Microsoft Sentinel

Cheat Sheet

KEY TERMINOLOGY

SIEM	Security Information & Event Management
SOAR	Security Orchestration, Automation & Response
SOC	Security Operations Center
CEF	Common Event Format
KQL	Kusto Query Language

FREE DATA SOURCES

Azure Activity	Azure Subscription-Level Events
M365 Activity	Exchange Online, SharePoint Online & Teams Audit Logs
Defender XDR Alerts	**Alerts** from: Defender for Cloud, Defender for Office365, Defender for Identity, Defender for Endpoints & Defender for Cloud Apps

KEY CAPABILITIES

Data Connectors	Create connections to your Data/Log sources
Analytical Rules	Rules to generate alerts against your log data
Hunting Queries	Ad-hoc queries for hunting low level activities
Workbooks	Provides insight and reporting against your data
Playbooks	Logic Apps for Automation

COST OPTIMISATION

Archiving	Archive data into “cold” storage at a lower cost. Search & Restoration charges apply.
Commitment Tier	Commit to predetermined GB per Day for cost savings on Ingestion.
Pre-Purchase Plan	Purchase Commit Units for 1 year at a discounted rate.

KEY DATA SOURCES

Log Source	Log Volume	Threat Detection	Threat Investigation
IAM	Medium	High	High
EDR	High	Medium	High
Firewall	High	Medium	Medium
Windows Security Events	High	High	High
Database	Medium	Medium	Medium