

Azure Sentinel Managed + Advanced Security Services

By: FyrSoft Engineering



“We’re dealing with applications that run our business, so to be able to do this transformation efficiently and manage the updates consistently, is very important to us. That’s why we chose FyrSoft.”

- John McConeghy,
IT Manager, Pella

8 Microsoft Competencies

2 years running
Cloud Partner of the Year


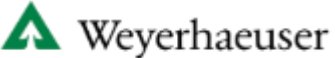

Over 350 years of collective
enterprise workplace
experience

Over 75 tailored
engagement plans tied to
Microsoft programs

Leading Fortune 500
clients choose to work with
FyrSoft

Over 250 enterprise clients
across 40 states



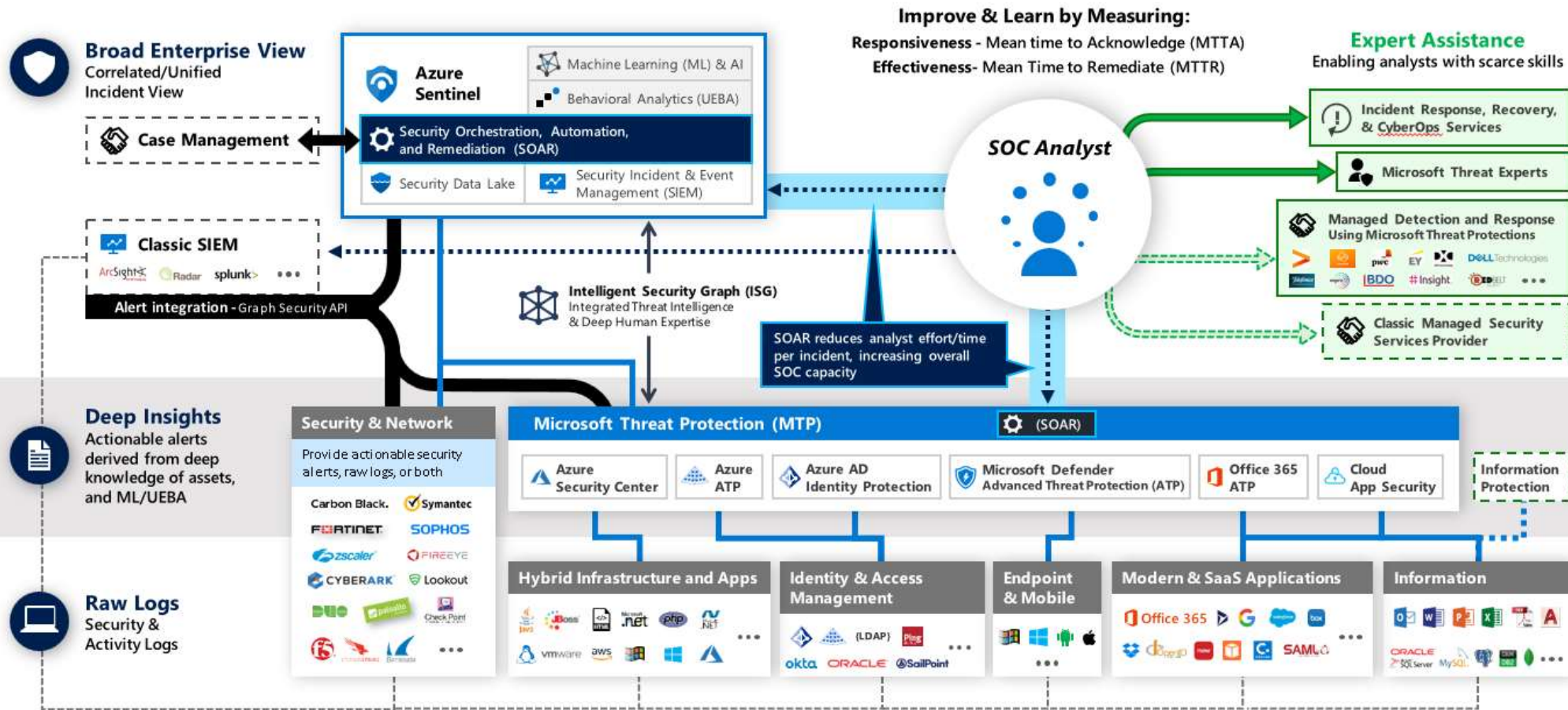
					
					
					
					
					
					

Security Operations Center

Microsoft Reference Architecture

Legend

- Event Log Based Monitoring
- Investigation & Proactive Hunting
- Outsourcing
- Consulting and Escalation
- Native Resource Monitoring



FyrLight Program for Cybersecurity

- Offer Includes:
 - Rapid Deployment of Azure Sentinel, Log Analytics, and Automation
 - Configure and Validate data connectivity for Azure Sentinel ingestion
 - Agent Deployment and Health Check to ensure information stability
 - Azure Sentinel cybersecurity validation of data and alert rules
 - Cybersecurity reporting and results orientation and review
 - 24x7 Security Operations Center monitoring and alerting

Azure Sentinel: Advanced Deployment

FyrFighter Program: Cybersecurity Rapid Deployment Kit

Azure Sentinel Management and Deployment



FyrFighter RDK and Assessment

- To gain a better understanding of existing infrastructure, we launch an assessment to gather requirements and provide a realistic cost estimate for the SIEM solution integration
- Immediately Plan and and configure Azure Sentinel
- Depending on endpoint agent availability, we help to understand which telemetry and signal data will be viable for the solution.
- Ensure successful onboarding

Rapid Deployment

- Deploy alerts and playbooks
- Operationalize and Tune alerts
- Ensure Rapid Agent Deployment
- Exercise real world threat hunting

Sentinel Managed

- Ensure you are running optimally and fine tune alerts and playbooks
- We will monitor the availability of your log data
- Ensure the right person is assigned with our Service Desk integration for ITSM
- Ensure you receive alerts of cost spikes out of range of budget
- Threat Intelligence feeds to assist in known attacks and mitigations
- Service support and assistance with monthly service calls
- Management of Agents

Managed Azure Sentinel (SIEM \ SOAR)

- We specialize in Azure Sentinel and the underlying technologies.
- We help companies to establish a clear understanding of cloud-born SIEM.
- The history of our experience in both on-premises and cloud implementations includes a breadth a history with complimentary awards for superior delivery.
- As organizations rush to migrate or enhance existing or new workloads, there is a real business need to ensure security is high on the radar.
- As the Traditional approach to security adopts modern solutions, our customers continue to rely on our experience in helping them with their cloud journey.

Managed Cybersecurity

Azure Sentinel + Managed Security Services

- Use Azure Sentinel now and auto-scale when you require, and don't pay for resources you don't need.
- Built on the best Operating Procedure principles, we perform a rapid deploy according to your requirements
- Deploy Azure Sentinel and connect it to our SOC in order to quickly strengthen your security posture so that you can ensure you are protected against potential threats. With managed security 24x7x365 , you are able to redirect your attention to the business where it matters most.

Cybersecurity Consulting

- We have the knowledge to integrate your existing tools and workloads with many commercial security solutions, and custom tools
- We can help you with your threat intelligence through tailored detections, alert integration, machine learning models
- Our team of threat hunting experts not only help you with the deployment, but we help monitor or augment your staff in the event of ongoing support and management or incident response

Cybersecurity Managed FyrSoft Threat Experts

Managed Cybersecurity Security Operations Center as a Service (SOCaaS)

Cybersecurity Services

Strategy

- Utilize our Cybersecurity Strategy services in order to help you establish a best practice design,
- Ensure you have an established program for your organization
- Cybersecurity Implementation services were created to help you maneuver quickly and provide maximum cybersecurity value
- Cyber Risk and Compliance services help your organization to understand the costs associated
- Threat services identify threats, remediate vulnerabilities and solve specific security challenges

Design

- Utilize FyrSoft Airlift and Rapid Deployment Services to enhance your Azure Sentinel Deployment.
- Our Security Architects are very experienced with NIST Cyber Security Framework

Defense

- We enable your organization with Security Incident Response through cybersecurity consulting services in order to allow you to help maintain business continuity
- Cybersecurity Training services help your staff understand what risks to look out for and help improve overall cybersecurity postures and reduce risk
- We help align your Identity and Access Management services that help ensure that your devices and identities are managed

Support Escalation Matrix

Tier 1	Tier 2	Tier 3
Initial Threats	Escalation of Critical Threats	Onsite Incident Response
Alert Remediation	Outages lasting longer than 4 hours	
Escalation to Tier 2	Included	Included
Email 24x7x365	Included	Included
Playbook Customization	Included	Included

How we align with Microsoft (four pillars)

Data & AI

M365

Advanced Security

WVD

