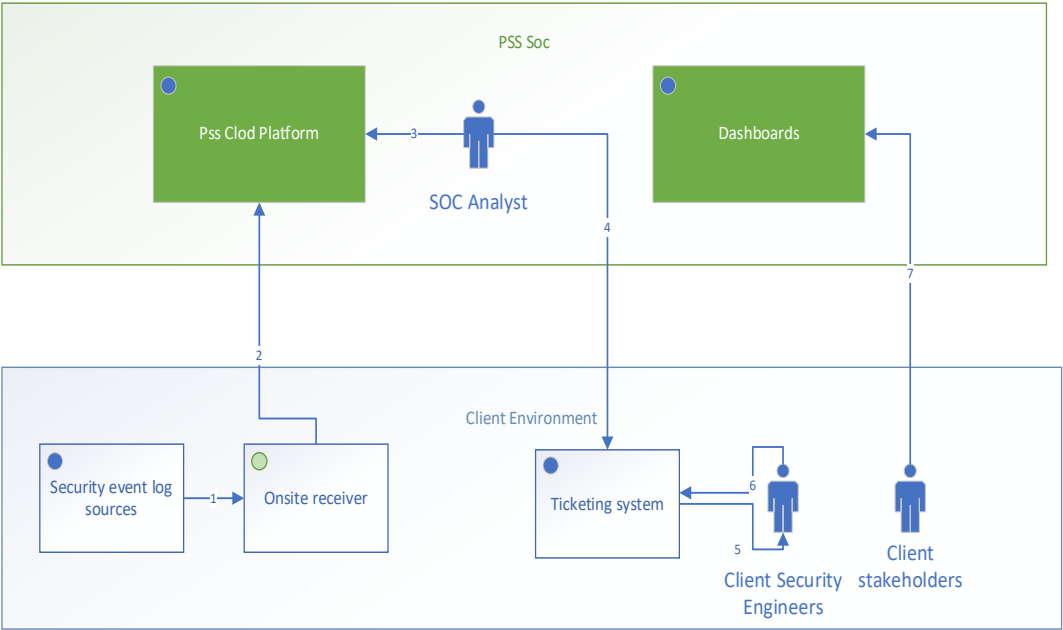
Visual: Dynamic table with icons per metric.

Service Metric	SLA Target	Platform	Responsibility
Incident Detection	≤5 minutes	Sentinel	Providence SOC
First Expert Verdict (FEV)	≤15 minutes	Sentinel/XDR	Providence SOC
Critical Incident Remediation	≤2 hours	Defender SOAR	Providence SOC
Report Delivery	Monthly	Power BI	Providence SOC
Governance Review	Quarterly	Workshop	Client + Providence



“SOC performance governed by ISO 27001:2022 and NIST CSF with 24x7 coverage.”

SOLUTION ARCHITECTURE



State

Existing

New

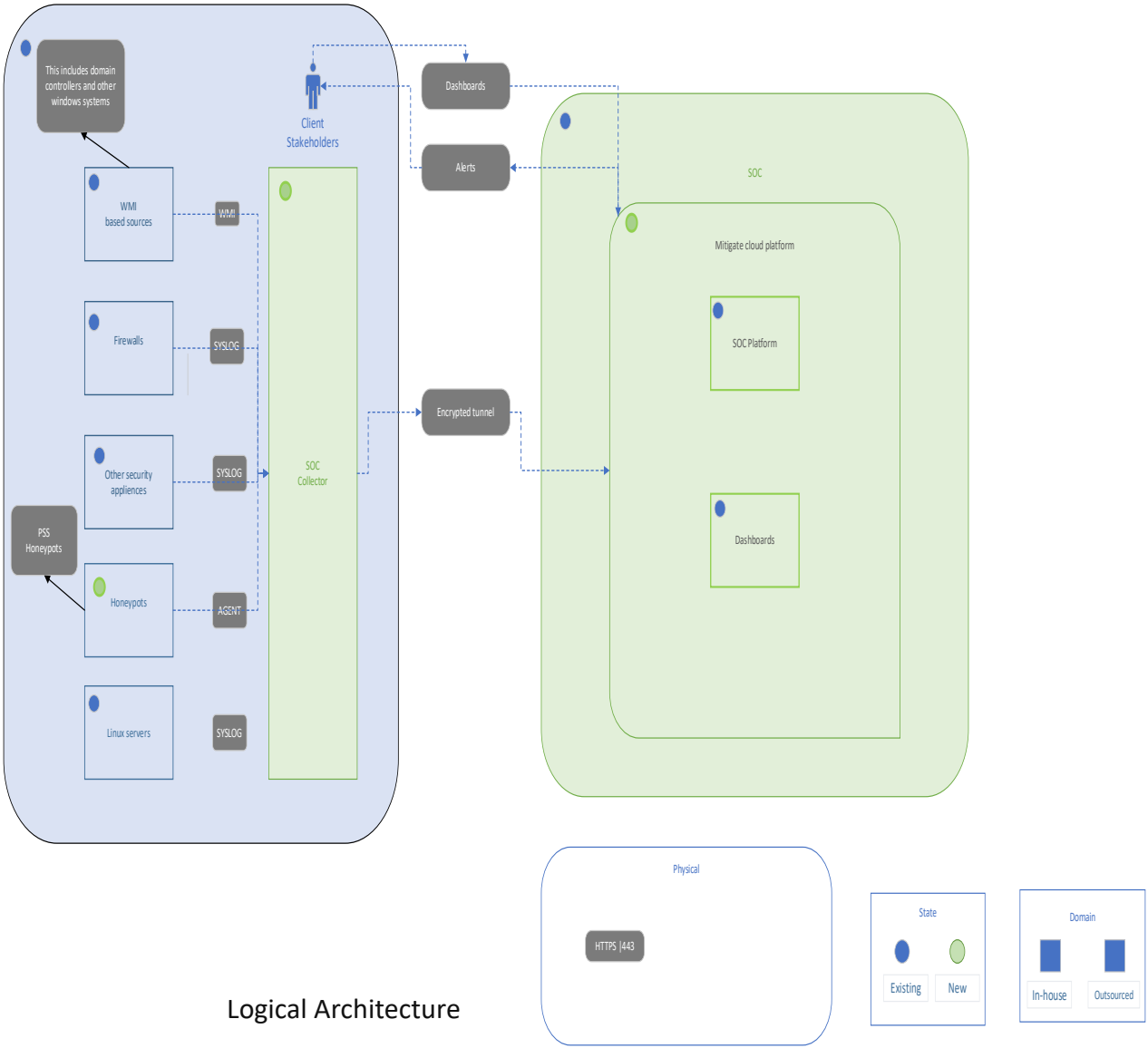
Domain

In-house

Outsourced

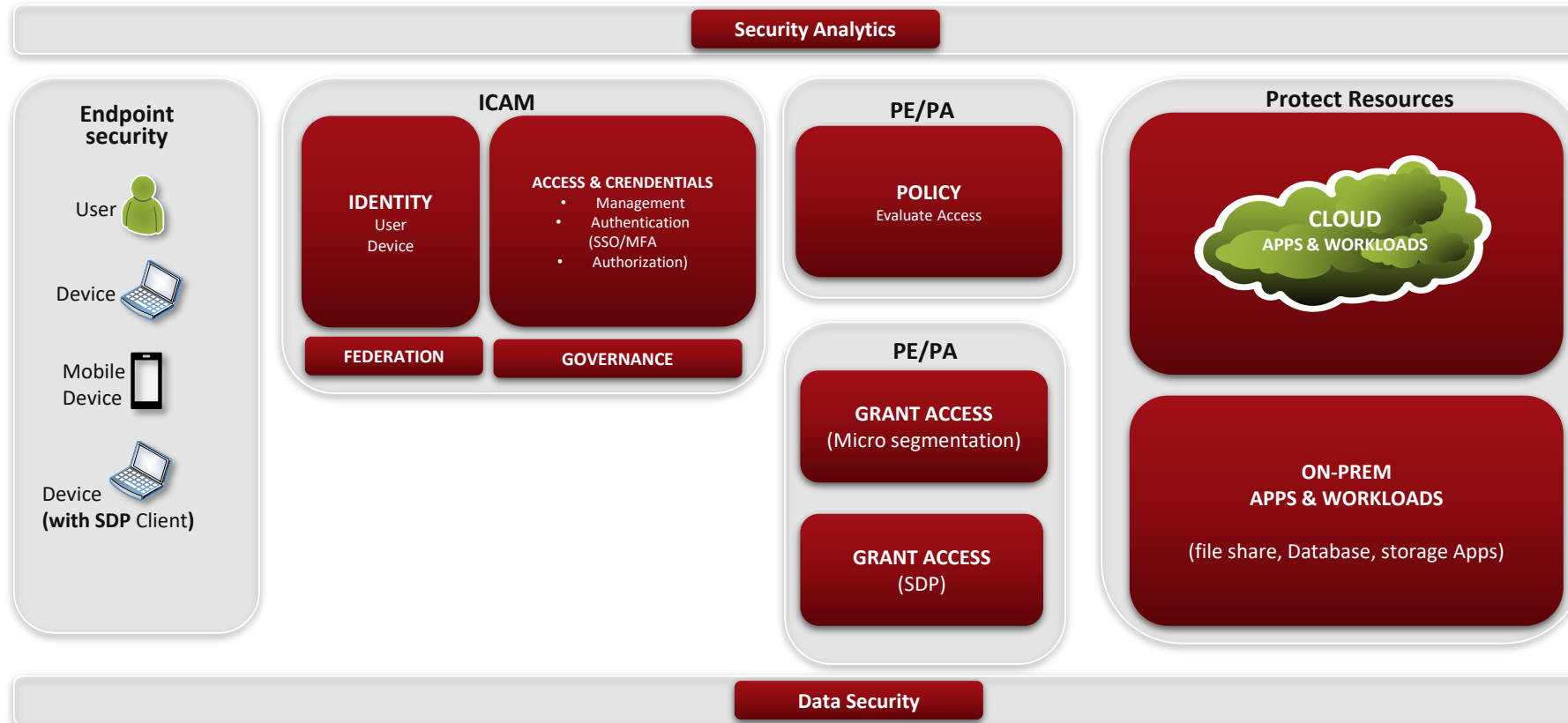
- Even logs are sent to the On-site receivers
- Events are forwarded to the cloud platform
- Analysts analyze log, detect incidents
- Tickets are logged for detected incidents and sent to the client
- Tickets are assigned to client security engineers for remediation
- Feedback sent to the SOC to confirm successful remediation
- Client stakeholders dashboards to quickly access security posture.

Conceptual Architecture: High-level depiction of telemetry ingestion, enrichment, correlation, and SOC workflows.



Logical Architecture

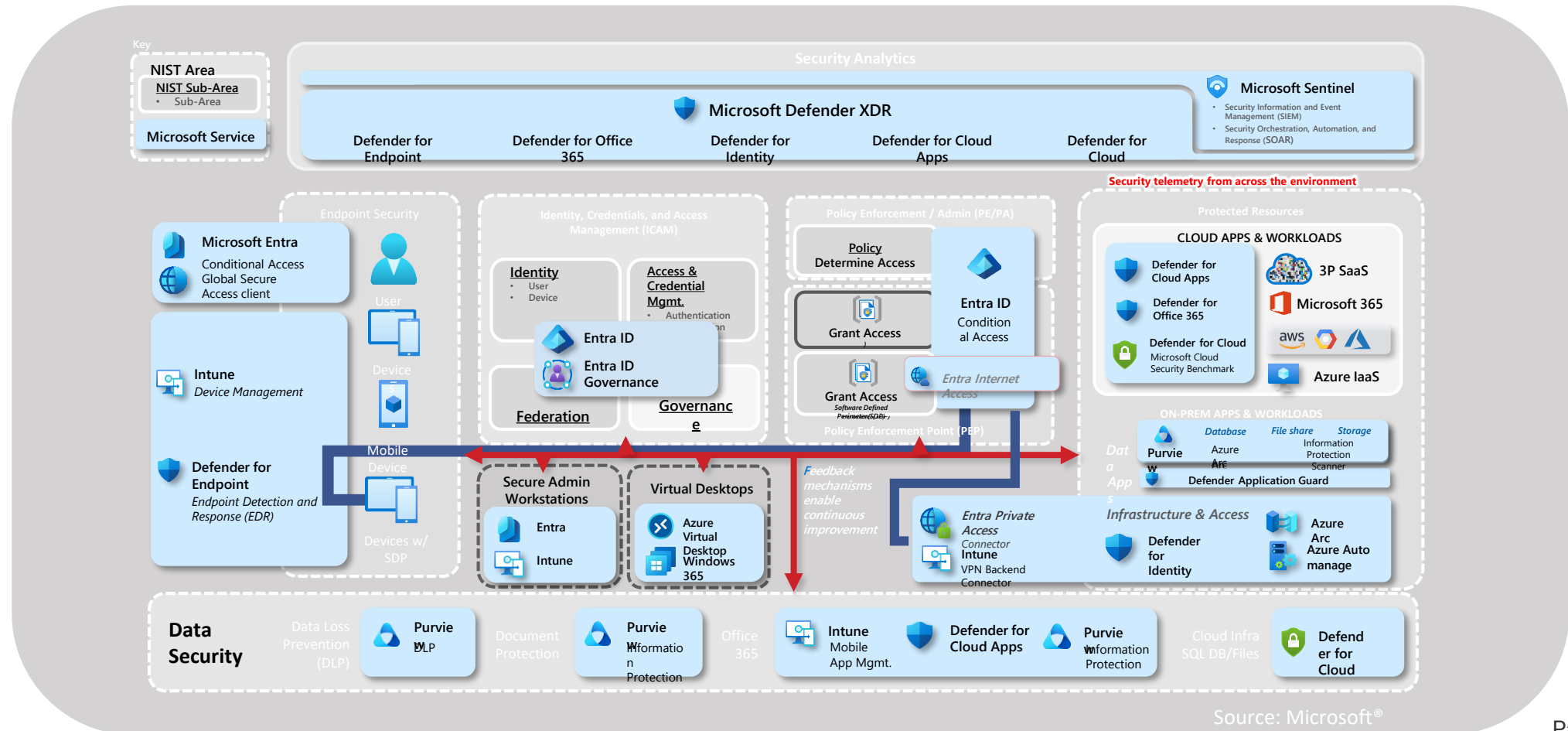
ZERO TRUST ARCHITECTURE (ZTA)



Source: Microsoft®

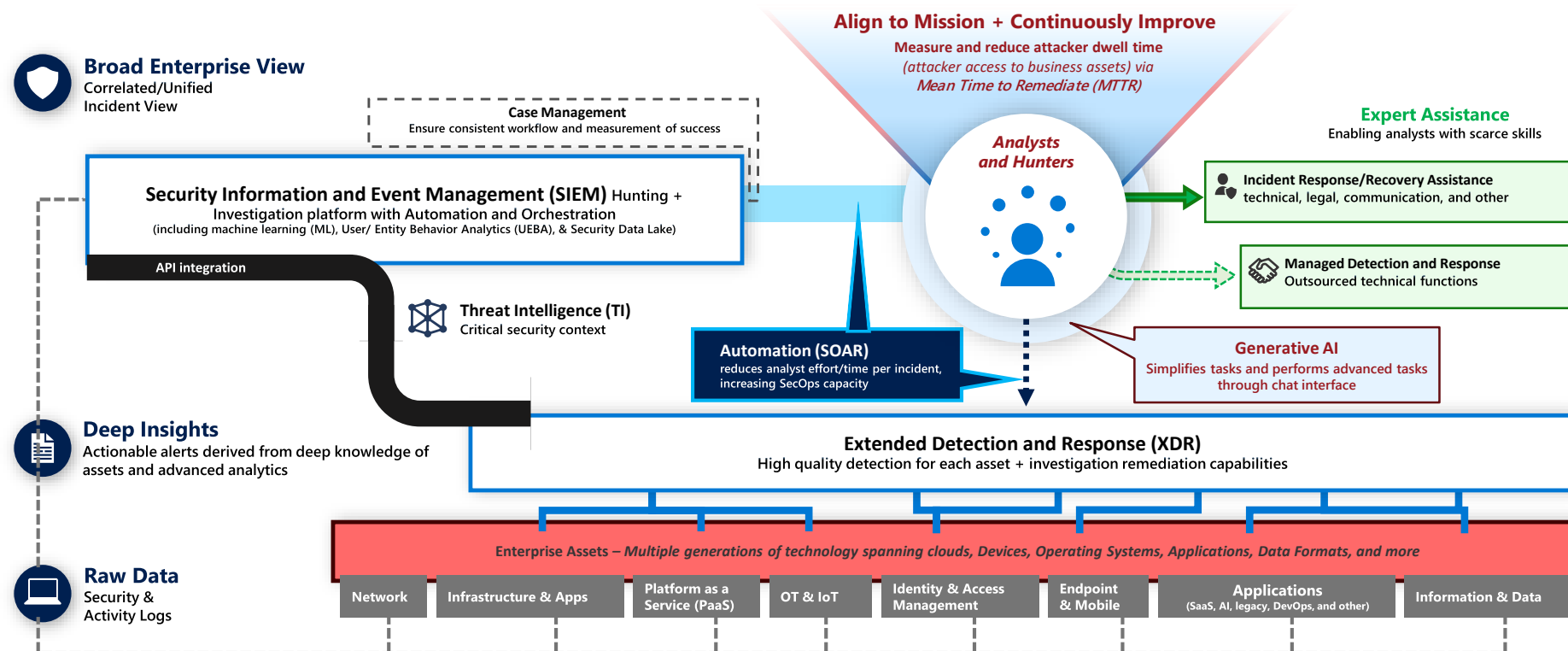
Microsoft Security Operations Centre — — —

MICROSOFT ZERO TRUST CAPABILITY MAPPING



Microsoft Security Operations Centre — — —

SECURITY OPERATIONS CAPABILITIES



Source: Microsoft®

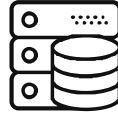
MICROSOFT CLOUD SOC ARCHITECTURE



Detection Layer

Microsoft Sentinel SIEM

- Threat intelligence
- Custom Analytics
- MITRE ATTACK Framework



Protection Layer

Defender for Endpoint

- Defender for identity
- Defender for Office
- Defender for cloud



Identity & Access

Entra ID P2

- Multi-Factor Auth
- Zero Trust Architecture
- Privileged Access Mgmt



Compliance Layer

Microsoft Purview

- Popia Compliance
- Data Classification
- Legal Evidence Chain

DETAILED TECHNICAL ARCHITECTURE

This diagram illustrates the end-to-end flow of security data, from the head office, regional offices and DC Servers through the Microsoft security stack, culminating in detection and response within the SOC.

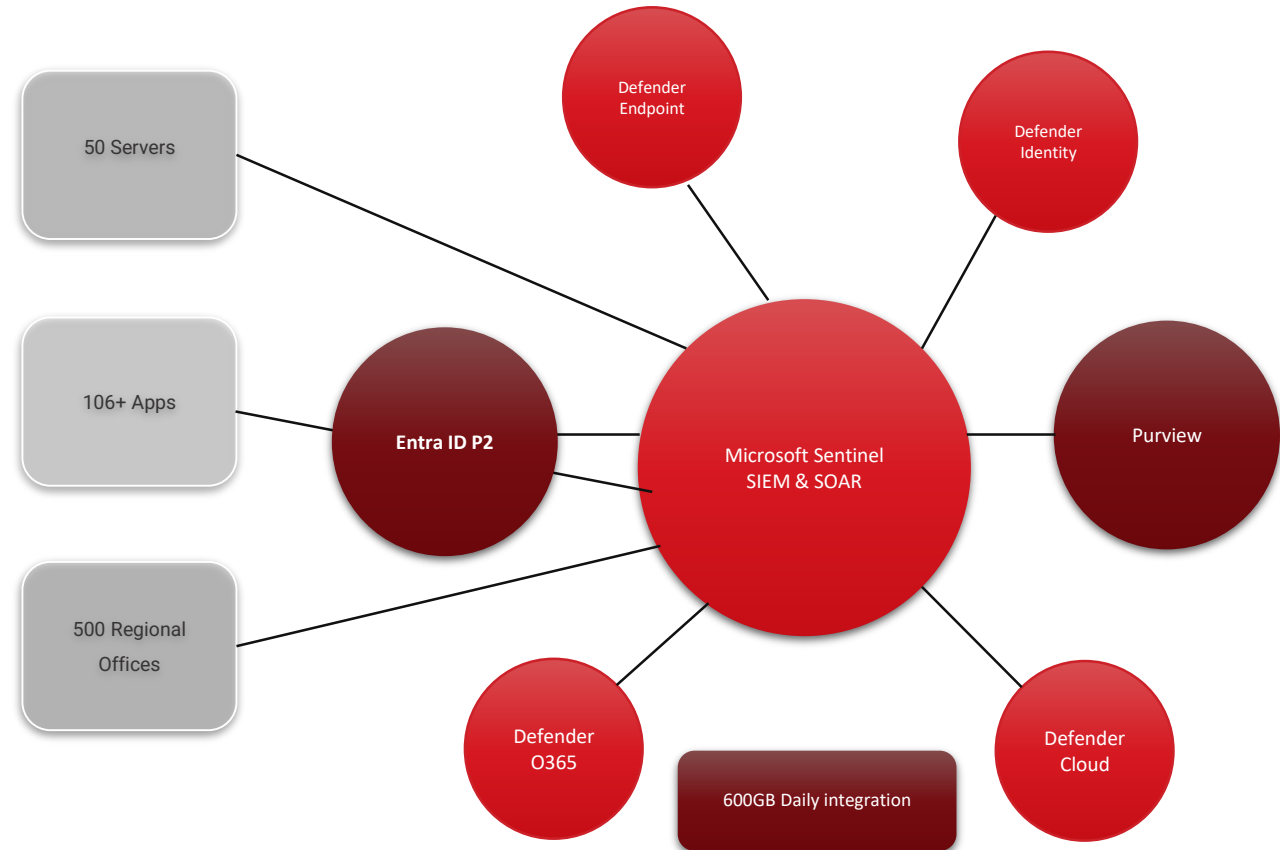
Key Integration Points:

Sentinel SIEM: Central correlation engine processing 600GB daily from all sources

Defender XDR: Unified threat protection across endpoints, identity, email, and cloud

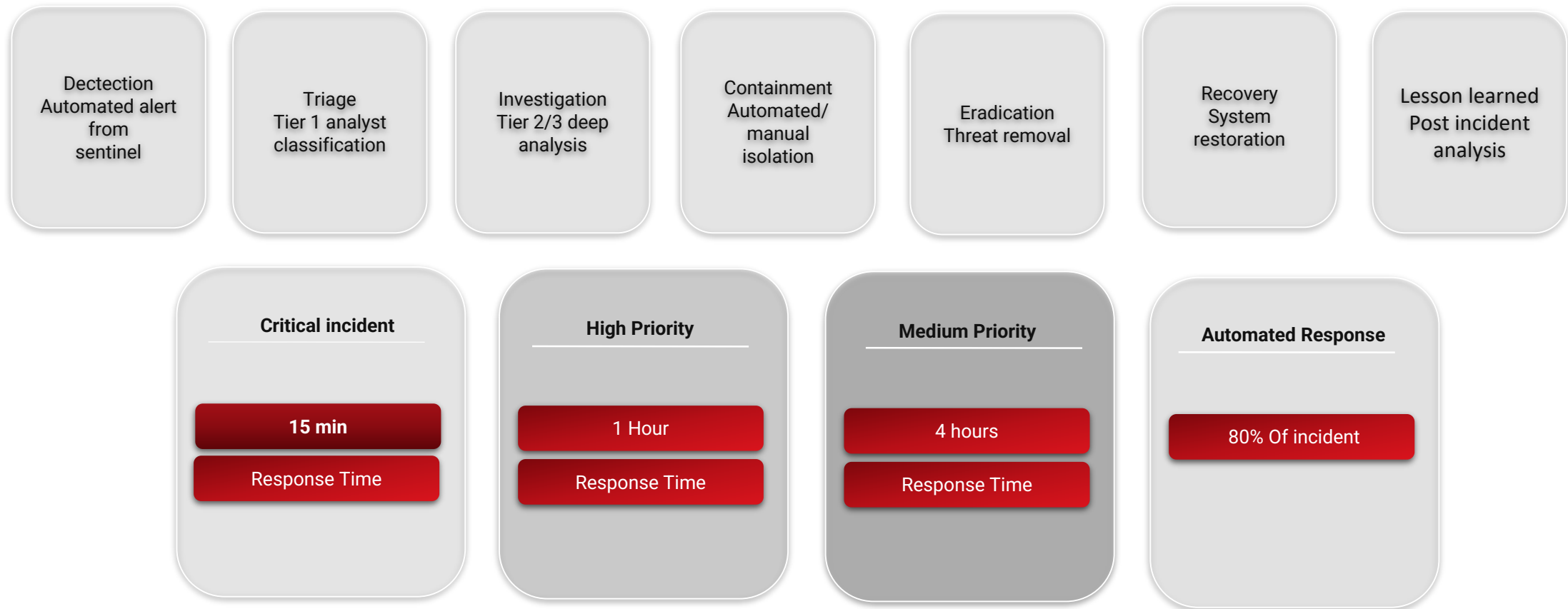
Entra ID P2: Identity governance with MFA and Zero Trust architecture

Purview: Data governance and compliance automation for POPIA/ GDPR requirements



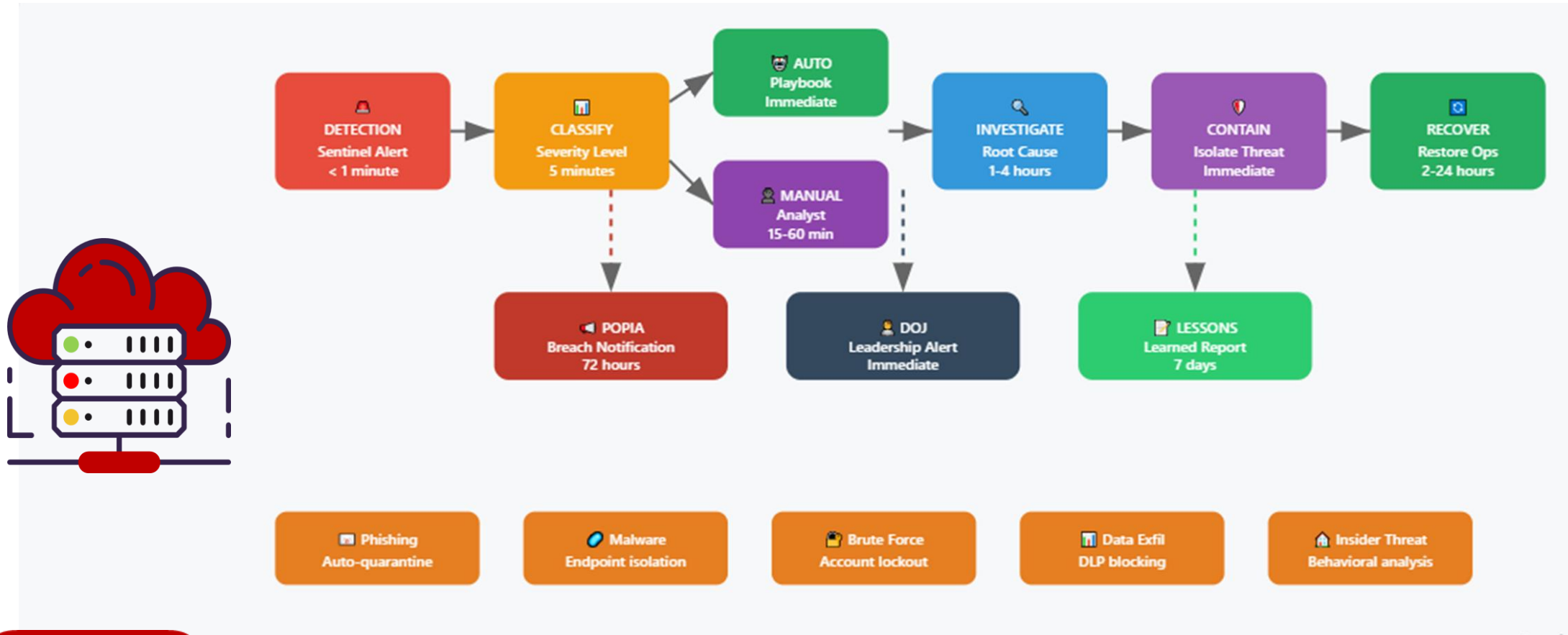
INCIDENT RESPONSE PROCESS & SLAS

Threat Detection & Response flow



Our operational process is designed for speed and efficiency, ensuring minimal impact from security incidents.

INCIDENT RESPONSE PLAYBOOK FLOW



ENTERPRISE RISK MANAGEMENT DASHBOARD

Data sources



SoC PoPIA OHS

...

Data ETL

<< Resolution rules >>

Feature Extraction

Data Enhancement

Data Modeling

Ai Agentic Predictive Models

Risk Threshold & Alerts

Mitigation Strategies

Action Plans

Notification & Workflow

Baseline data-model establishment

Visualization

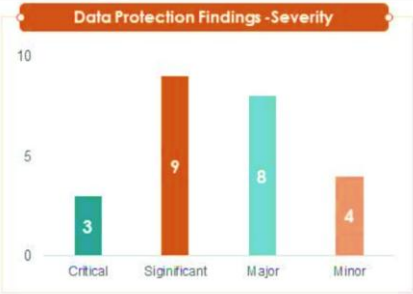


Visualized display of multi-dimensional data



Enterprise Health situational Awareness

ENTERPRISE RISK MANAGEMENT DASHBOARD



Non Conformance’s Resolution Tracking

External Audit

Internal Audit

PoPI /GDPR

ISO 45001: OHS

ISO 27001:ISMS

ISO 22301: BCM

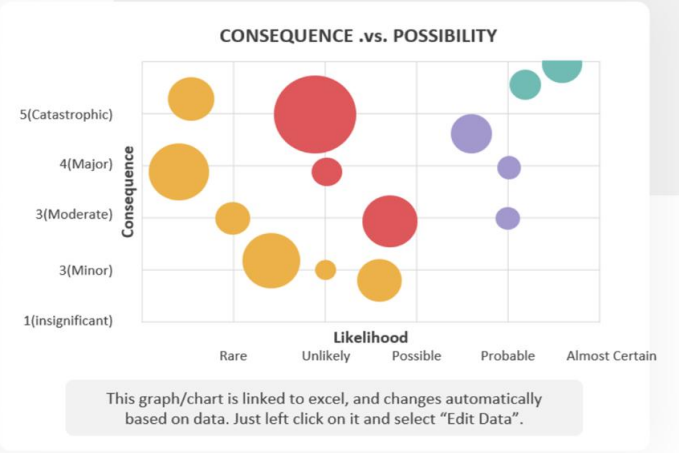
Real-time risk monitoring and alerts

Customizable reporting for audits.

Automated regulatory compliance updates

Proactive incident tracking and resolution.

RISK DASHBOARD



Regulatory and Compliance Risk Assessment Dashboard



SECURITY RISK MONITORING OF THE CUSTOMER'S INTERNAL USERS IN THE ENTERPRISE ENVIRONMENT



THREATS

35

ANOMALIES

744

USERS

202

Anomalous

DEVICES

197

Anomalous

APPS

14

Anomalous

Threat Review

User Review

Analytics Dashboard

148

All Known

69.8K

All Internal

43

All Apps

9.9K

All Unknown

115

All External

Latest Threats

Insider: Suspicious Behavior

Aug 2, 2016

5

Insider: Lateral Movement

Aug 2, 2016

5

External: Malware Activity

Aug 1, 2016

4

Insider: Lateral Movement

Aug 1, 2016

4

External: Data Exfiltration by Malware

Aug 1, 2016

5

External: Data Exfiltration by Malware

Aug 1, 2016

5

Showing top 20 of 35 threats

View Details

Threats by Threat Type

35

THREATS

External: Malware Activity

14

40%

Insider: Suspicious Behavior

4

11%

Insider: Lateral Movement

4

11%

Insider: Data Exfiltration by Suspicious User or Device

3

9%

External: Remote Account Takeover

2

6%

Showing all 12 threat types

View Details

Enterprise cyber risk management dashboard

This slide represents the key metrics dashboard representing details related to management of cyber security incidents by an enterprise. It includes key performance indicators such as risk analysis progress, risk rating breakdown etc.

% Risks >= threshold

38.6%

Of risks >= threshold

397

Average risks threshold 12.4

Risks analysis progress

88.8%

Response progress for risks >= threshold

52.6%

#Risks >= threshold: top 5 vulnerabilities

Encryption vulnerabilities

26

Excessive user permissions

68

Dormant accounts

34

Add text here

45

Add text here

29

Risks >= threshold: top 5 entities

General hospital

55

Internal medicine east

20

Asheville Vascular Care

19

Add text here

17

Add text here

17

Risk rating breakdown

Medium risk

33%

High risk

14%

Low risk

48%

Risk heart map

Total # of risk rating

Severe

20

51

44

4

4

Major

50

44

51

52

4

Moderate

40

105

140

162

107

Minor

150

208

102

91

82

Insignificance

200

405

105

105

22

Rare

Unlikely

Moderate

Likely

Almost certain

Action plan breakdown

Deferred

10.4%

Implemented

30.9%

Planned

8.5%

TBD

50.2%

This graph/chart is linked to excel, and changes automatically based on data. Just left click on it and select "Edit Data".

All Anomalies

Hide from Dashboard

Domain

Microsoft.com

Average Risk Score

30

Peak Risk Score

31

Current Risk Score

42

▲ 13 Increased in Domain Risk Score

View Notes

Cards Based Peak Risk Score

Insider Threat

Last Update: 03/12/2018 08:30 PM

91

Data Ex-Filtration

Last Update: 03/12/2018 08:30 PM

12

Data Ex-Filtration

Last Update: 03/12/2018 08:30 PM

65

A

Aubrey Sithole

All Anomalies

Hide from Dashboard

23 Sep 2025 11:00 00 AM

LottoStar

https://lottostar.co.za

Average Risk Score

30

Peak Risk Score

31

Current Risk Score

31

Card Based Peak Risk Score

Insider Threats

21

Data Exfiltration

16

Compromised Accounts

0

Logon Anomalies

34

Page | 27

SENSITIVE DATA DISCOVERY & SECURITY ENFORCEMENT

1

Universally compatible

Seamlessly connect and discover all your data systems with powerful integrations and new tools, all without data exfiltration.

2

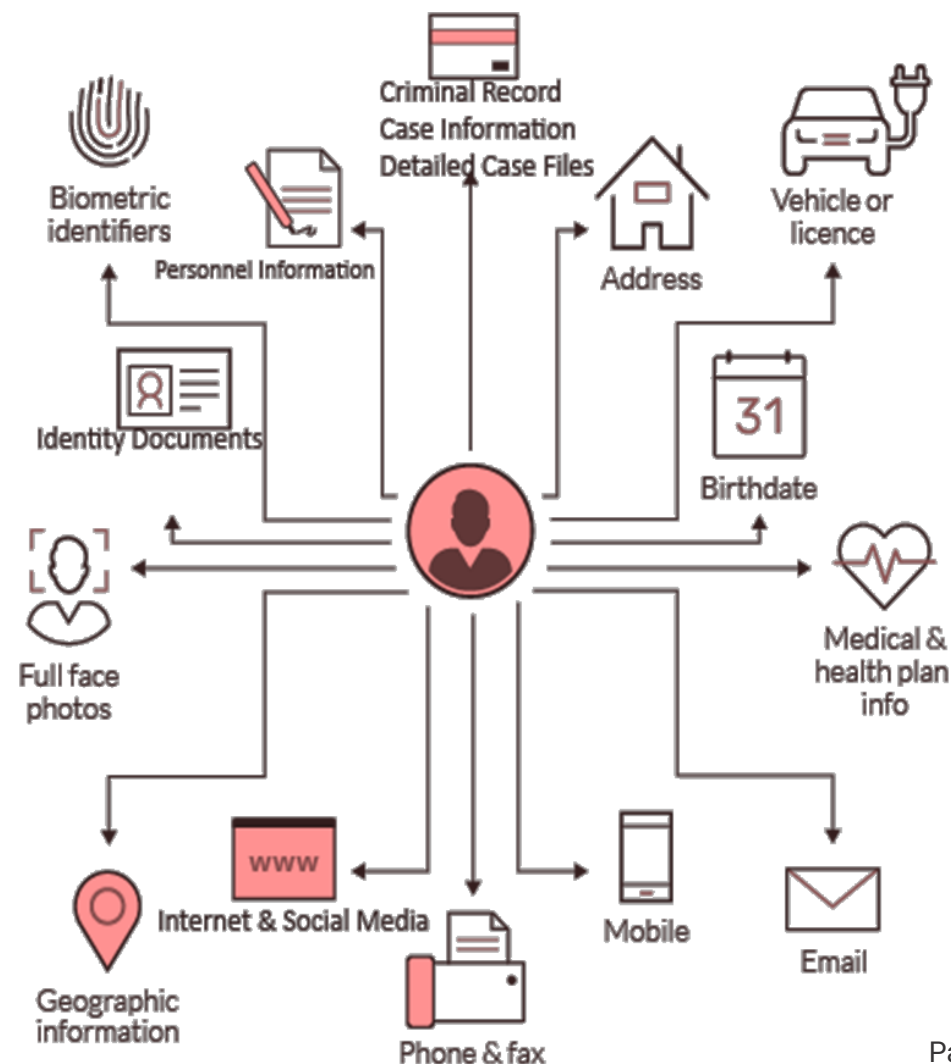
Complete data context

Centralize your understanding of what data exists, when the data is collected, where the data is stored, and how the data is used with live data discovery maps.

3

Powered by machine learning

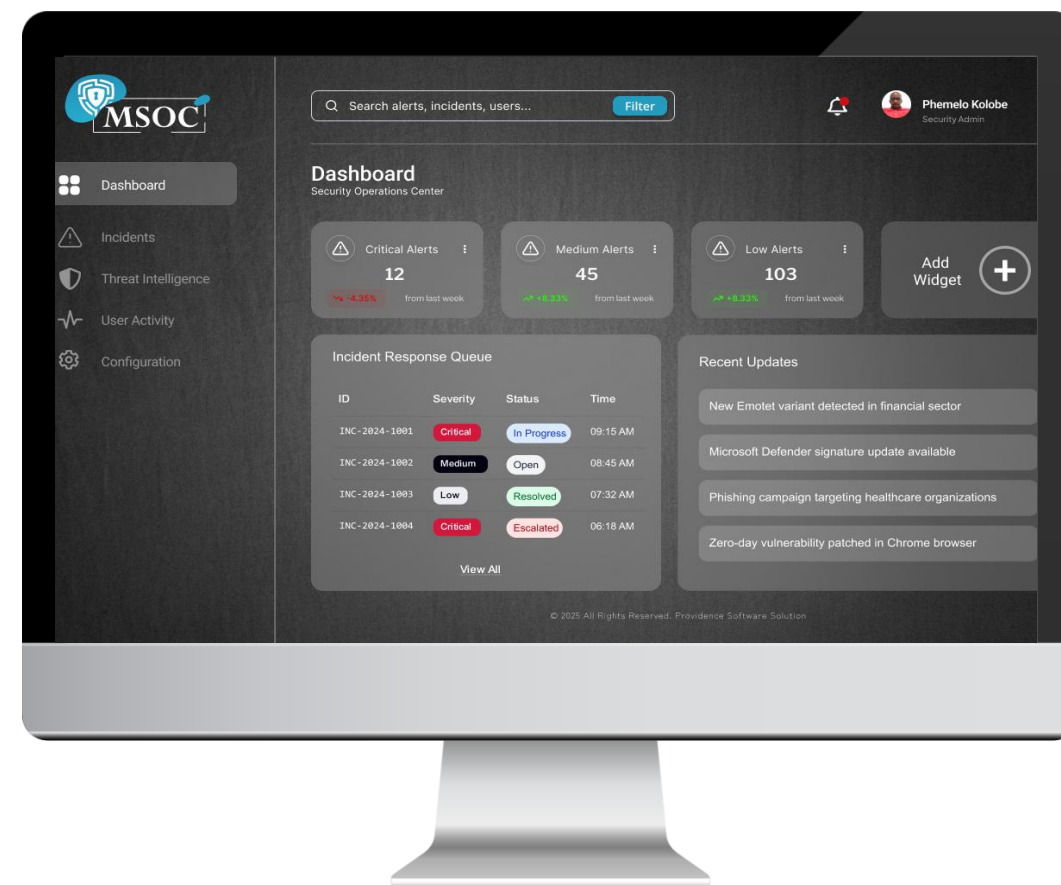
Leverage advanced machine learning and AI to give meaning to your data; identify business context, sensitivity score, privacy risk, and more.



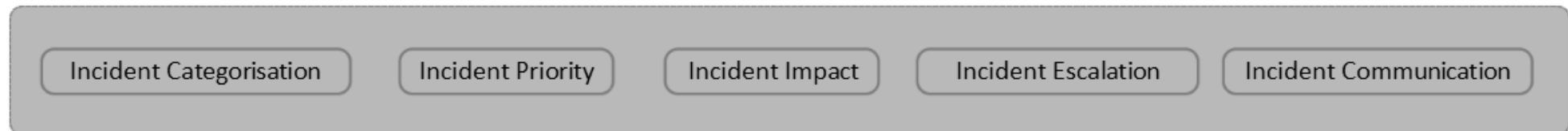
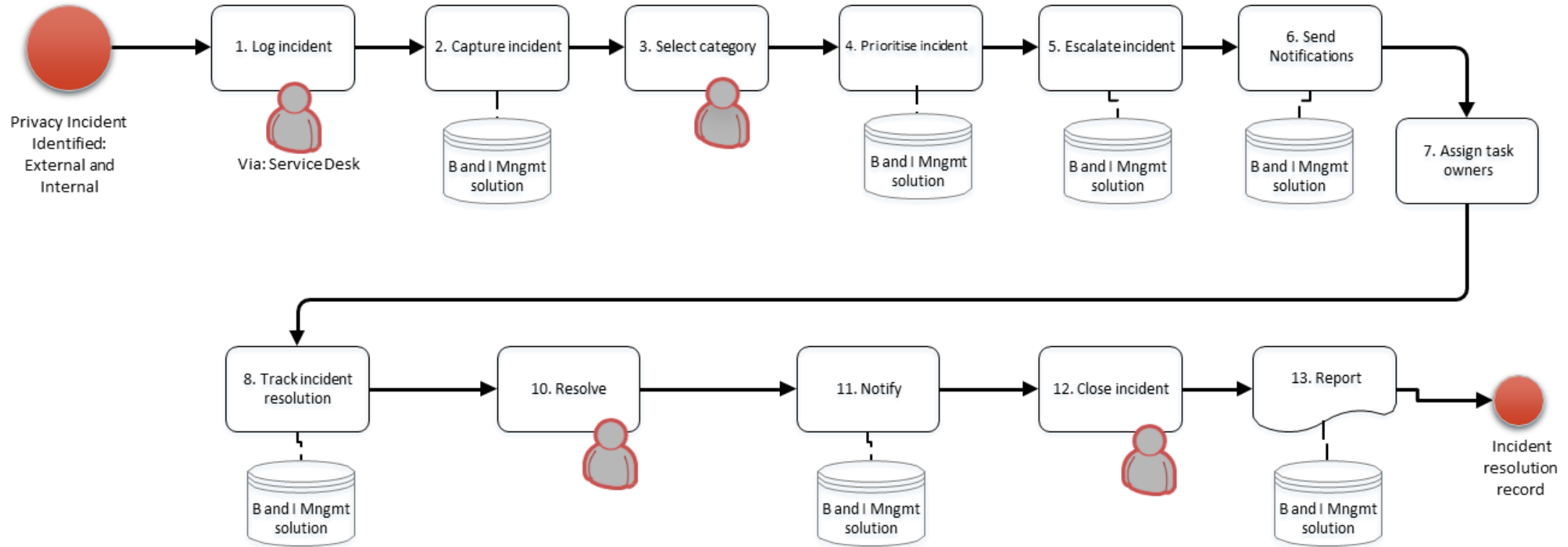
SENSITIVE DATA DISCOVERY & SECURITY ENFORCEMENT

Providence's Data Discovery, Classification and security enforcement tool will assist Customers to obtain complete visibility into your sensitive data with efficient data discovery, classification, and risk analysis across heterogeneous data stores, the cloud, big data, and traditional environments.

Our solution is simple to deploy and to use, it will provide Customers with a single pane of glass that allows you to get a clear understanding of what sensitive data you have, where it is located, and its risks of exposure. With rich visualizations and detailed reports, you can more easily uncover and close your gaps, make better decisions about third-party data sharing and cloud migration, and proactively respond to data privacy and security regulations including GDPR/PoPIA, CCPA, LGPD, PCI DSS and ISO 27001.



SENSITIVE DATA DISCOVERY & SECURITY ENFORCEMENT



IMPLEMENTATION TIMELINE



Project Timeline - 21 Weeks

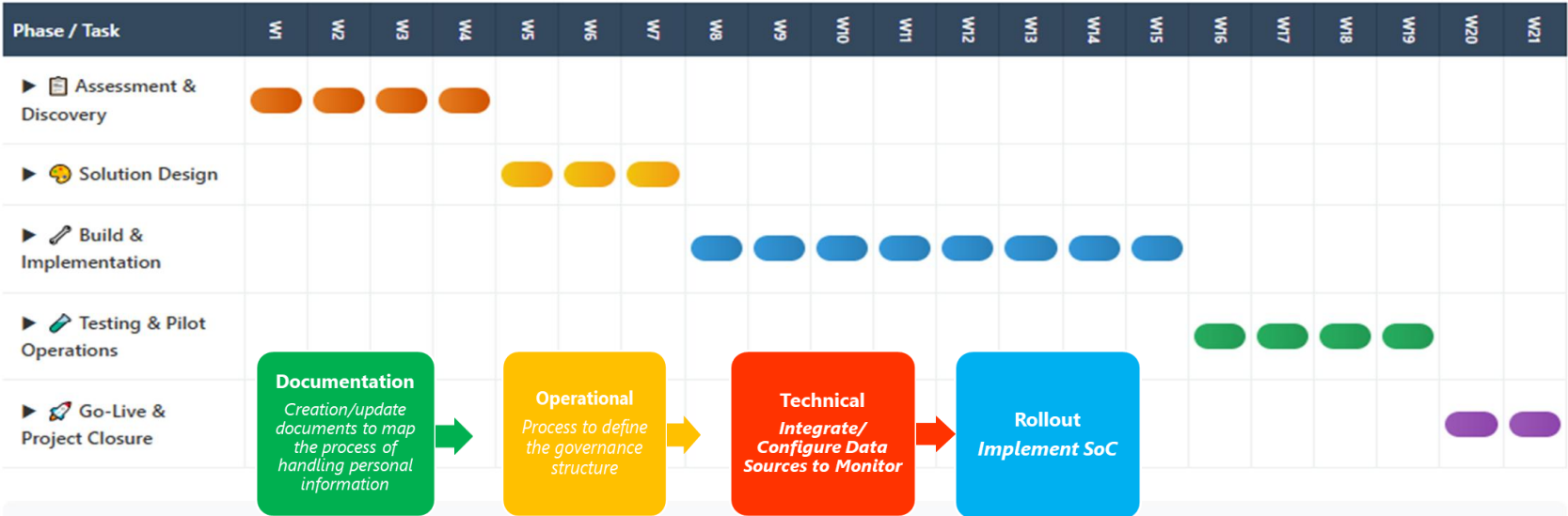
Normal Speed

▶ Play

⏸ Pause

⏮ Reset

Current Progress: Week 0.0 of 21



Phase Details:

█ Assessment: 4 weeks

█ Design: 3 weeks

█ Implementation: 8 weeks

█ Testing: 4 weeks

█ Go-Live: 2 weeks

POLICY AND BUSINESS PROCESSES

ISO 27001 Certification



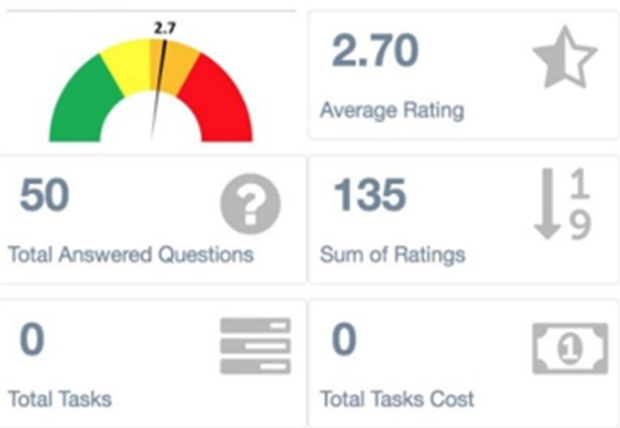
- Integrated Management System Kit
 - documents
 - Implementation Standards
 - Section 1 - Premises and Housekeeping
 - Section 2 - Mechanical, Electrical and P
 - Section 3 - Management of Fire and Ot
 - Section 4 - SHE Incident Recording and
 - Section 5 - Organisational Management
 - Supporting Documentation
 - Appointment Letters
 - Informational and Guideline Document
 - NOSA Standards & Documents
 - OHS Act Annexures & other Legal Docu
 - Policies, Standards and Work Procedure
 - Registers, Checklists and Other Control
 - Risk Assessment
 - Survey Instruments
- Element 5.02(IND) SHE Risk and Impact Assess...
 - Element 5.03(IND) Legal Requirements and-or ...
 - Element 5.04(IND) SHE Corporate Standards!.d...
 - Element 5.05(IND) SHE Objectives and Targets!...
 - Element 5.06(IND) SHE Plan!.docx
 - Element 5.07(IND) SHE System Review!.docx
 - Element 5.10(IND) Responsibility of Chief Exec...
 - Element 5.11(IND) SHE Appointments!.docx
 - Element 5.12(IND) SHE Representatives!.docx
 - Element 5.13(IND) SHE Committees!.docx
 - Element 5.14(IND) SHE Communication!.docx
 - Element 5.15(IND) First Aider and Occupationa...
 - Element 5.16(IND) First Aid Training!.docx
 - Element 5.21(IND) SHE Awareness and Promot...
 - Element 5.22(IND) SHE Performance Display B...
 - Element 5.23(IND) SHE Suggestion Scheme!.d...
 - Element 5.24(IND) SHE Reference Resources!.d...
 - Element 5.25(IND) SHE Annual Report!.docx
 - Element 5.30(IND) SHE Training!.docx
 - Element 5.32(IND) Medical Services!.docx



ISO 27001 Implementation and execution automation

SS_9001_Internal_Audit_201804

Initial internal audit post successful readiness assessment conducting in January 2018
19-Mar-18 21:25



ISO27001



OUR DIFFERENTIATORS: WHY PROVIDENCE



Public Sector Expertise

Our proven experience, we understand government processes and compliance demands.



Certified Security & Quality

Our ISO/IEC 27001 (Security) and ISO 9001 (Quality) certifications provide a certified framework for reliable and secure service delivery.



Strategic Microsoft Partnership

As a Microsoft Gold Partner, we have direct access to technical expertise and best practices, ensuring a best-in-class implementation.



Commitment to Transformation

Our 100% BEE Level 1 status contributes significantly to the Client's own transformation goals, and we include a robust skills development program.



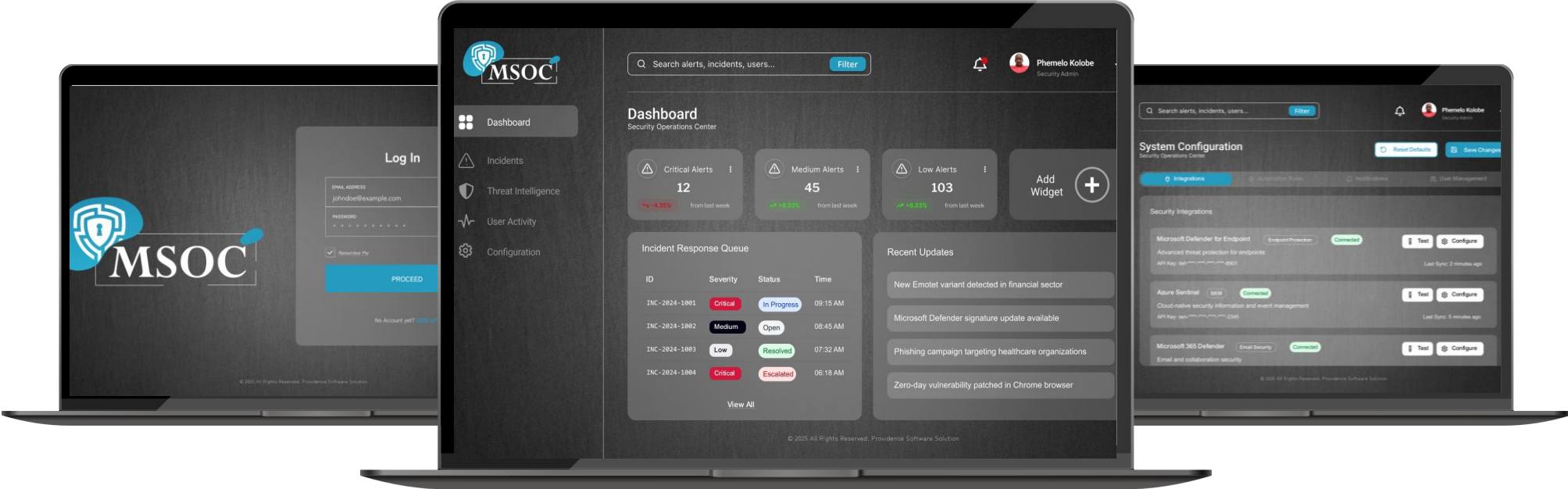
CONCLUSION

As a cybersecurity partner that understands the criticality of your mission. Providence Software offers a partnership built on trust, security excellence, compliance rigor, and a shared commitment to your Cybersecurity Roadmap.

We are confident that our proposed Microsoft Technology SOC will significantly enhance your resilience against cyber threats, safeguard the integrity, and ensure the privacy.



MOCK UP SYSTEM SCREENS





THANK YOU

+27 (0) 87-711-5555

 www.providencesoft.com

 admin@providencesoft.com



Providence Software Solutions