Microsoft
Solutions Partner

Infrastructure
Azure

Specialist
Infra and Database Migration

Accelerate Growth on Cloud

Microsoft Sentinel

Microsoft Sentinel

About Blazeclan

- Born in Cloud in 2011
- 750+ Resources 500+ Cloud Certified
- End to End Cloud Competencies
- Focus on Innovation
- Vast Experience Across Domains
- 500+ Customers Engagements
- Culturally Aligned- One Team
- Revenue Growth at 50% CAGR
- Differentiated Proprietary Frameworks

blazeclan

- Microsoft Solution Partner - Infrastructure
- Microsoft Solution Partner - Data & AI
- Microsoft Solution Partner - Digital & App Innovation
- Infra & Database Migration Specialization

Microsoft Solutions Partner
Infrastructure
Azure

Specialist
Infra and Database Migration

- Mentioned in Gartner's Market Guide for Public Cloud Managed & Professional Services, Asia/Pacific 2022
- CRN recognition in MSP500 list in the Pioneer 250 category for 2022
- Ranked 72 in Top 100 Vertical Market MSPs List 2022

Market Recognition & Compliance Certification

Gartner Magic Quadrant
Gartner 'Notable Vendor' – 'Magic Quadrant for Public Cloud Infrastructure Managed Service Providers, Worldwide'

IDC Analyze the Future
IDC 'Major Player' – 'IDC MarketScape: APAC Managed Cloud Services Vendor Assessment Report'

ISO 27001 Certified
ISMS

ISO 22301
BCMS

GDPR
GDPR Compliant

PCI DSS Compliant

Great Place To Work. Certified
Back to Back 3 years (2020, 2021,2022)

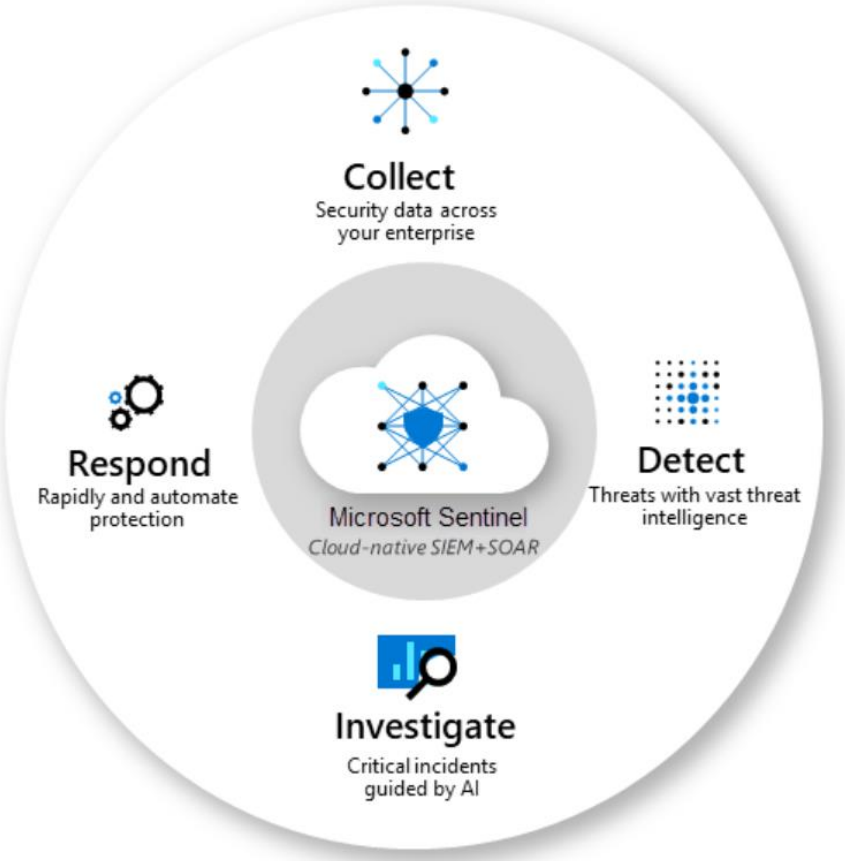
Key Partnerships

CLOUDFLARE
paloalto NETWORKS
HashiCorp
New Relic.
vmware Partner Connect
TREND MICRO
snowflake
databricks

Microsoft Sentinel (Cloud Native SIEM)

Microsoft Sentinel is a scalable, cloud-native solution that provides:

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)



Incident Management & Reporting

Network Traffic Analytics

Workspace

Active Threat Watch

Governance Reporting

Security Orchestration, Automation and Response

What we Offer in Microsoft Sentinel Deployment

Platform Setup, Deployment and Integration

- Azure Portal Setup
- Data Collection
- Data Ingestion
- Data Parsing and Normalization
- Security policy and alert management.
- Detection Rules and Playbook Creation
- Threat Intelligence Integration
- Visualization and Reporting.
- Integration with Azure services and SOAR Platforms

Search and Hunting

- Wide search and correlation across infrastructure for anomaly and probable threat.
- Recommendation of new security policy based on emerging threat to industry.

Governance Reporting

- Configure weekly and monthly incident reporting.
- Configure security incident dashboard for broader view of SOC maturity and support.
- Configure KPI and SLA reporting for executive view.
- Configure compliance-based reporting, which includes SOC2 / ISO 27001 / PCI-DSS.

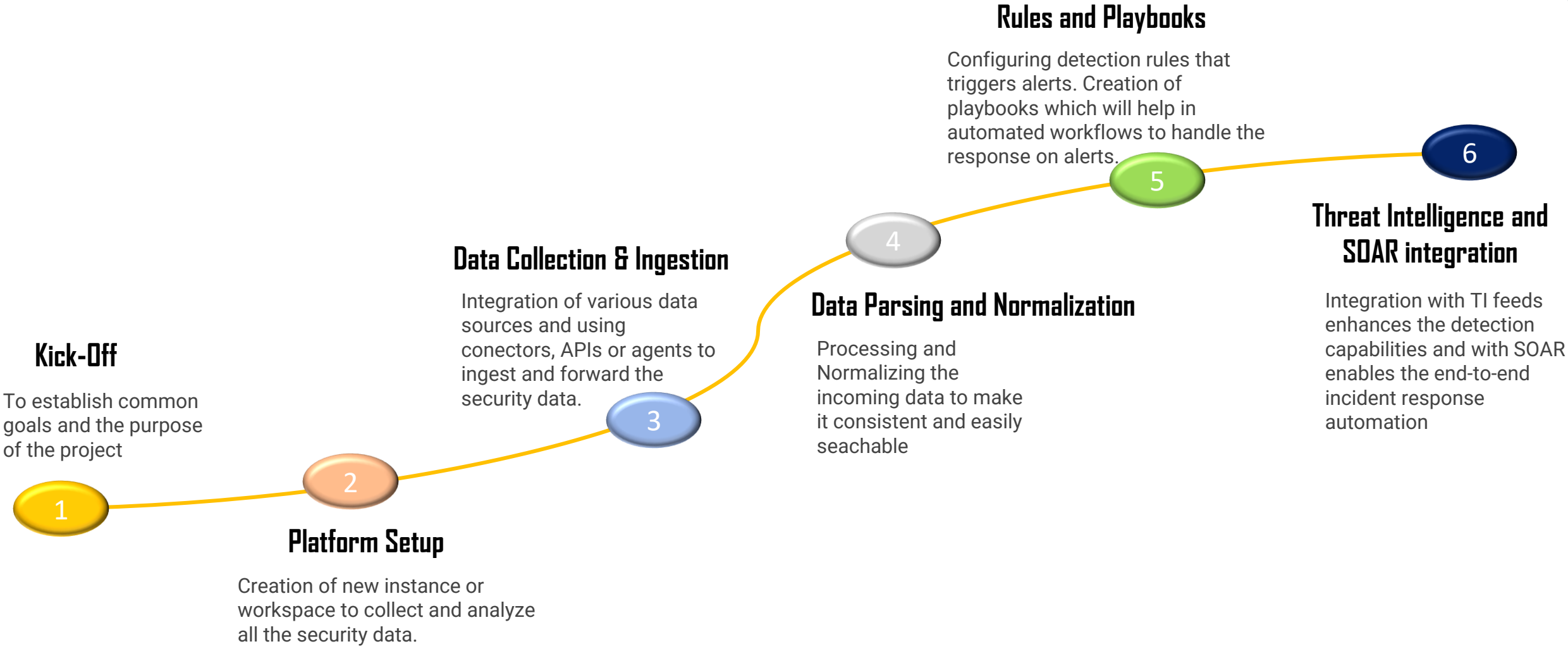
Access to Runbook Library

- Wide range of runbook library.
- MITRE ATT&CK framework integrated use cases repository.
- Support for incident response automation playbook creation.

Technology Supported

Sr. No	Technology
1	Firewall
2	Load Balancer (HLB)
3	Windows / Linux servers
4	Intrusion Prevention System (IPS)
5	VPN
6	Anti-SPAM/Mail Relay/Anti-Phishing
7	Proxy (Forward)
8	Anti-Malware
9	Data Loss Prevention (DLP)
10	Network Behavior anomaly detection (NBAD)
11	Active Directory
12	Domain Controller
13	DHCP
14	Database
15	Virtualize Infrastructure
16	ITSM Tool
17	PIM
18	WAF
19	DDOS
20	Cloud services (Azure / AWS / GCP)

Service Delivery Roadmap



Deliverables

Areas	Activities	Deliverables
Azure Portal Setup	Create a new instance or workplace to collect and analyze all the security data.	• Provisioning Resources • Configuration Settings • Access Credentials • Security Measures • Connectivity • Compliance and Governance
Data Collection	Integrate data sources like Azure services, 3rd party security solutions like firewalls, IDS/IPS and many more.	• Data Sources Configuration • Log Collection Rules • Log Integration and Mapping
Data Ingestion	Use connectors, APIs or agents to ingest and forward security data to Aure Sentinel	• Data Source Discovery • Data Collection Strategy • Connector Configuration • Data Mapping and Transformation
Data Parsing and Normalization	Process and normalize the incoming data to make it consistent and easily searchable.	• Field Extraction Rules • Regular Expressions or Parsing Logic • Field Mapping and Renaming
Creating Custom Connectors	To gather data from sources not covered by the default connectors.	• Connector Design Documentation • Connector Architecture • Data Source Configuration
Detection Rules and Playbooks	Configure detection rules that trigger alerts when specific patterns or anomalies are detected. Playbooks helps in automated workflows to handle responses to the alerts.	• Rule Description and Context • Detection Logic or Query • Logic and Criteria definition • Use Case Mapping • Playbook Design and Workflow

Deliverables

Areas	Activities	Deliverables
Analytics	Write custom queries using KQL for data analysis.	• Detection Logic and Query • False Positive Mitigation
Threat Intelligence Integration	Integrate TI feeds to enhance the detection capabilities.	• TI Source Selection • Data Source Configuration • Integration Logic • Threat Data Visibility
Incident Management	Azure Sentinel helps investigate, respond and manage incidents via automated or manual response.	• IM Strategy • Incident Classification Criterya • Incident Investigation Guidelines • Escalation and Response Procedures • Post-Incident Analysis • Incident Closure and Documentation
Visualization and Reporting	Use built-in or custom dashboards to visualize security data and insights.	• Dashboard Layout and Composition • Drill-Down Capabilities • Real-Time and Historical Data • Automation of Reporting • Compliance based reporting, which includes SOC2 / ISO 27001 / PCI-DSS
Integration with Azure Services and SOAR platforms	Integrate with Active Directory and SOAR platforms to enable end-to-end incident response automation.	• SOAR tool selection • Data Integration Plan • Incident Workflow Definition • Automated Response Logic

Blazeclan Technologies Pvt ltd

Godrej Eternia C, A-Wing, 8th Floor, Old Pune-Mumbai Rd, Wakadewadi,
Shivajinagar, Pune, Maharashtra 411005

+91 9689889138

sales@blazeclan.com

www.blazeclan.com

blazeclan