satisnet
streamlining security management

Microsoft

Azure Sentinel SOC Service

Azure Sentinel - SIEM reinvented for the Modern World

Satisnet provides a 7 x 24 x 365 Azure Sentinel based Security Operations Centre SOC, UK based & staffed.

- Zero Hours Contract – Pay as You Go!
- Use Cases – largest online library, Compliance, MITRE ATT&CK and REAL TIME
- Managed Detection & Response
- Automation of tasks and tooling
- Full Incident Response
- Threat - Intelligence & Hunting
- Vulnerability Management Integration
- Network Detection
- Purple Teaming constant tuning

Satisnet Security Operations Team

Delivers instant value to your defenders

Cloud + Artificial Intelligence

Scales to support your growing digital estate
Uses AI & Automation to improve effectiveness

Azure Sentinel uses Machine learning and AI, but like all SIEM's it still needs skilled resource to understand the detections that surface and investigate alerts to ascertain if they are true incidents and how Incident Response should be handled.

Satisnet have been deploying and managing SIEM solutions for 15+ years, providing an array of cybersecurity skills and expertise aimed at ensuring customers obtain real benefit and security protection from a SIEM. As leaders in the SIEM domain we have developed a Security Orchestration Automation & Response SOAR platform, a Threat Hunting platform and are a contributor\investor in SOC-Prime the recognised leader in SIEM Use Cases content via the Threat Detection Marketplace TDM platform. Satisnet also provide 'real world' SIEM/SOC training courses that are hands-on and aimed at ensuring security analysts 'think outside the box'.

Copyright Satisnet Ltd. 2021

satisnet
streamlining security management

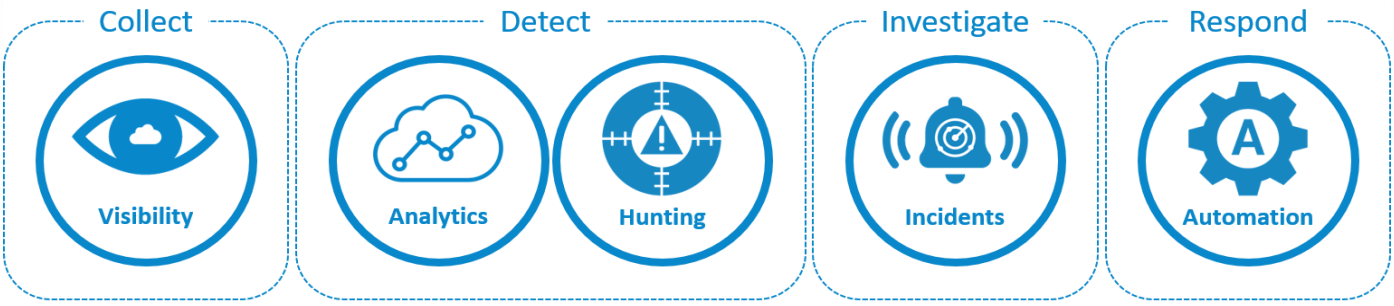
Microsoft

The SIEM Journey

Satisnet work with customers in all aspects of designing and implementing a SIEM and SOC solution. Implementations consist of 4 main phases; Collect, Detect, Investigate and Respond. The journey typically starts with requirements gathering, customers often know they require a SIEM but are unsure of what the 'art of possible' is in using it and this is where we can help. We can highlight what problems the SIEM can solve and also assist in the nitty gritty of;

- **Scoping how to achieve specific compliance requirements.**
- **How to achieve specific business use cases.**
- **How to size and price the solution, to include ongoing Business as Usual (BAU) operational resourcing and costs.**
- **Provide speedy PoV (Proof of Value) instance of Sentinel using the customers data to quickly illustrate the value it can bring.**

Once the journey begins Satisnet has a range of services that can further assist the customer to ensure they obtain maximum benefit from Azure Sentinel as outlined below;



Azure Sentinel Functions

- Gap Analysis
- MITRE ATT&CK Mapping
- Compliance Mapping
  - PCI
  - Gov Connect
- Definition of Use Cases
- On-Boarding of log sources
- Workbooks (Dashboards)
- Reports
- Alert Handling
- Incident Response

- Auto-collection of context/IOC's
- Rules-Tuning
- Machine Learning – Tuning
- Vulnerability Mgt Integration
- KQL Searches
- Threat Intelligent Based
- Using Opensource & Commercial TI
- Vertical Intelligence
- Latest Threats
- Brand Abuse
- VIP
- Triggered Hunts

- Managed Detection/Response
- Ticketing Integration
- Advanced Hunting (Jupyter)

- Customer Team Engagement:

- Containment
- Triage
- Remediation
- Auto-Tuning of Incident Response
- Recommendations

- Workflow – Logic Apps Power BI mapping to customer processes
- API Integrations
- SOCAutomation
- SDA Integration
- Security Datamining of any Data
- Terraform - Running security stack as code

MSSP Services – Pay as you Go

Satisnet offer a unique Azure Sentinel 'Zero Hour contract' MSSP service to our customers. Sign up to use our SOC services with a manageable monthly investment and minimum period. No lock-in means you can cancel the service at any time. In addition, we can offer this service as 'Business Hours', 'Out of Hours (OOH)' or as '7x24x365'.

www.satisnet.co.uk
+44 (0) 1582 369330

satisnet
streamlining security management

Copyright Satisnet Ltd. 2021