SUNDAR KRISHNAN

CISSP, CISM, CDPSE, PMP, ITIL, Six Sigma BB | Sundar_Krishnan@Outlook.com

PROFESSIONAL SUMMARY

- Cybersecurity professional & management executive having 27 years of IT experience including 10+ years of Information Security experience, with ability to connect security goals and objectives with business mission.
- Possess a passion to develop, lead, execute and manage customized Cybersecurity programs against business requirements.

INDUSTRY CERTIFICATIONS

- Certified Information Systems Security Professional **(CISSP)**
- Certified Data Privacy Solutions Engineer **(CDPSE)**
- Project Management Professional (**PMP**)
- **Six Sigma Black Belt**
- **ITIL** v3 Foundation
- Certified Information Security Manager (**CISM**)
- SEI-CMMI **ATM** (Assessment Team Member SCAMPI-B)
- Microsoft Certified Professional in 70-562 (**MCP** .NET 3.5 and Web application)
- Certified in **Industrial Control Systems Cybersecurity -** ICS-CERT, DHS

AREAS OF EXPERTISE

- PHI and PII protection
- HIPPA, Privacy
- Risk Management
- Security Audits
- Change Management
- Identity & Access Management
- Asset Management
- Machine Learning
- Penetration Testing
- Business Continuity
- Threat Hunting
- Disaster Recovery
- Application Security
- Continuous Processes Improvement
- Cyber Kill Chain
- PCI Security
- Asset Hardening
- Vulnerability Management
- Incident Management
- Digital Forensics
- Project Management
- Root Cause Analysis
- Six Sigma Methodology
- Patch Management
- Biomedical Device Cybersecurity
- Cryptography/PKI
- Information Security Governance
- Threat Modelling
- Industrial Cybersecurity
- Malware Sandboxing
- Security policies and standards
- Cybersecurity Awareness Trainings
- Critical Data Management
- Legal and eDiscovery Security

FRAMEWORKS AND CONTROLS

♦ NIST – Cybersecurity ♦ OWASP ♦ ISO 27001 ♦ PCI ♦ HIPPA ♦ SEI-CMMI ♦ COBIT

TECHNICAL SKILLS

- **Artificial Intelligence:** Machine Learning, Neural Networks, Natural Language Processing (NLP)
- **Access controls/ IdM/IAM**: NetIQ, Sailpoint
- **Cryptography:** AES, 2DES, PKI, Key Management
- **Data Loss Prevention (DLP):** Forcepoint(Websense) 8.1, McAfee
- **eDiscovery:** Relativity, Logicull, Casefleet, Office 365
- **eMail monitoring & anti-phishing:** Forcepoint(Websense) 8.1, Proofpoint, PishMe
- **Endpoint Monitoring**: Carbon Black, FireAMP, McAfee
- **Endpoint Disk Encryption**: Sophos SafeGuard, McAfee, Bitlocker
- **Endpoint Security**: McAfee, Windows Defender, Symantec
- **Endpoint Privilege Management**: CyberArk (Viewfinity) EPM
- **Encryption**: SSL/TLS, Microsoft Public Key Infrastructure (PKI)
- **Forensics tools**: FTK Imager, Paraben, Encase, Ida, FTPPro, Magnet Internet Evidence Finder, OllyDb, Encase
- **Industrial Control Systems Protocols**: MODBUS TCP/IP, DNP 3.0, OPC, KOYO, CodeSys ARTI
- **Load Balancers**: F5, Netscaler
- **Medical Devices Security**: Firewall and network segmentation of Drager Fusion Pumps, Imaging systems and more
- **Mobile Device Management (BYOD):** Airwatch, MaaS360, Openpeak Toggle, MobileIron
- **Multifactor authentication:** Duo, RSA
- **Network Sniffing tools**: Wireshark, BurpSuite, Network Miner
- **Network Security**: Palo Alto Firewalls, Juniper Firewalls, F5 Load Balancers
- **Operating System:** Windows, Linux Distros, Unix, Kali Linux, Samurai Web Testing Framework
- **Penetration Testing:** Metasploit, SQLmap, BurpSuit, Aircrack, custom scripts
- **Privilege Account Management:** familiar with CyberArk PAM
- **Privilege Access Management:** CyberArk EPM
- **Programming**: Python, .NET, C#, VB .NET, C++, C, Visual C++, JavaScript, VBScript, ML.NET and more
- **RDBMS & related**: Oracle, SQL Server, MYSQL, SSIS, SSRS and more

- **Security Information and Event Management (SIEM)**: QRadar, RSA Secure Analytics, familiar with Splunk
- **SCADA/HMI**: Indusoft Web Studio
- **SSO**: Ping Federate, Form-fill
- **Threat Intelligence feeds**: ThreatConnect, IBM Threat Intelligence, Palo Alto Wildfire
- **Virtual Platforms:** VMware, Virtual Box
- **Vulnerability Tools:** Qualys , SQLMap, NMAP, OpenVAS, Nessus, Nexpose, OWASP, IBM AppScan, HP Fortify WebInspect
- **Vendor Management platforms:** SecureLink, CyberArk
- **Web Application Firewalls**: Imperva Securesphere, F5

WORK EXPERIENCE

Assistant Professor in Cybersecurity **Angelo State University, San Angelo, TX** **Sept 2022 till date**

- Official coach and mentor for students at 2022 Hivestorm (3 students) security competition and 2023 The National Collegiate Cyber Defense Competition (NCCDC) (6 students).
- Manage the Cybersecurity Lab for research activity and pen testing.
- Training and mentoring undergraduates in below following CompTIA's Security+ certification syllabus:
  - Cybersecurity (computers and network)
  - Security Risk & Privacy
  - Network Security
  - IoT & Industrial security
  - Network Forensics
  - Vulnerability Management
  - Incident Management
  - Identity Management (IAM)
  - Cryptography (DES, 3DES, AES, RC4, etc.)
  - PKI, web certificates, and Key management
  - Unix System Administration and Shell Scripting
  - Trained students on security tools such as nmap, OpenVas, Wireshark, AirCrack, etc.
  - Engage with security vendors to present their products to students (online presentations)

Cybersecurity/Digital Forensics Researcher, Cybersecurity Principal Investigator (PI) **Sam Houston State University, Huntsville, TX** **Aug 2018 till Aug 2022**

- Conducted and managed high-impact data-driven projects in;
  - Cybersecurity around vulnerabilities of devices and applications
  - Data privacy evaluation of TikTok and FaceApp
  - Digital forensics (smartphone/data/disk/cloud)
  - Security risks
  - Vendor's security posture evaluation
  - Threat detection and profiling
  - System hardening
  - Security Vulnerabilities of streaming devices
  - eDiscovery
- Applied analytics (machine learning and neural networks) to forensically analyzing network traffic and forensic data for threats mapping/tracking, case investigation clues, timeline analysis and actor profiling.
- Helped deploy GNS3, virtual firewalls, virtual routers at the Cyber Forensics Lab.
- Managed and led projects that developed custom software to mine digital forensic evidence and case ESI using Machine learning and Neural Networks thereby reducing analysis time for investigators and paralegals.
- Worked on development of policies and standards based on DIR TX - Security Control Standards Catalog.
- Identified and reviewed existing security control gaps. Identified plans to close security gaps.
- Performed security risk assessments against SHSU policies and standards.
- Worked with global IEEE teams on development of standards for "Secure and Trusted Learning Systems" and "Big Data Governance and Metadata Management".

Information Security Operations Manager **Methodist Le Bonheur Healthcare, Memphis, TN** **Mar/2017 - June/2018**

- Responsible for managing the information security operations across the organization thereby keeping an eye on organization's digital security footprint.
- Responsible for the enterprise security program in the areas of risk management, vulnerability management, incident response, security operations, governance, compliance, and forensics.
- Key areas of responsibilities.
    1. Cybersecurity Strategy and Implementation across all facets of the security discipline
    2. Ensuring strategic alignment of Cybersecurity with business objectives
    3. Manage the Cybersecurity Operations team consisting of six FTE (network security, security analysts, incident responders and threat hunters)
    4. Manage a team of Network security resources managing enterprise firewalls, remote access and VPN
    5. Manage enterprise network security
    6. Managed operations on active security threat hunting and anomaly identification.
    7. Managed and advise on medical device security.
    8. Manage the vulnerability management Program
    9. Manage endpoint encryption process
    10. Deployed and managed SIEM with assistance of a MSSP
    11. Managed the Cybersecurity Incident Response Program overseeing cyber incidents response, containment, resolution, and forensics.
    12. Participated in key IT Security and Privacy Governance teams
    13. Managed Application Security and hardening
    14. Managed the vulnerability program and penetration testing
    15. Maintained all Cybersecurity tools and technology of the organization.
    16. Ensured Cybersecurity stays on the organizational radar.
    17. Assisted on Network Segmentation and Isolation
    18. Assisted with monitoring internal and external policy compliance.
    19. Assisted with audits of policies and controls continuously.
    20. Coordinated on new technology adoption like cloud services with an eye on minimizing risk and attack surface.
    21. Assisted with Security Risk Management, Risk Acceptance and Risk Mitigation
    22. Assisted with identifying remote access solution for vendors
    23. Worked with different departments in the organization to reduce overall security risk.
- Key accomplishments and implementations
    1. Deployed QRadar (SIEM) to monitor critical assets.
    2. Established SIEM continuous monitoring program with MSSP
    3. Redeployed vulnerability scanner across almost 100% cross-platform servers and network gear.
    4. Managed deployment of MFA/2FA against Virtual Private Network (VPN) and Enterprise Reverse proxies.
    5. Managed Local Admin Privs revocation of users and systems across enterprise.
    6. Managed deployment of CyberArk EPM to manage user's privileges on endpoints.
    7. Managed Privilege Account Management solution POC/POT
    8. Performed security gap analysis a needed
    9. Assisted with promoting security awareness, trainings and conducting internal presentations.
    10. Created security polices standards and operating procedures as applicable.
    11. Redeployed QRadar for vulnerability management.

Information Systems Security Manager **University Health System, San Antonio, TX** **Nov/2015 - Mar/2017**

- Responsible for implementing the information systems security program from ground-up across the organization.
- Responsible for the enterprise security program in the areas of risk management, vulnerability management, incident response, security operations, governance, and compliance.
- Managed a security team of 2 FTE (Security analysts, Incident responders and Threat hunters)
- Key areas of involvement, implementation, and improvement.
    1. Security Strategy and Implementation across all facets of the security discipline
    2. Ensuring strategic alignment of Security with business objectives
    3. Manage the Cyber Security Operations Center
    4. Introduce and manage the Vulnerability Management Program
    5. Manage the Cyber Security Incident Response Program
    6. Participation in key IT Governance teams

7. Tuning and tightening the server patching process
8. Implemented Risk Management, Risk Acceptance and Risk Mitigation standards
9. Defined Asset Management thereby laying foundation for identifying critical assets and data.
10. Performed security gap analysis
11. Scoping the Penetration testing exercise, vetting external pen-test vendors.
12. Promoting security awareness, trainings and conducting internal presentations.
13. Creating polices/standards, introducing controls and governance.
14. Defining critical data criteria, its handling, protection, and storage.

- Management and administration of staff responsible for security tools such as SIEM, vulnerability management/configuration management, malware detection, file integrity monitoring, multi-factor, web content filtering, and others.
- Manage a team of security professionals (Security Analysts and IAM security provisioning administrators).
- Manage operations support of endpoint disk encryption software (Sophos), Websense (email, web and DLP), Netbotz security cameras, BYOD/MDM, IAM/IDM, Malware sandboxing, RSA SA, PHI and PII discovery, device hardening.
- Oversee various Cybersecurity initiatives while working with cross-functional teams (Applications, developers, vendors, clinicians, project managers, end users, helpdesk, networking, storage, middleware and server teams)
- Research and recommend the appropriate industry standards to alleviate security threats thereby contributing to information/Cybersecurity continuous improvements and strategic planning.
- Manage the IAM Team functional tracks: User Compliance, Provisioning/De-provisioning, Privileged User Management.
- Communicate with IT leadership on security gaps, governance, risk exposure and health of IT security program.
- Conduct and communicate Cybersecurity status reviews with various stakeholders.
- Perform Security Risk Assessments against operations/program/projects.
- Designed, developed and implemented Security Risk Assessment toolkit based on NIST and HIPPA frameworks.
- Oversee security incidents to containment and closure, impact to business, complete RCAs and investigative reports.
- Monitor the organization's vulnerability-scanning program for internal and external-facing hosts.
- Oversee security newsletters publications, awareness trainings and security related stakeholder communications.
- Ensured all approved policies related to change control, security, and segregation of duties are strictly adhered to.
- Ensured adherence to privacy and security policies in accordance to HIPPA.
- Stay abreast of technology, security trends and Industry best practices by evaluating new solutions and products.
- Performed estimation, ROI, Risk assessments, change control and process improvements on security projects.
- Provide direction, constructive feedback, and technical guidance to staff. Set goals, priorities, review and evaluate work, and conduct performance reviews.
- Ensure vendor security compliance to business agreements.
- Reported and worked under the CISO of the organization.
- Proposed and established various security groups and committees focusing on key problem areas and gaps.
- Key accomplishments:
    1. Upgrade of Forcepoint Websense to 8.1
    2. Implement email processing and spam Filtering in Forcepoint (Websense) TRITON-EMAIL
    3. Evaluate and deploy a replacement BYOD/Mobile Data Management solution
    4. Configure PHI eDiscovery on Websense [Endpoints and network]
    5. SOPHOS Safeguard upgrade (end point protection via disk encryption)
    6. Finalize, Rollout and Implement Incident Response Plan (IRP tabletop exercises in progress).
    7. Rollout/Implement IAM solution (access provisioning maintaining a degree of SOD. Final phase in progress.)
    8. Upgraded DLP monitoring across 8000+ endpoints
    9. Implemented endpoint monitoring through CISCO FireAMP agents across 8000+ endpoints.
    10. Implemented email Phishing awareness and education solutions using Forcepoint (Websense) TRITON-EMAIL
    11. Implemented malware threat processing in the cloud using Forcepoint (Websense) TRITON-EMAIL
    12. Upgrade of digital forensic tools like EnCase.
    13. Security questionnaires for vendors and project managers during system acquisitions and project delivery.

Principal Consultant, Security Intelligence Analytics & Assurance **Wipro Ltd, Houston, TX, USA** **Jun/2011-Nov/2015**

- Worked as a Principal Consultant in the Enterprise Security Solutions (ESS) practice as part of the Security Intelligence Analytics Assurance (SIAA) team.
- Provided consulting services (advisory services, transformational solutions and managed security services) around end-to-end security and compliance solutions globally across industry verticals.
- Led a team of five resources based in Houston, TX.
- Led and manage Public Key Infrastructure (PKI) and Single Sign On (SSO) implementation, QRadar log archival to AWS.

- Consulted on Multi-Factor Authentication Implementation and improvement of Patch Management process driven by vulnerability assessments.
- Conducted security exercises focused on penetration tests and vulnerability assessments against websites, routers, switches, and databases with technical teams spread across Geos.
- Managed incident management and investigations at Security Operations Nodal Center, ensuring security events are investigated and remediated for 24x7 continuous operations by support team.
- Advised senior management by identifying critical security gaps and recommended risk-reduction solutions.
- Responsible for integrating processes between Identity and Access Management (IAM) systems with the client's AD.
- Interpreted information security vulnerabilities, risks, policies, and procedures to Application and infrastructure teams
- Responsible for Identifying, analyzing, conduct triage, containment, resolution, monitoring and reporting of information security incidents.
- Analyzed logs from webservers, services, databases, applications, and log data to determine security weaknesses.
- Monitored enterprise user access provisioning (LDAP and AD) processes and related jobs.
- Proactively protected the availability, integrity, confidentiality, and privacy of business data.
- Planned and implement application security by developing security solutions, directing system control development and access management, monitoring and evaluation.
- Performed Security Risk Assessments against operations/program/projects
- Conducted security code reviews.
- Participated in vendor management, SLAs and security governance.
- Participated in Disaster Recovery exercises.
- Advised technical teams in designing and implementing security solutions and technologies.
- Document and maintain security standards, guidelines, and procedures

Technical Lead / Project Manager Science Applications International Corp (SAIC), Houston, TX Sep/2003-Jun/2011

- Led and managed full development lifecycle projects of various sizes and complexities. Coordinated the timeliness and quality of work effort for the team onshore and offshore).
- Managed a team of five resources based in Houston, TX, one resource based in UK and ten resources based out of India
- Managed escalations for project related issues, challenges, or questions from project team. Played a role of Lead architect with team members at onshore and offshore. Provided technical and process guidance to the project and support team.
- Played a role of Operations Coordinator (technical) on the ADM service delivery program involving 250 applications as on portfolio. Provided 24/7 support on various applications as a SME (Subject Matter Expert).
- Worked as a technical lead on projects developing code and mentoring teams across Geos. Have programmed project modules in .NET, MVC and SharePoint technologies
- Managed systems responsible for Active Directory Account Creation, Group Memberships
- Designed, developed and deployed .NET project for change management for the Terminal Transport and Marine business.
- Implemented and managed web security certificates on webservers for various customers.
- Designed, developed and deployed a .Net project for change management for the downstream Pipeline business.
- Designed and developed .NET alternatives to legacy HR applications due for retirement in 2013 using MVC and JQuery.
- Designed and developed SSIS packages for data integration across Data centers.
- Enhanced a .NET console application that caters to the sync between enterprise AD, HR data and Exchange Mailboxes.
- Owned Root Cause Analysis and Problem Management for managed services provided to customer.
- Served as escalation point for application support and troubleshooting, provides guidance and direction in resolution of escalated issues around application or system problems.
- Served as the first line of escalation for domain technology issues that cannot be resolved by tier one and two support.
- Assisted staff developers with code maintenance, unit test and new feature development using the .NET platform
- Setup and maintain cloud-based Windows web and application servers utilizing Window Server 2008 & IIS 7.5.
- Setup and manage the application database utilizing Microsoft SQL Server 2008. This included configuring maintenance plans, database backups and data maintenance.
- Worked on RFP/Bid process for projects along with the PMs providing technical consultation around .NET technologies, MOSS(SharePoint), SQL Server (DB design, SSIS, SSRS, SSAS programming) and Oracle (DB Design and programming).
- Kept development team and management informed about applicable security issues as they relate to web applications or applicable government regulations (e.g. SOX, Microsoft coding best practices).
- Worked with applications that integrate into Customer SharePoint environment using .NET technologies. Supported applications built around asp, .NET, SQL Server and Oracle technologies for customer. Provided support for the Customer Rebill system involving Autosys jobs, DTS packages and OLAP Cubes.
- Provided primary support SAP Portal for customer

- Integrated multi-factor authentication systems into an enterprise web application.
- Worked with SSO for SAL Portals
- Worked on application defect investigations and resolution as part of service delivery services
- Worked on mainframe conversion to .NET projects for payroll processing.
- Performed code reviews as part of pair programming and training peers on secure coding practices.
- Performed code maintenance, unit test and new features development using the .NET platform.
- Led and managed full development lifecycle projects of various sizes and complexities.
- Coordinated the timeliness and quality of work effort for the team (onshore and offshore).
- Performed Incident management related to security during ongoing service delivery.
- Presented papers on ROI of application security controls and process improvements
- Participated as Assessment Team Member to evaluate SAIC-India against CMMI process maturity.
- Led ADM program transitions and transformations. Worked on RFP/Bid process for projects.
- Assisted with network setup and configuration, security scanning at SAIC-India during SAIC's India operations rollout.
- Ensured all approved policies related to change control, security, and segregation of duties are strictly adhered to.

Cybersecurity Intern **InduSoft, Invensys (Schneider Electric), Austin, TX** **May/2014-Aug/2014**

- Participated in internal training sessions to learn the products, services offered by InduSoft, as well as the Industrial Automation market where the company plays a role.
- Created documents and presentations about best practices in cyber security, based on the products and services offered by InduSoft.
- Collaborated with the QA team to identify current and future cyber security vulnerabilities in the products offered by InduSoft.
- Conducted custom presentations for technical internal teams (development, QA, technical support), describing best practices and concepts that must be applied to improve the cyber security reliability of products and services provided by the company.
- Conducted custom presentations for marketing/sales internal teams, describing advantages of the InduSoft products and services regarding cyber security, so InduSoft can properly convey the main concepts to customers.
- Conducted presentations to current and potential customers describing best practices in cyber security and demonstrating how InduSoft products and services follow such procedures.
- Elaborated a Cyber Security guideline manual and presentations for HMI/SCADA applications, focused on the products offered by InduSoft.
- Elaborated case scenarios and test procedures focused on Cyber Security reliability for the QA department.
- Improved the InduSoft's product quality assurance and testing team's awareness about good practices in cyber security and, consequently, the credibility of the company in the market.
- Reported to the VP, Consulting services on progress.

Worked as Software Programmer at various Information Technologies companies in Bangalore, India between June' 1995 to Sept' 2003 (many closed since 2002)

SEMINARS & WEBINARS – Presentation

- 7th International Symposium on Digital Forensic and Security (ISDFS 2019) conference presentation of "SCADA Testbed for Vulnerability Assessments, Penetration Testing and Incident Forensics"
- Presenter and Panelist on technology and Cybersecurity, Center for Russian, East European, and Eurasian Studies, University of Pittsburgh, on Security, Privacy and Steganographic Analysis of FaceApp and TikTok
- Webinar on SCADA and HMI Security in InduSoft Web Studio
  YOUTUBE Link: https://www.youtube.com/watch?v=kBcXCM7Y3vA
- Sam Houston State University PhD program Seminar on Security, Privacy and Steganographic Analysis of FaceApp and TikTok

EDUCATION

PhD in Cyber and Digital Forensics Sam Houston State University, USA Aug/2022
(Cyber/Computer Forensics and Counterterrorism)
Dissertation focus: *Sentiment Analysis, Financial Fraud Detection and Sexual Harassment detection of threat actors using forensic evidence*

Master's in digital Forensics Sam Houston State University, USA May/2015
(Cyber/Computer Forensics and Counterterrorism)
Academic project: *Design and deploy a fully functional HMI/SCADA lab for vulnerability testing, penetration testing and incident forensics*

Master's in Computer Applications	Bharathiar University, India	Dec/2002
Bachelor of Science (Major in Electronics)	Bangalore University, India	May/1995