Cyber Operations

Built for
Microsoft Azure

pwc | Microsoft

Threat Detection & Response (TDR) challenges

Despite increases in cybersecurity spending and awareness, organizations are struggling to keep pace with the ever-changing threat landscape. The average cost of a data breach is estimated to cost around $4.24m per breach*, an over 10% increase year over year. Furthermore, different stakeholders within an organization face different sets of security challenges:

CISO

- Rapid scalability & availability
- Lack of end-to-end threat visibility
- Suboptimal SIEM infrastructure
- Increasing SIEM costs due to expanding digital estate
- Lack of true cloud-based monitoring and detection capability
- Increasing threat surface with remote working model

SOC team

- Alert fatigue
- Data integrity issues
- Automated detection & routine tasks
- Custom APIs need to be built
- Lack of automated workflows
- High analyst turnover

IR team

- Missing contextual information
- Lack of security orchestration
- Lack of prioritization
- Lack of visibility of key stakeholders
- Lack of efficient ways to communicate/collaborate

Deployment & Integration Complexity

- Dealing with varied data sources
- Unscalable security architectures not keeping pace with expansion of digital estate
- Skills gap to support new cybersecurity technologies

Manage & Monitoring Challenges

- Focus on addressing alert fatigue
- Cybersecurity technologies lack business agility
- Inability to automate monitoring and response capabilities

* Source: Ponemon Institute - 2021 Cost of a Data Breach Report

An integrated TDR solution is key to overcoming challenges

TDR

Log management	Threat intelligence	Incident management
• Custom connector • UEBA/UBA • Interactive Dashboard	• Effective correlation rules • Critical asset identification • Threat modeling • Contextual data	• Automated Response • Risk-based prioritization • Custom reporting • SOAR

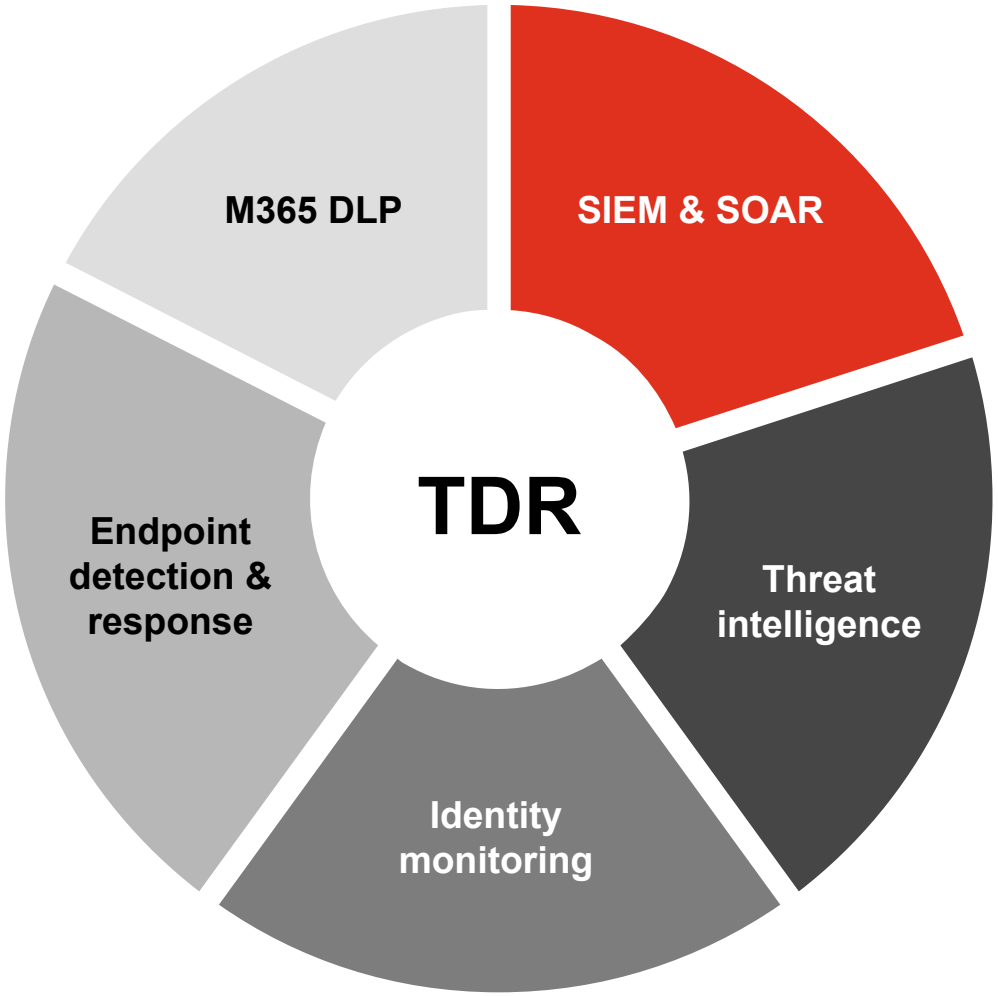
Align all aspects of your organization for improved synergy, speed, and savings

- Integrate multiple technologies
- Streamline threat detection and response capabilities
- Capture, analyze, and apply your data assets

Leverage enhanced automation and intelligence across your IT footprint

- unstructured data sources
- Better predict, manage, and react to security incidents
- Move quickly to turn data into actionable information
- Increase competitive advantage
- Tap into exponentially growing data

Building an integrated TDR solution



Microsoft technologies

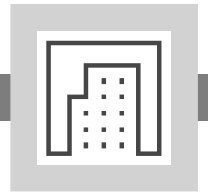
- Enable key cybersecurity operations capabilities via integrated Microsoft technologies
- Leverage cloud-native TDR to collect and correlate cloud and on-premises data
- Facilitate future growth and scaling in line with your business needs

PwC professional services

- Deploy and manage your TDR solution within 100 days
- Develop custom content (e.g., SIEM use cases, DLP policies, custom data source connectors, etc.)
- Established processes and automation via a hybrid on-site and remote team
- Continuous optimization and tuning

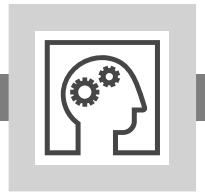
Introducing cloud-based TDR

- Smarter and faster TDR capabilities using Microsoft Azure Sentinel with artificial intelligence, machine learning and threat intelligence capabilities
- Ingest Microsoft-native and third-party data sources and alerts into Azure Sentinel to obtain visibility of both cloud and on-premises systems
- PwC's CyberOps team will tailor the solution to your organization's unique needs via customized connectors and use cases
- Leverage PwC's proven CyberOps team and processes to operate your TDR function via a hybrid on/off-site team that tightly is integrated with your existing cybersecurity resources



Flexible architecture

Collects data from hybrid enterprise (cloud and on-premises assets)

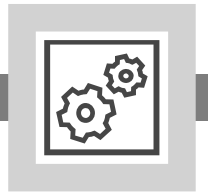


Analytical threat intelligence

Integration with Microsoft's Intelligent Security Graph for unique threat intelligence and analytics

Threat-driven monitoring

Custom PwC use cases based on the MITRE ATT&CK framework



Advanced & faster triaging

Using entity mapping and automated response workflows/playbooks

Solution overview

TDR

Microsoft TDR technologies

Detect and respond to threats via integrated technologies for improved visibility, speed, and response

Azure Sentinel	• SIEM • Threat Intelligence • SOAR	**TDR platform** • Cloud and on-premises threat monitoring • SIEM use case development • Workflows and automation • Threat intelligence
Azure ATP	• Identity Monitoring	• Prevent, detect, and investigate identity threats • Detect and respond to compromised users • Detect and respond to lateral movement
M365 DLP	• Data Loss Prevention (DLP)	• M365 security and compliance monitoring • M365 DLP
Defender ATP	• Endpoint Detection and Response (EDR)	• Cloud workloads and on-premises EDR • Investigations and threat hunting • Monitoring, reporting and response

Our approach – Accelerate deployment and operations support

Combine Microsoft's cybersecurity technologies with PwC's CyberOps managed service to design, build and operate your TDR solution within 100 days

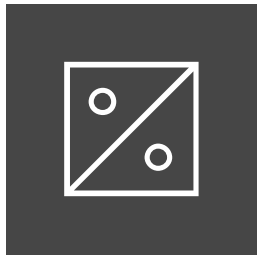
1
Analyze

2
Design

(4 weeks)

- Understand current capabilities (if any)
- Define business and technical requirements
- Identify log data sources and use cases
- Identify default and custom connectors
- Develop future-state capabilities roadmap

3
Deploy

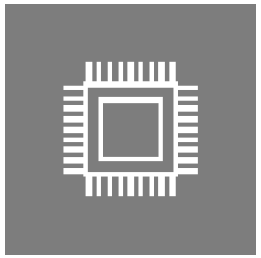


4
Integrate

5
Build

(10 weeks)

- Onboard Azure Sentinel and workspaces
- Develop custom connectors
- Onboard log and data sources
- Develop and configure use cases
- Develop SOPs and related documentation
- Start transition to PwC's CyberOps services team



6
Operate

(Ongoing)

- Begin 24x7x365 operations
- Identify and action opportunities for continuous improvement

Learn more

Contact us to learn more about how you can transform your cybersecurity operations

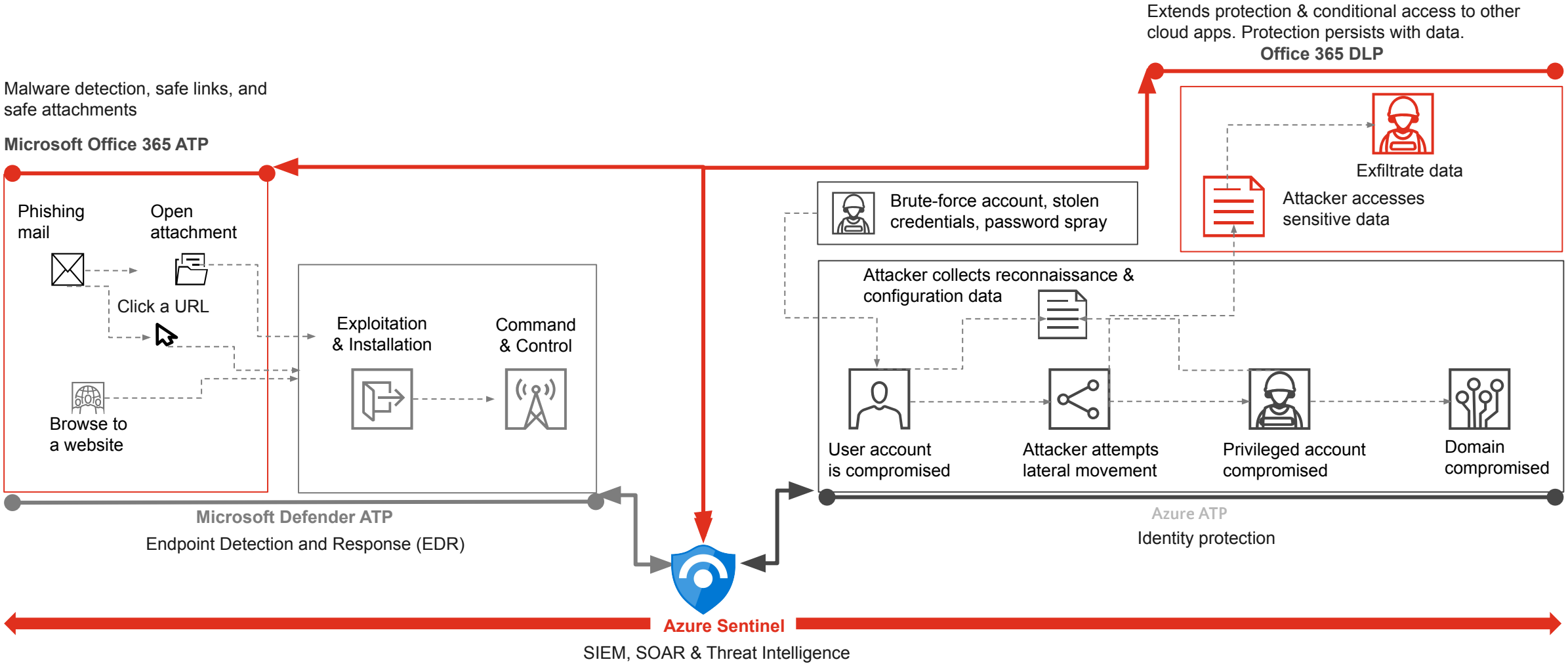
Haitham Al-Jowhari
Partner
Haitham.Al-Jowhari@pwc.com
+971 56676 1146

James Toulman
Director, Cloud Services
James.Toulman@pwc.com
+971 56227 1811

Appendix

Integrated architecture overview

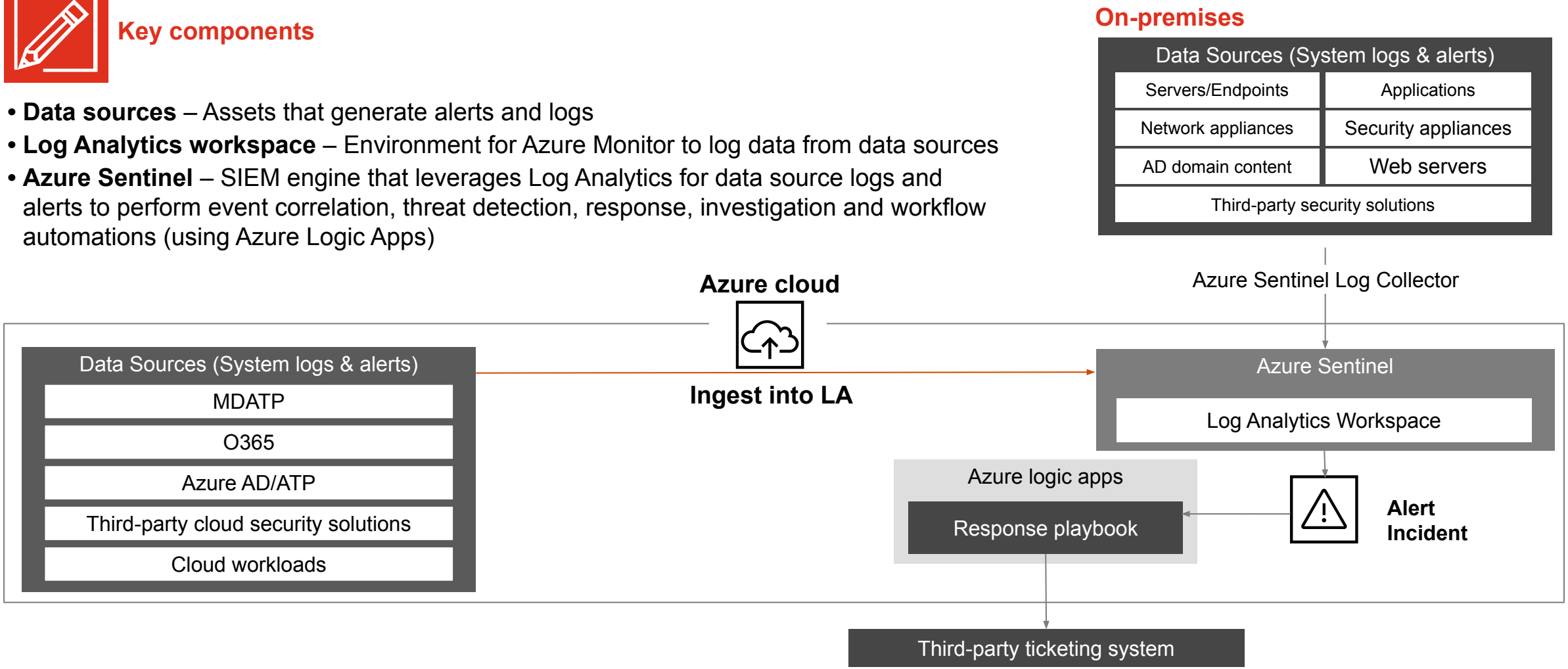
Maximize TDR capabilities during attack stages



TDR integrated architecture

Key components

- **Data sources** – Assets that generate alerts and logs
- **Log Analytics workspace** – Environment for Azure Monitor to log data from data sources
- **Azure Sentinel** – SIEM engine that leverages Log Analytics for data source logs and alerts to perform event correlation, threat detection, response, investigation and workflow automations (using Azure Logic Apps)



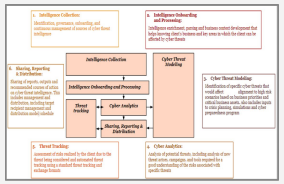
Microsoft & PwC capabilities

PwC has extensive implementation and operational experience with Microsoft products. Our experienced personnel help accelerate TDR deployments by utilizing architecture blueprints and leading engineering practices collected from a variety of engagement experiences. Our teams have experience with various leading SIEMs, SOAR, and UEBA products, along with a threat-driven approach that helps our clients identify how to utilize these toolsets to their full extent.

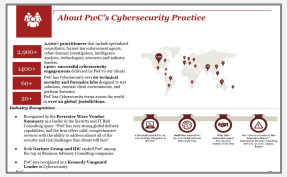
Key accelerators

SIEM use case library & sizing framework

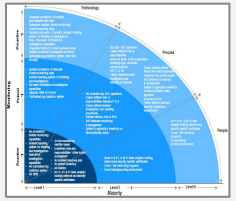
Threat methodology



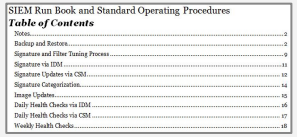
PwC IOC test environment



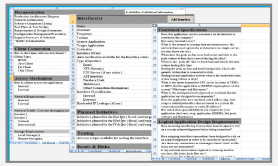
Prioritized integration roadmap based upon current maturity



SOC/SIEM runbooks & processes



PwC CyberOps knowledgebase



PwC's perspective

Microsoft's Azure Sentinel's strong cloud-first focus and advanced capabilities offer a compelling alternative to traditional SIEMs

Microsoft's Azure Sentinel is the first enterprise SIEM built from the ground up on cloud architecture. This is key to scaling rapidly and with agility to detect and mitigate modern-day threats.

Advantages:

- Competitive pricing model
- Free ingestion and analysis of Azure Logs
- Ease of deployment - can be up and running with a few clicks (for MS sources)
- Strong support for historic data-hunting activities
- Leverages Microsoft Advanced Threat Protection intelligence
- Data enrichment happens throughout the data cycle
- Use cases aligned to MITRE ATT&CK framework
- Investigation workflows retain history across multiple user screens/views
- Intelligent automation powered by Jupyter Notebook

Things to note:

- Product features are still being actively developed to a future-state roadmap
- Limited number of connectors to existing security tools are pre-built today
- Currently customization of dashboards is limited to users (but can be achieved through Jupyter Notebook)
- Relies on Microsoft Event Collector & Forwarder

Thank you

pwc.com/me