Microsoft Security Services

Microsoft Sentinel

AUJAS CYBERSECURITY™

Key Proficiency Aujas Cybersecurity using Microsoft Sentinel

- ✓ Integration with 120+ Built in Data Connectors
- ✓ MITRE ATT&CK mapped analytic rules.
- ✓ ML based User Entity Behavior Analytics
- ✓ Advanced Threat Hunting
- ✓ Threat intelligence
- ✓ Security, Orchestration, Automation and Response
- ✓ Machine Learning Notebook

Introduction

- Aujas provides detailed workshop on Microsoft Sentinel. This workshop intends to discuss on how managed security services capabilities, including 24x7 security monitoring, threat detection, incident handling and response services can be leveraged for effective threat and incident management using Microsoft Sentinel.

Aujas Microsoft Sentinel Workshop Agenda

Aujas team covers below areas in detailed workshop

- Cloud native SIEM
  - Implement, configure Microsoft Sentinel and connect different security and network log sources to Microsoft Sentinel.
  - Configure and customize MITRE ATT&CK framework mapped analytic rules.
  - Configure and customize dashboards and reports.
- User Entity Behavior Analytics
  - UEBA Anomaly Detection – Utilizes machine learning to detect anomalous activities of users and entities.
- Threat Hunting and Threat Intelligence
  - Threat Hunting – Utilizes machine learning for hunting
  - Threat Intelligence – It integrates with many threat feeds using the TAXII connector.
- SOAR
  - Multiple playbooks to automate task, provides integration with your ticketing tool.

Values we deliver through our workshop

Advance AI/ML

- Capability demonstration on Microsoft Sentinel exploring advanced AI/ML capabilities.

Security Automation

- Demonstration on security automation around customized analytic rules, customized playbooks to automate incident response.

Benefits over Traditional SIEM

- Demonstration around Log optimization.
- Less false positives.
- Comprehensive threat management, SecOps, UEBA

Contact us

For more details, please connect us at email: suhas.desai@aujas.com