Hydra Security

Service Overview

HydraSecurity

Who are we?

Microsoft Partner

- Founded by Security Professionals from industries such as Critical National Infrastructure, Government, Military, Financial and Telecommunications Sectors.
- Key strength lies in understanding organisations security operational needs and security use cases. We are cloud focused and intent on building cyber security solutions to meet our customers demands and requirements without selling unnecessary technology.
- Utilizing Innovative and cost-efficient solutions to combat the growing cost and complexity of Cyber Security.

CISSP. CCSP. Microsoft CERTIFIED ASSOCIATE GIAC CERTIFICATIONS

About us

We pride ourselves on searching for new innovative ways are helping clients build security within the business needs

Security Operations

Powered by Microsoft Azure Sentinel

What is SOC & Security Information and Event Management

Security Information and Event Management – Gartner (Gartner,2019) defines the security and information event management (SIEM) market by the customer's need to analyse event data in real time for early detection of targeted attacks and data breaches, and to collect, store, investigate and report on log data for incident response, forensics and regulatory compliance. SIEM technology aggregates event data produced by security devices, network infrastructure, systems and applications.

SOC-as-a-Service

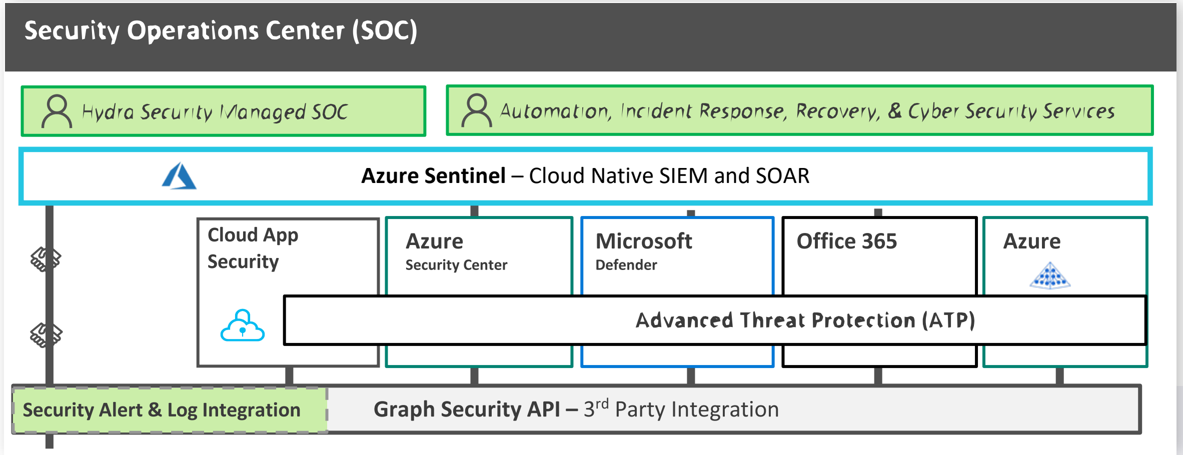
provides companies with the knowledge and skills necessary to combat cybersecurity threats.

Azure Sentinel Managed SIEM

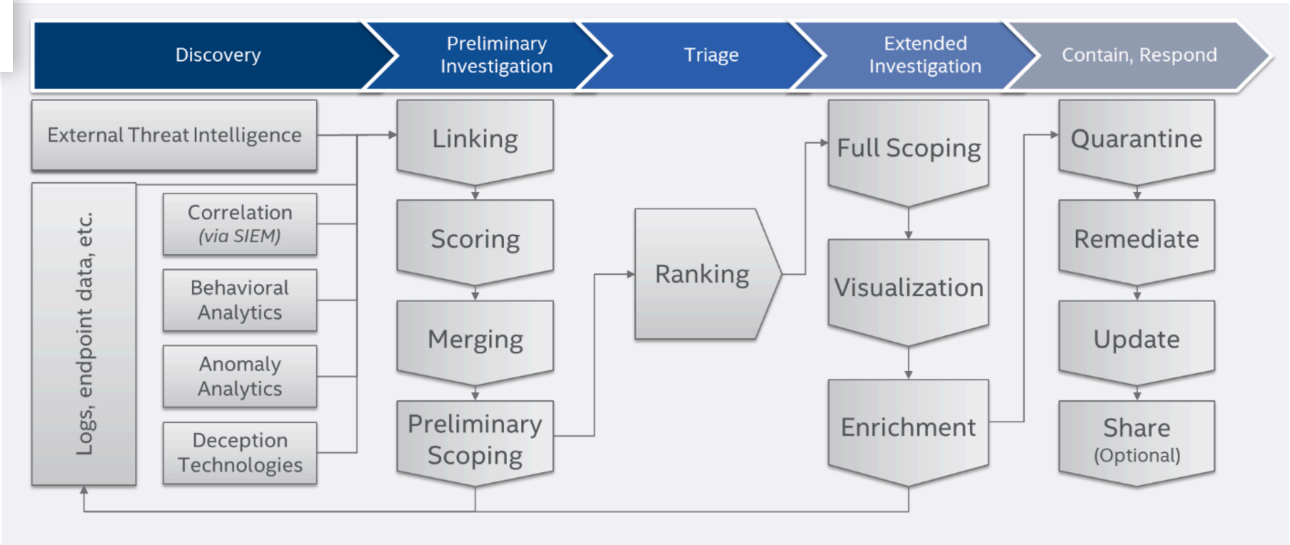
- A cost-effective, cloud-native Managed SOC Service with predictable billing and flexible commitments - Pay for the data you want and flexible subscriptions for expertise
- Potential 24/7 Protective Monitoring
- Trained and Accredited Security & Cloud Expertise
- Pro-Active Threat Hunting
- Security Orchestration Automated Response
- Custom use cases & continuous fine-tuning of existing alerts, playbooks
- Monitor availability of all security log sources (cloud or on-premises)
- Integration with customer organisations ticketing system
- Utilise Microsoft Azure and On-Prem “SIEM-less” integration for POC testing and value

Technology and Process

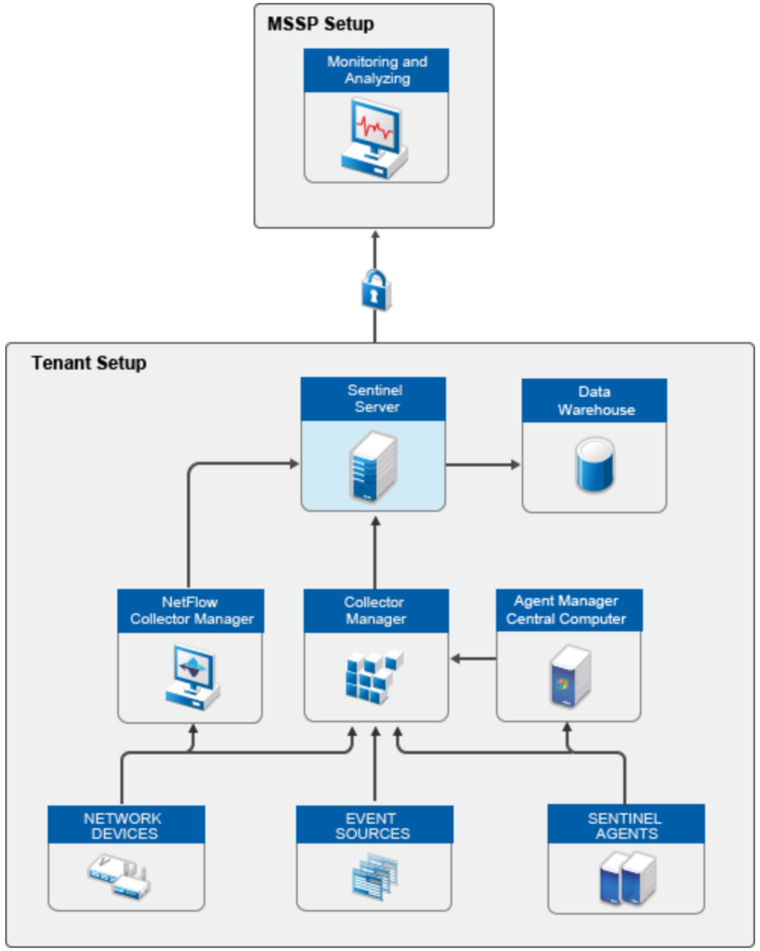
Technology


Security Operations Center (SOC)
Hydra Security Managed SOC
Automation, Incident Response, Recovery, & Cyber Security Services
Azure Sentinel – Cloud Native SIEM and SOAR
Cloud App Security
Azure Security Center
Microsoft Defender
Office 365
Azure
Advanced Threat Protection (ATP)
Security Alert & Log Integration
Graph Security API – 3rd Party Integration

Process



Azure Sentinel Managed Service Model



Sentinel Responder plan

Tier 1 Support – Sentinel Reader
Security Analysts – Sentinel Responder
Automation (SPN) – Sentinel Responder

Full Sentinel Managed Services plan

Tier 1 Support – Sentinel Reader
Security Analysts – Sentinel Responder
Security Engineers – Sentinel Contributor
Automation (SPN) – Sentinel Contributor

Customer Security Monitoring Roadmap

Phase 1 (Month 1)

- Azure Sentinel SIEM Enablement
- Custom Use Cases & Continuous fine-tuning of existing alerts, playbooks
- Azure Sentinel Implementation and Onboarding
- Continuous Security Use Case and Content Management
- Additional Cloud Security Consultancy & Audit Review (Optional)
- Windows Defender ATP Enablement (License Required)
- Fully Customisable Dashboard and Alerting

Phase 2 (Month 2+)

- Full 24/7 Capability
- Security Orchestration, Automation & Response for Incident Response
- Full Incident Response Capability for Incidents (Retained)
- Weekly Reporting for first 3 Months (Baseline Phase)
- Monthly Reporting

Benefits of the Hydra Security Azure Model

- Own your Subscriptions, Data & Modelling
- Transparent SIEM and SOC Costing
- Own your own Intellectual Property (Use Case & Content, Log Source Management etc)
- Utilise the built in capability for all Azure Log Source (O365, Azure AD etc)
- Simple Integration & Windows Native environments
- Cost Efficient Analysis and Access to Top Industry Expertise
- Cloud-Native
- Automation
- Unified Console with restricted access to your subscription ID for better security