SHAHBAZ AHMED

m: +966 549 464 270
e: cybextalk@gmail.com

HANDS ON EXPERIENCE/SKILLSET

- Symantec Endpoint Protection
- Symantec Endpoint Protection Cloud
- Symantec Data Center Security : Server Advance
- Symantec Protection Engine for Cloud
- Symantec Protection Engine for SharePoint
- Symantec Advance Threat Protection
- FireEye HX Advance Endpoint Security
- CB Protection - Application Whitelisting
- Cisco Advance Malware Protection
- CTM360 - Cyber Threat Management
- Symantec Email Security Cloud
- Symantec Mail Security for exchange
- McAfee Client Proxy
- SecureWorks - MSS
- Sophos Advanced Endpoint Security and Control
- iDahboards Performance Analysis
- Splunk Enterprise - SIEM
- Structured Queries Language (SQL)

KEY ACHIEVEMENTS

- **Lateral Movement Implementation -** Implemented customized host-based firewall across all organization's workstations globally with a network of 40,000 endpoints to prevent threat lateral movement and reduction in malware spread.
- **Web Server Configuration and Defacement Prevention** - Implemented File Integrity Monitoring to prevent unauthorized access/changes to the web server configurations and application directories.
- **System Lockdown Implementation** - Implemented system lockdown by Symantec across the globe, a network 40,000 endpoints to proactively block the IOCs shared by threat intelligence vendors in case there are no definitions released by security vendor or agents are outdated.
- **Global Endpoint Security Implementation** - Deployment of Symantec Endpoint Protection solution (around 40,000 endpoints) across the globe.
- **iDashboard Project** - Interactive dashboard creations for Carbon Black protection, Symantec endpoint protection, Sophos Endpoint protection and McAfee encryption for compliance, health and to monitor alerts 24*7
- **Sophos Endpoint Security and Control Implementation**- Anti-malware solution deployment across 300+ branches of a leading bank in Pakistan
- **Sophos Endpoint Security and Control Implementation** - Anti-malware solution deployment for leading Defence organization in Pakistan

Cyber Security Professional - 14+ years experience

Major Responsibilities

- Install, configure and maintain endpoint security tools such as host firewalls, antimalware software and work with departments to ensure security configurations are set appropriately to secure the systems and information.
- Creation of real-time reports by interacting with endpoint security backend SQL databases to proactively measure the health of agents i.e. agent versions, up-to-date status, top systems indicating alerts etc.
- **Mitre ATT & CK** framework implementation guideline, test scenarios study and mapping use cases for event correlation to create security incidents for SOC analyst to work.
- Analyse the latest threats news in context to the organization and preparing actions plans, recommendations and reports for senior management.

- Perform analysis of events/incidents and provide remediation suggestions to relevant owners
- Create and deliver reports to business lines pertaining to endpoint security, compliance, etc
- Research and document security best practices for Endpoints to continually improve endpoint security
- Participate in application troubleshooting and incident problem resolution with other infrastructure teams, including application, storage, messaging, and server teams
- Conducts analysis using a variety of tools and data sets to identify indicators of malicious activity on the network
- Support/ownership of application and hardware for Endpoint Protection and participate in on-call rotation
- Collaborates with technical and threat intelligence analysts to provide indications and warnings, and contributes to predictive analysis of malicious activity
- Handle security incidents ensuring containment, eradication, and recovery with proper evidence collection and documentation through to closure
- Escalate threats and incidents to management as defined through documented processes
- Proactively search for threats and suspicious behaviour within the enterprise
- Creating, raising and presenting change management requests in Global Change Advisory Board meetings for the new implementation and configurations.
- Plans, develops, installs, troubleshoots, maintains and supports an operating system and associated server hardware, software and databases ensuring optimum system integrity, security, backup and performance.
- Creative, innovative, willing to take responsibilities and accept challenges
- Gathering threat intelligence and stay up-to-date with trends in information security in order to provide advice to management on the larger IT security environment and current events.

EDUCATION

Master in Business Administration 2007-2009
Major: Management Information System

CERTIFICATIONS

- ISO/IEC 27001 Lead Implementer
- Sophos Sales Developer
- Sophos Certified Sales Consultant
- Sophos Certified Engineer
- Sophos Technical Support

TRAININGS

- Symantec Endpoint Administration 12.1
- Symantec Endpoint Administration 14
- Symantec Data Center Security : Server Advanced
- iDashboard
- Securing Windows 2016 Server
- Root Cause Analysis Failure

SELF STUDY

- CompTIA CASP
- Post Exploitation Hacking
- Nessus Fundamentals