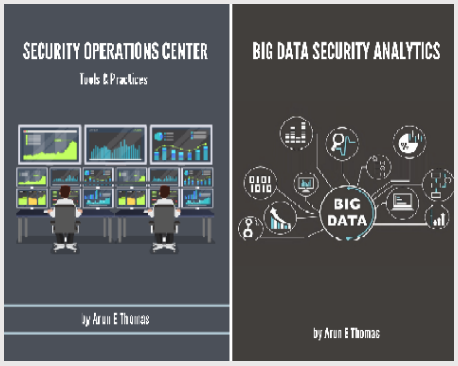
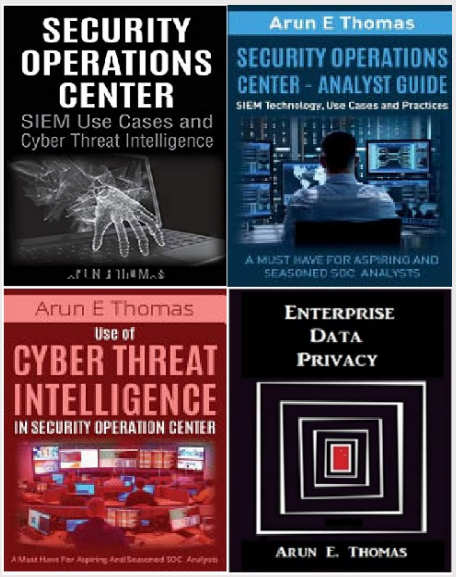
Published Books





2015-06
Enterprise Data Privacy ‣ Big Data Security Analytics
2016-06
Security Operations Center - Analyst Guide: SIEM Technology, Use Cases and Practices
2017-06
Security Operations Center - Tools & Practices
2018
Use of Cyber Threat Intelligence in Security Operations Center
2020-07
Blockchain Security for Banking, FINTECH professionals and security assessors

1.)

Arun Thomas

CTO - NetSentries Technologies , Trusted Cyber Threat Management Advisor/Researcher for leading Banks/FINSERV,Prominent Author/Speaker

A high profile Technologist with 17 plus years of experience in Core Enterprise Security, SOC, Cloud Security and IoT, IIoT and Industrial Control System Threat Analytics. An Information Security Guru, holds numerous certificates and patents in Information Security domain. Regularly receive executive special invitation to organizations and universities for seminars, workshops and guest lecturing. An active promoter of Open source security solutions for IoT, IIoT and Industrial Control Systems.

A prominent personality in the Information Security industry throughout the Middle East, APAC and EMEA. An Information Security expert, author and Inventor who has achieved remarkable success for his contributions to Threat Analytics, Threat Management, Incident Response and Advanced cyber security consulting.

Notable Highlights

- Holds four IP/Patents and bestselling Author of 6 books on Information Security Trusted Banking/Finserv Security Advisor and SME to leading Banks in MENA region
- Global SME of several large Fortune 500 organizations
- Previously in charge of designing and operating very large SOCs for large enterprises and Government Organizations ⊙ Consultant SME for several fortune 100 companies

Certifications

ISC2 – ISSAP
ISC2 - ISSEP
ISC2 - ISSMP
ISC2 - CISSP
ISC2 - SSCP
Comptia - CASP
EC Council - Licensed Penetration Tester Master: Lab
EC Council - CHFI EC Council - ECSA
EC Council - CTIA
Checkpoint - CCSA Checkpoint - CCSE CISCO - CCIE Security CISCO - CCIE-R&S CISCO - CCNP R&S CISCO - CCIP
Juniper – JNCIA
Juniper - JNCIP-SEC
Microsoft – MCSE
Cloud Security Alliance – CCSK
Qualys Guard – Vulnerability Management
Qualys Guard - Web Application Scanning
Qualys Guard - Malware Detection
Snort Certified Professional (SnortCP)
VMware – VCP
EC Council - ECSA Practical: Lab

- SGG-Global: Cybersecurity Protecting Critical Infrastructure conference (London) Advisory Board member
- Years of diverse experience in security operations, network & system security, systems engineering, research, and security management.
- Extensive experience architecting security solutions with multi-vendor IDS/IPS, Firewalls, UTM, SIM, SIEM , Virtualization Security & Fault Management & Monitoring solutions to corporations in finance, biotech, aerospace, manufacturing, Internet services, telecommunications, government, pharmaceuticals, and entertainment business sectors.
- Expertise in corporate security, with in-depth experience in Network Security solutions, project management, integrated security architectures, investigations and incident response programs, compliance, security technologies, and developing new corporate security programs.

Experience:

2016-08 - Present : Chief Technology Officer/*NetSentries Technologies, Dubai*

- Support business growth through strategic planning and process development.
- Make decisions with broad and positive impact on security management operations.
- Lead organization by developing professional and ethical culture focused on service excellence.
- Streamline company processes and procedures while enhancing customer satisfaction.
- Spearhead design and implementation of best practices in Service delivery workflow and project management
- Provide transformational support to clients by planning and implementing security interventions.
- Define targets and goals for the organization.
- Responsible for all operational and technical aspects of SOC consulting and MSSP services.
- Direct staff in the areas of Governance Risk and Compliance, Cyber Threat Management and Advanced Security Consulting services.

- Create and Centralize Technical Management and Support Organization, responsible for supporting all technical aspects for the operation of two geographically dispersed sites.
- Responsible for the Information Technology Operations Control Center, all IT Helpdesk, Security Administration and Enterprise Systems Management.
- Maintain information security processes and security control standards for application development and technology deployment.
- Head Research and Development practices translating to New Service Offering, Enhance existing Service Offering and Enhance Service Delivery

2015-08 - 2016-08-CTO/Chief Security Architect - Information Security SME

/SecuritySkool Technologies Pvt. Ltd/

- Architect & Build world class MSSP solutions for customers.
- Help organizations to build new security verticals acting as the Chief SME & Mentor
- Work with Service Design teams to drive strong security best practices
- Evaluates and recommends security technologies for use throughout the enterprise.
- Works with all architects & Security experts to drive Enterprise Architecture (EA) processes and best practices.
- Ensures that all security solutions, architecture design and analysis work is documented in a structured fashion.
- Works closely with peers in Security Operations, Security Compliance, to ensure that security reviews regarding information security technologies
- provide feasible requirements and are consistent with contracts, and regulations
- Designs in-house solutions for maintaining security posture.

- Proactively remains abreast of related evaluating technology trends and requirements, such as emerging standards for new technology opportunities
- Works with IT architects and management to stay abreast of planned and future business and technical directions as it relates to the company's evolving needs
- Works with project teams and unit level team members to ensure strong alignment with security policy, standards, and best practices.
- Protects system by defining access privileges, control structures, and resources.
- Recognizes problems by identifying abnormalities; reporting violations.
- Implements security improvements by assessing current situation;
- Determines security violations and inefficiencies by conducting periodic audits.
- Identifies user requirements by researching and analyzing user needs, preferences, objectives, and working methods, studying how users consume content, including data categorization and labeling; meeting with focus groups.
- Identifying security gaps; evaluating and implementing enhancements.
- Identify the weak points of the systems.
- Recommend ways to improve a system's security through both hardware and software

2014-06 - 2015-08 -Senior Staff Engineer - Information Security Special/Microfocus (NetIQ/Novell)

- Security Analytics Research & SIEM Product Design.
- Threat Intelligence Integration Research & Design.
- Oversee and coordinate regular activities of different SIEM development & maintenance teams & provide
- Design Suggestions & Modifications.
- Ensure the delivery of world-class SIEM plugins , solution packs & services to meet different customer requirements. Supply technical oversight to ensure capabilities and technology is being used in SIEM Product to its most effective state.
- Collaborate with key stakeholders such as Senior Management, system owners and operators to ensure effective design ideas & processes are implemented for overall quality.

- Work closely with Customers, Pre-sales & Technical Support Teams to analyze and resolve issues reported on SIEM platform and components.
- Provide Exception, C&A, and design review and approval on architecture to ensure a system of independent checks and balances are in place.
- Coordinate technical design/review activities with application development, enterprise architecture, information security, systems, network, and database groups to develop secure frameworks and enterprise applications.
- Designs the enterprise security infrastructure and architectural topology,including recommending hardware, operating system, software, and Ensure consistency and sufficient integration with existing infrastructure.
- Recommends and implements Design revisions as appropriate.
- Research ,recommend and implement changes to procedures and systems used in SIEM to enhance systems security & stability.
- Educate Employees / Partners to increase awareness of information
- security policies and best practices. Collaborates with business Management to communicate product design modification , innovations & new design ides/concepts.
- Define use cases for different SIEM plugins & help the dev team to understand the business requirements. Assists and/or provides limited direction to lower level technical personnel.
- Provide Solution Architecture Design & Mentoring on SIEM integration Project

2012-04 - 2014-06- Advanced TAC Lead Support Engineer

/Juniper Networks India Pvt Ltd/

- Handling last level Information Security & network Security related Escalation issues of Firewalls, IPS/IDS, UTM & other security Products.
- Intrusion / Incident Analysis & Review .
- Continuous Security Monitoring of critical IT resources .
- SIM, SIEM – Security Threat & Response Manager Configuration & Troubleshooting.
- Compliance Checking & Vulnerability Management through STRM.
- Network & Security Manager Configuration & Troubleshooting.
- Risk Assessment Consulting
- Junos Space , NSM & STRM Troubleshooting.
- Security Policy Review & Analysis .
- Compliance Reporting.
- Compliance Implementation – ISO 27000, PCI DSS

2007-06 - 2012-04 -Senior Information & Network Security Consultant /Covenant Network Technologies Pvt. Ltd/

- Consult on a wide variety of Information security & network security issues.
- Provide/Recommend/Engineer/Support information & network security solutions for clients.
- Provide High Level Escalation & troubleshooting support on various network security issues.
- Manage Monitoring solutions like Cisco MARS.
- Manage, Implement & Troubleshoot Log Correlation & SIM/SIEM Solutions.
- Develop & Implement Enterprise level Security Policies.
- Attack modeling & trend analysis support with SIM/SIEM solutions.
- Cisco/Checkpoint/ Open Source (Snort) IPS , IDS & IDP management ,monitoring, policy rewriting & threat correlation.
- Managing web based content filtering with Cisco IPS , Checkpoint gateways , Microsoft ISA 2006 / Microsoft TMG Forefront 2010 & Linux based Open source solutions like dansguardian.
- Manage , implement & troubleshoot Load Balancing with Cisco ACEAP/ACESM & Microsoft TMG Forefront 2010.
- AntiVirus & OS Patch management.
- Provide BCP/DRP planning support to clients.
- Provide Information Security Auditing Support to clients.
- Provide Penetration Testing & Vulnerability Assessment services to clients .
- Provide SIEM/SIM/Log Correlation consulting to clients.
- Develop and deliver both instructor-led training and virtual classroom delivery of different Information & Network Security Courses.
- Position as Team Lead/Mentor to other employees.
- Teach Information & Network security courses as well as custom developed courses throughout the world as per the requirements of clients.

- Responsible for content development of Information security topics as per the requirements of the clients.
- Chief Penetration Testing Consultant for NetSentries, Bangalore– Network & Compliance Checking Lead & mentor the Penetration Testing team in:
- OS/Network Level Vulnerabilities Identification.
- Firewall testing , Router testing , IDS/IPS testing, Database testing,
- Perimeter testing, Password cracking, Denial of Service (DOS) testing.
- Network protocol vulnerability testing.
- ISO-27001 compliant quarterly penetration testing.
- PCI-DSS Scanning including compliance templates & auto fill-in form

2006-12 - 2007-06-System Security Consultant-/Accenture Bangalore/

- Installation, configuration, monitoring and response to security system.
- Troubleshoot Network & System level security issues.

- Monitor & analyze threats real time.
- Patch Management & compliance checking of end systems.
- System file integrity checking.

2003-06 - 2006-11- Security Engineer/Confidential Company /

- Installation, configuration, monitoring and response to security system.
- Troubleshoot Network & System level security issues.
- Monitor & analyze threats real time.
- Patch Management & compliance checking of end systems.
- System file integrity checking.

Recently Published Blogs/Articles

- DNA Hack https://www.netsentries.com/blog/dna-hack/
- SOC – Cyber Threat Intelligence Analysis - https://www.netsentries.com/blog/soc-cyber-threat-intelligence-analysis/
- Mobile application penetration testing- https://www.netsentries.com/blog/mobile-application-penetration-testing/
- Role Of SOC In PCI DSS-https://www.netsentries.com/blog/role-of-soc-in-pci-dss/
- Importance of automation in SOC- https://www.netsentries.com/blog/importance-of-automation-in-soc/
- The Curious Case of Banking Frauds -Malware –Part1- https://www.netsentries.com/blog/the-curious-case-of-banking-frauds- malware-part-1\
- The Curious Case of Banking Frauds–Malware–Part 2- https://www.netsentries.com/blog/the-curious-case-of-banking-frauds-malware- part2/
- Operation DigitalTornado- https://www.netsentries.com/blog/operation- digital-tornado/
- Greedy- Greedyhttps://www.netsentries.com/blog/greedy-greedy/
- Stories of Indian banks, who lost out to EndPoint Security- https://www.netsentries.com/blog/stories-of-indian-banks-who-lost-out-to- endpoint-security/
- A Chronology of stolenMillions-https://www.netsentries.com/blog/a-chronology-of-stolen-millions/
- One cyber attack that led up to WAR- https://www.netsentries.com/blog/one- cyber-attack-that-led-up-to-war/
- DDoS Protection : When your Defense fails, Site Crashes and Business Down-https://www.netsentries.com/blog/ddos-protection-when-your-defense- fails-site-crashes-and-business-down/
- What a Hacker Can do? Anything- https://www.netsentries.com/blog/what- a-hacker-can-do-anything/

- Brilliance of the hacker or is it your Ignorance https://www.netsentries.com/blog/brilliance-of-the-hacker-or-is-it-your- ignorance/
- Security Breach, Data Intrusion and lost Fortune https://www.netsentries.com/blog/security-breach-data- intrusion-and-lost- fortune/
- From losing 150 million to Shutdown- https://www.netsentries.com/blog/from-losing-150-million-to-shutdown/
- When one email costs you millions- https://www.netsentries.com/blog/when- one-email-costs-you-millions/
- Human – The weakest link- https://www.netsentries.com/blog/human-the- weakest-link/
- When you don't need bombs to blow up a safe any more- https://www.netsentries.com/blog/when-you-dont-need-bombs-to-blow-up-a- safe-any-more/
- Immobilizing Critical Financial Services- https://www.netsentries.com/blog/immobilizing-critical-financial-services/
- Spear Phishing: Amateurs Hack Systems, Professional Hack PEOPLE- https://www.netsentries.com/blog/spear-phishing-amateurs-hack-systems- professional-hack-people/
- Nasty Financial Data Breaches- https://www.netsentries.com/blog/nasty- financial-data-breaches/
- Dark Web Market Places and Stolen Cards- https://www.netsentries.com/blog/dark-web-market-places-and-stolen-cards/
- Disrupting Banking Service Availability- https://www.netsentries.com/blog/disrupting-banking-service-availability/
- Human Exploitation in Cybersecurity- https://www.netsentries.com/blog/human-exploitation-in-cybersecurity/
- The Spotted ATM Skimming-https://www.netsentries.com/blog/the-spotted- atm-skimming/
- Cyber Attack, Looted millions & Bankruptcy- https://www.netsentries.com/blog/cyber-attack-looted-millions-bankruptcy/
- Faded Anti-Malware-https://www.netsentries.com/blog/faded-anti-malware/
- Significance of Secure data Storage- https://www.netsentries.com/blog/significance-of-secure-data-storage/
- Outdated security and Lost Millions- https://www.netsentries.com/blog/outdated-security-and-lost-millions/
- Caution: Malware may be leaching on your Money- https://www.netsentries.com/blog/caution-malware-may-be-leaching-on-your- money/
- 3 million User's data, 10 Iranian banks and One True Hacker- https://www.netsentries.com/blog/3-million-users-data-10-iranian-banks-and-one-true-hacker/
- Guard Against - Card Skimming- https://www.netsentries.com/blog/guard against-card-skimming/

- ATM Jackpotting – The sophisticated crime of the Millennium- https://www.netsentries.com/blog/atm-jackpotting-the-sophisticated-crime-of- the-millennium/
- ATM Security - Black box attacks- https://www.netsentries.com/blog/atm- security-black-box-attacks/
- ATM Security – When Shimming Attacks happen- https://www.netsentries.com/blog/atm-security-when-shimming-attacks- happen/
- SWIFT- The Way the World moves Value. Part 3- https://www.netsentries.com/blog/swift-the-way-the-world-moves-value-part-3/
- SWIFT- The Way the World moves Value. Part 2- https://www.netsentries.com/blog/swift-the-way-the-world-moves-value-part-2/
- SWIFT- The Way the World moves Value. Part 1- https://www.netsentries.com/blog/swift-the-way-the-world-moves-value-part-1/-How Cyber Thieves are Caughthttps://www.netsentries.com/blog/how-cyber-thieves-are-caught/
- Know and Safeguard: Digital Banking – Part1- https://www.netsentries.com/blog/know-and-safeguard-digital-banking-part-1/
- Logical and Physical attacks on ATM Machines- https://www.netsentries.com/blog/logical-and-physical-attacks-on-atm- machines/
- Hold your Card Against Card Trapping- https://www.netsentries.com/blog/hold-your-card-against-card-trapping/
- ATM Shoulder Surfing - Watch Your Back- https://www.netsentries.com/blog/atm-shoulder-surfing-watch-your-back/
- Transaction Reversal Fraud (TRF) – Don't be the next Target- https://www.netsentries.com/blog/transaction-reversal-fraud-trf-dont-be-the- next-target/
- ATM Cash-Out: The Biggest Threat We Ignore- https://www.netsentries.com/blog/atm-cash-out-the-biggest-threat-we-ignore/
- Beware of ATM Cash Trapping- https://www.netsentries.com/blog/beware-of-atm-cash-trapping/
- Significance of Cyber Security in Account analysis of banking and Financial institutions –https://www.netsentries.com/blog/significance-of-cyber- security-in-account-analysis-of-banking-and-financial-institutions/
- Open Banking System : Implementation and risks- https://www.netsentries.com/blog/open-banking-system-implementation-and-risks/
- Open Banking Technology and PSD2: What You Need to Know as A Banking Security Expert?-https://www.netsentries.com/blog/open-banking- technology-and-psd2-what-you-need-to-know-as-a-banking-security-expert/
- Robotic Process Automation (RPA): Risks and Controls- https://www.netsentries.com/blog/robotic-process-automation-rpa-risks-and-controls/
- RPA – The obscure guardian of Cyber Security System- https://www.netsentries.com/blog/rpa-the-obscure-guardian-of-cyber-security-system/

- A Spotlight on Robotics Security Attacks- https://www.netsentries.com/blog/a-spotlight-on-robotics-security-attacks/
- Business Benefits of RPA(Robotic Process Automation)- https://www.netsentries.com/blog/business-benefits-of-rparobotic-process-automation/
- Why and How - Robotic process automation(RPA)- https://www.netsentries.com/blog/why-and-how-robotic-process-automation- rpa/

- Know and Safeguard: Digital Banking - Part 2- https://www.netsentries.com/blog/know-and-safeguard-digital-banking-part-2/
- Circumstances wherein Audio Calls Need to Be Tagged and Protected- https://www.netsentries.com/blog/circumstances-wherein-audio-calls-need-to-be-tagged-and-protected/
- Cybersecurity in Data Processing of FINSERV- https://www.netsentries.com/blog/cybersecurity-in-data-processing-of-finserv/
- Secure File Transfer Service is not as Secure- https://www.netsentries.com/blog/secure-file-transfer-service-is-not-as-secure/
- Cybercrime: Types and Implications for Financial Institutions- https://www.netsentries.com/blog/cybercrime-types-and-implications-for-financial-institutions/
- The Cybercrime Culture and Types of Scams- https://www.netsentries.com/blog/the-cybercrime-culture-and-types-of-scams/
- The Nature of Cybercrime and Scams- https://www.netsentries.com/blog/the-nature-of-cybercrime-and-scams/
- Techniques and Tricks Used in Scams - https://www.netsentries.com/blog/the-nature-of-cybercrime-and-scams/