SANDEEP BALKRISHNA KANVINDE

E-Mail: sandeepbalkrishnak@gmail.com
Phone: +91-9870013336/ +971-545562787

Endpoint Security ~ SOC Operations ~ Cyber Security Analyst ~ Vulnerability Assessment ~ Security Audits

PROFILE SUMMARY

Abilities in developing information security frameworks, conceptualizing information security policies and ensuring compliance with security standards & procedures. Comprehensive understanding & proficiency in Security Products/ Tools, Incident Analysis, Vulnerability Assessments and Penetration Testing,

Skilled in handling security audits & compliance assessment for evaluating the effectiveness of controls and compliances. Capable of directing overall operations of the organization, inclusive of formulation of strategies, planning for achieving targets, and achieving all round business growth, using IT as a strategic platform.

Seeking a competitive position in the Information Security area and evolve as an Information Security Professional.

SKILLS

Network	OSI Model, TCP/IP, VPN, Cisco (Sourcefire, WSA, ESA, IDS/IPS), FortiGATE NGFW, Network Security, FireEye (Hx/Nx/Ex/Ax), Wireshark, NetMinner.
Software	ArcSight, LogRhythm, McAfee (ePO, ATP, ATD, ENS, Proxy), Symantec (DLP, ICE, ICT), Seclore (RMS, DRM & Classification), MDM (AirWatch & 1Mobility), Arcos IDM/PAM, Nmap, Nessus, Burp Suite, Sqlmap, ProcMon, Netsparker, Metasploit,, MBSA, Vega, Acunetix, W3af, Qualys Guard, OWASP Top 10. Sophos Encryption, WinMagic Encryption.
Operating System	Windows, Linux (Red Hat, Ubuntu, Kali).
Security	Incident Response, Malware Analysis, Intrusion Detection, Security Operations, Security Analysis, SIEM Tools, Threat & Vulnerability Mgmt, ArcSight, Packet Analysis, System and Security Monitoring, Network Security, Operating System Security, Threat Analyst, CIS Benchmark, ISO 27001/2, NESA framework.
Comp Skills	Word. Excel, PowerPoint, Outlook and Office365 Suite.

WORK EXPERIENCE

Security Consultant – SOC and Compliance
GTFS Bin Zayed Group, Abu Dhabi - 10th Feb, 2019 till 30th May 2019
Security implementation and consulting for an Abu Dhabi based Government Organization:

- Plan, research and design robust security architectures for any IT project and test security solutions using industry standard analysis criteria.
- Define, implement and maintain corporate security policies.
- Review vulnerability testing, risk analyses, security assessments reports and prepare risk register for tracking.
- Coordinate with client and end-user to understand their Vulnerability Assessment requirements.
- Conduct meetings with client/end-user and recommend application owner to apply new patches according to CIS benchmark, ISO 27001 and NESA guidelines on application to mitigate vulnerability.
- Developed plans for a quarterly Vulnerability Management and Risk Assessment activities to mitigate identified vulnerabilities inside network to prevent future attacks.
- Proactively monitored security event queues and recommend improvements based on events or incidents of security breaches in the areas of networks, applications, databases, systems, and endpoints.
- Supported in defining and updating security policies & processes, led security solutions for Antivirus, Next Generations Firewall Management, Email Security, and Advance Threat Protection.

Security Analyst – SOC
Catalyst Business Solutions LLC, Dubai - 14th Jan, 2018 to 4th Feb 2019
Federal Network Wipro project partner payroll with Catalyst Business Solutions LLC

- Proactively hunt for and research potential malicious activity and incidents across multiple platforms using tools like HP ArcSight, LogRhythm, advanced threat network and host-based tools.
- Build indicators of compromise into monitoring tools using internal and external sources to integrate these tools with one another to provide data enrichment
- Strong TCP/IP networking skills used in performing network analysis. Also isolate and diagnose potential threats and anomalous network behaviour
- Worked on advanced behavioural analytics, threat hunting, built-in incident response and SOC automation

- Recognize potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information.
- Perform static and dynamic malware analysis on virtual servers with proper documentation and steps for removal on infected systems.
- Analyse traffic, review logs and identify potential security threats and manage all confirmed incidents as per the Incident management processes.
- Interact with malicious programs by redirecting and intercepting network traffic to properly explore its capabilities
- Analyse malicious Microsoft Office, RTF, and PDF files
- Worked on EDR solutions like FireEye (Hx, Nx, Ex, Nx), Sophos for advance threat detection and management.
- Managed security tools: Cisco (ESA, WSA), Sourcefire (IPS/IDS), Arbor DDOS solution, MS Exchange email activity monitor.
- Perform vulnerability assessment using QualysGuard and Nessus VA Scanner.
- Worked in a 24x7 Security Operations Center.

Lead - Cyber Security Analyst
Network Intelligence Pvt Ltd., Mumbai, India - 9nd May, 2016 till 17th Dec 2017
Security implementation for an Indian Insurance Organization:

- Develop plans to safeguard computer files against unauthorized modification, destruction or disclosure. Implement and maintain corporate security policies.
- Choose, implement, monitor and upgrade computer/ server anti-virus and malware protection systems. Create custom policies to prevent virus attacks.
- Encrypt data transmissions and erect firewalls to conceal confidential information during transmit.
- Educate workers about computer security and promote security awareness and security protocols.
- Keep accurate and current backup files of all important data on the shared corporate network.
- Conduct quarterly internal/external security audits.
- Perform vulnerability testing using various product such as:
  Nessus VA Scanner (Port Scanning, Host and Device detection, Credentials scanning, Generate Reports, Analyse Malicious activity, Plugins configuration), Acunetix, MBSA, NMAP/SPARTA, NetSparker, Vega, OWASP Top 10 etc.
- Anticipate security alerts, incidents and disasters and reduce their likelihood
- Manage network, intrusion detection and prevention systems.

Security tools Implemented for IndiaFirst Life Insurance (Network Intelligence Client):

1. Mobile Device Management: 1Mobility & AirWatch
2. McAfee (ePO, Virus Scan, ENS, ATP, HDLP, NDLP, Proxy)
3. Seclore (IRM/DRM/ Document Classification)
4. IBM Qradar SIEM Integration with Proxy, AV and Firewall

Tech Support Engineer (Information Security)
Infovie Software Solutions Pvt. Ltd., Mumbai, India - 16nd Sept, 2015 to 4th May, 2016
End point Security product implementation for an Indian Insurance Organization

- Implemented Cososys End Point Protector DLP for over 700 endpoints
- Designed and configured the DLP implementation singlehandedly
- Provided guidance, recommendations, best practices, etc. for DLP operations, stabilize and optimize DLP system performance, including rules and reports, assist with DLP upgrades, installations and configuration.
- Liaise with EPP DLP Support, Engineering, Product Management, and other areas within EPP on behalf of the customer.
- Provide single point of contact and hands-on escalation and remediation for critical issues.

Projects Handled:

Title: Endpoint Protector Data Security Implementation (DLP) in Infrastructure Environment
Client: Insurance Company, Mumbai
Duration: 5 Months
Role: Project Lead
Description: This involved updating of Security patches & applying local group polices. It dealt with port changing, implementation of backup process, Applying user based device policy. Applying Content based security policy. Troubleshooting, Support, Live Production testing.

Title: Endpoint Protector Data Security Implementation (DLP) in Infrastructure (Remote Deployment)
Client: Software Company, Pune
Duration: 1 Months
Role: Project Lead
Description: This involved updating of Security patches & applying local group polices. It dealt with port changing, implementation of backup process, Applying user based device policy. Applying Content based security policy. Troubleshooting, Support, Live Production testing.

System Administrator
eMudhra Ltd., Mumbai, India - 22nd Sept, 2014 to 11th Sept, 2015

- Maintain and administer computer networks and related computing environments, including computer hardware, systems software, applications software, and system configurations.
- Perform data backups and disaster recovery operations.
- Operate master consoles in order to monitor the performance of computer systems and networks, and to coordinate computer network access and use.
- Perform routine network startup and shutdown procedures, and maintain control records.
- Recommend changes to improve systems and network configurations, and determine hardware or software requirements related to such changes.
- Maintain logs related to network functions, as well as maintenance and repair records.
- Coordinate with vendors and with company personnel in order to facilitate purchases.

IT Executive
YOMA Multinational LLP, Mumbai, India - 22nd June, 2014 to 11th Sept, 2015

- System Integration and Vendor management
- Maintain and administer computer networks and related computing environments, including computer hardware, systems software, applications software, and system configurations.
- Perform routine network startup and shutdown procedures, and maintain control records

Desktop Support
IDC Technologies Inc, Mumbai, India - Feb, 2014 to 24thJune, 2014

- Application Troubleshooting, Tally, Spine, Intuit Quick Books, Digital Signature installation.
- VM VSphere, Thin Client, Network Printer, WiFi Router, VoIP Phone and overall Network Troubleshooting and Management.
- User Management in Active Directory, OS and MS Office Installation, Outlook Configuration, & Troubleshooting.
- MS-SQL Server 2008 & Visual Studio installation and troubleshooting.
- Maintaining Asset inventory of all computer parts and vendor management.

Desktop Support
Harjai Computers Pvt. Ltd., Mumbai, India - 26 Nov, 2012 to 6 Dec, 2013

- Handling all sort types of Desktop level issues on windows 2000/XP Professional/ Vista/ Win7.
- Configuring & Troubleshooting Issues withMS Office & MS-Outlook 2003/ 2007.
- User Management in Active Directory, OS and MS Office Installation, Outlook Configuration, & Troubleshooting.
- Maintaining Asset inventory of all computer parts and vendor management.
- Handling the LAN network of more than 4500+workstation of Win 2000, XP, Win7

EDUCATOIN DETAILS

- Master of Management Studies (MMS), Alamuri Ratnamala Institute of Engineering & Technology, Aug 2013-2015.
- Bachelor of Computer Application (BCA), YCMOU, July 2009 - June 2012

CERTIFICATIONS

- Certified Ethical Hacker – EC-Council, June 2019
- Certified Information Security and Ethical Hacking (CISEH), Pristine Info Solutions in 2015.
- ITIL v3 – PeopleCert, March 2019
- Malware Analysis training certification by Udemy e-learning portal
- IBM Qradar Foundation and Administrator training certification by Udemy e-learning portal
- ISO 27001 Lead Implementer training from TUV-SUD, Apr 2019
- CMS Certified Network Specialist Certification (CCNS) A+/ N+/ MCSE/ RHCE/ S+ from CMS Institute in 2011
- CCNA Cisco Certification Training from Nirmal Datacom Pvt. Ltd. in 2012
- Diploma in Computer Hardware from Sonali Computer Specials in 2006
- MSC-IT, MKCL in 2009

PERSONAL DETAILS

Nationality	: Indian
Date of Birth	: On Request
Languages Known	: English, Hindi & Marathi
Passport no	: On Request
Mailing Address	: Bur Dubai, 31219, Dubai, UAE,