Dr. Stuart Makowski, WEC-SG (PO)

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

Chief Scientist

- Exceptionally accomplished cyber warfare professional with **over 28 years** of progressive experience.
- Architected, managed, and administered enterprise environment that had **2,600,000 global users**.
- Designed and wrote the strategic roadmap for clients whose annual sales were over **$15,000,000,000**.
- Supervised up to **174 personnel worldwide**.
- Managed budgets up to **$87,000,000**.
- Implemented cost-saving strategies to achieve budget goals in public and private enterprises.
- Performed all levels of incident response and cyber intelligence; Subject matter expert cyber warfare.
- Hands-on incident response, computer forensics, network and application security.
- Master at identifying and clarifying cyber security and technology risks and coordinating remediation efforts.
- Established security policies, procedures, practice, and methodology.
- Advised National Command Authority, Special Executive Service, and classified federal agencies on cybersecurity, cyberwarfare, and cyberspace defense and offense operations.
- Designed numerous vendor credit card systems in compliance with Payment Card Industry (PCI) regulations.
- Revised and integrated military policies into national antiterrorism program covering multiple defense agencies, including Raven Rock Mountain Complex and over 100 other facilities.
- Led project development with new clients, conducting economic analysis, establishing objectives, and developing project budget.
- Provided antiterrorism support to the Department of Defense, Agencies, Field Activities, Raven Rock Mountain Complex and Pentagon Facilities.
- Architected, engineered, maintained, and administered: intrusion detection/prevention systems (IDS/IPS), security information event management solutions (SIEM), data loss prevention (DLP), malware analysis, wireless application firewall (WAF), firewalls, automated/manual threat forensics, dynamic threat protection, and packet analysis tools.
- Extensive experience with ISO9000, ISO9001, ISO17799, ISO27001, ISO27002, ISO27002:2005, HIPAA, HITECH, SOX, PCI-DSS, FISMA, CJCSI, FIPS, NIST,PKI, SSLDC, DIACAP, COSO, COBIT, RA,VA, INFOSEC, OPSEC, C&A, FAM, FAH, DITSCAP, NFPA, NIACAP, SAS70 (I & II), SSAE16, DIACAP, RMF, Fast Track ATO, Continuous ATO, POA&M, ERP, DCID 6/3, NISPOM, OMB A-130, SST&E, SSA, SSP, ITIL, DoD 8510.01 (RMF), DoDI 8500 series (Information Assurance/Cybersecurity), CNSSI 1253, DoDI 2000.12, 2000.16 Vol. 1 & 2, DoDD 3020.40 Mission Assurance NCI 10-222, DoD 3020.26, Emergency Programs, Interagency Security Committee (ISC) Security Guidance, National Capital Region (NCR) Force Protection Plan, and DoD Mission Assurance Benchmarks with ISC Standards, and DAA/IATO.

FULFILLED ROLES

- ★ Chief Scientist | United States Space Force – Office of Chief Operations Officer
- ★ Cyber Warfare / Cyber Security Subject Matter Expert | United States Space Force – Chief of Space Operations
- ★ Senior Distinguished Member Technical Staff 1 – Fellow | General Dynamics Mission Systems
- ★ Chief Cyber Warfare Fellow | Cyber Security Service Provider – Missile Defense Agency
- ★ Cyber Terrorism and Communication Subject Matter Expert | Office of Secretary of Defense
- ★ Security Operations Center Subject Matter Expert | Federal Agency
- ★ Information Assurance Manager | United States Army Corps of Engineers
- ★ ArcSight Global Capability Leader | Hewlett Packard Enterprise
- ★ Executive Security Consultant | Children's Hospital Los Angeles
- ★ ArcSight Architect | Defense Information Systems Agency
- ★ Security Architect| United States Courts
- ★ Global Information Security Director | MGM Resorts
- ★ Senior Cyber Security Engineer | Department of Energy

Dr. Stuart Makowski, WEC-SG (PO)

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

EDUCATION

Doctor of Science in Information Security Management – Charter University June 2004
Master of Science in Computer Information Systems Management – Charter University December 1998
Bachelor of Science in Computer Information Systems Management – Charter University December 1995

CERTIFICATIONS (NON-INCLUSIVE)

Project Management Professional (PMP)
Antiterrorism Officer 1 (ATO-1)
ArcSight Certified Security Analyst (ACSA)
ArcSight ESM Administrator (ACEA)
Certified Information Systems Auditor (CISA)
Certified Information Security Manager (CISM)
CompTIA Network+
CompTIA Project+
CompTIA Security+
CompTIA Server+
Certified Information Systems Security Professional (CISSP)
Certified Novell Administrator (CNA)
Citrix Certified Administrator (CCA)
Cisco Certified Network Administrator (CCNA)
CompTIA Advanced Security Practitioner (CASP)
CompTIA I-Net+
Hewlett-Packard Technician (**17 Different Certifications**)
Microsoft Certified Professional (MCP)
Microsoft Certified Professional + Internet (MCP+I)
Microsoft Certified Systems Engineer + Internet NT (MCSE+I)
Microsoft Certified Systems Engineer 2000 (MCSE)
Palantir Foundry 101 – Navigation
Palantir Foundry 102 – Data Analytics
Palantir Foundry 103 – Reports
Palantir Foundry 104 – Data Lineage
Palantir Foundry 105 – Code Workbook
Palantir Foundry 106 – Data Preparation
Palantir Foundry 107 – Code Repositories
Palantir Foundry 201 – Advanced Contour F
Palantir Foundry 202 – Advanced Code Workbooks – Analytic
Palantir Foundry 203 – Advanced Code Workbooks – Foundry Machine Language
Splunk Core Certified User
Splunk Core Certified Power User
Splunk Enterprise Certified Administrator

SECURITY CLEARANCES

Department of Defense - Top Secret Sensitive Compartmented Information
Department of Defense - Top Secret Restricted Data - Critical Nuclear Weapon Design Information
North Atlantic Treaty Organization (NATO) - COSMIC Top Secret

PROFESSIONAL ASSOCIATIONS

World Electronic Consortium – Security Group
Department of Defense / Intelligence Community Cyber Roundtable
Huntsville (AL) Cyber Roundtable

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

PROFESSIONAL EXPERIENCE

Ten Zero Consulting August 1995 – Present
Chief Scientist

- Responsible for Data Engineering, Foundry Data Pipeline Creation, Foundry Analysis Reporting, Slate Application development, re-usable code development management and integrating Internal or External System with Palantir Foundry for data ingestion with high quality.
- Worked closely with United States Space Force Space Operation Command, Space and Missile System Center, Space Command, Space Force Deltas, National Military Command Center Cyber operators and other stakeholders to coordinate Foundry engineering and developing requirements.
- Solid understanding on Foundry Platform landscape and it's capabilities.
- Evaluated and validated new Foundry platform features and align with the architecture team to realize / enable tech spikes on the foundry platform.
- Developed custom Foundry Apps on Palantir Platform.
- Designed and implemented integration with Internal, External Systems, and AWS platform using Foundry Data Connector or Magritte Agent.
- Provide level 4 internal technical support for the overall foundry platform and provide support/advice to product and services teams when required.
- Collaborated with data scientists, data analyst and technology teams to document and leverage their understanding of the Foundry integration with different data sources - Actively participate in agile work practices.
- Decades of vast experience with data management, data ingestion, and data transformation in big data analytic platforms.
- Experienced in cleansing and analyzing complex data, and generating actionable insights to drive and implement change.
- Redesigned timeseries pipeline architecture to better handle the increasing scale of data (TB to PB), coordinating with teams within the United States Space Force to ensure data usage workflows and constraints were considered.
- Developed a suite of tooling to manage dynamic pipeline creation, ensured a simple maintenance story despite an increased number of parallel pipelines, and contributed to fleshing out similar use-cases across the United States Space Force.
- A firm grasp on data analysis using R, pandas, matplotlib, sklearn, Python and other stats packages.
- Provided technical, operational, acquisition-related, and support advisory and assistance services support to both United States Space Force Office of the Chief of Space Operations (USSF/OCSO) and Headquarters United States Air Force, Directorate of Space Operations (HAF/A3S).
- Provided the United States Space Force/S6 Cyber 2-letter organization with direct support related to Cyber Operations, Cybersecurity and Space Communications.
- Represented and advocated United States Space Force interests and collaborate with other units to achieve synchronization and unity of effort.
- Coordinated with and provided direct support to Department of the Air Force staff in planning, coordinating, and executing assigned actions.
- Provided status and awareness to Headquarters Air Force staff of strategic and operational issues affecting the United States Space Force missions.
- Supported United States Space Force key leaders, staff, and component/sub-unit activities in the National Capital Region and engagements with key mission partners.

- Served as the United States Space Force focal point for international treaties and agreements related to military space cooperation, in cooperation with Headquarters Air Force staff.
- Provided expertise to United States Space Force/S6 to conduct and cyber-related support analyses and assessments.
- Provided cybersecurity Risk Management Framework research, analysis, and recommendations to assess and accredit emerging cybersecurity capabilities and methodologies to include assessing controls, monitoring and reporting on controls and on the status of mitigation actions.
- Documented, coordinated, advised, assisted, reviewed, and inspected required cybersecurity assessments, processes, and artifacts.
- Conducted cybersecurity analysis of system certification and accreditation plans to ensure systems are properly certified and accredited according to current Cybersecurity Policy available within the Division.
- Assessed information security related products and documents and interpret Department of Defense, Air Force issuances.
- Coordinated with other United States Space Force entities in order to complete cybersecurity risk assessments.
- Provided cybersecurity services, E/APL Certification and Technical Assessments, Technology Investigation and AoAs for Space and DoD/US intelligence information systems, and applications.
- Performed analysis services for United States Space Force/S6 expertise, to include planning the objectives and requirements for the test event; assisting the customer to prepare required documentation by providing review and feedback; preparing the test environment; executing the test activities and reporting results.
- Developed methods for validating cybersecurity requirements, determining vulnerabilities, developing cybersecurity tools and methods and conducting AoAs.
- Coordinated engineering analysis-level support to program management offices (PMOs) and System Program Offices (SPOs) throughout the Systems Engineering Lifecycle Process to ensure successful certification and authorization technology transition.
- Assessed the cybersecurity process with the objective of identifying gaps and recommending improvements for cybersecurity package submissions and for the content and structure of required artifacts that will reflect and comply with the latest cybersecurity policies and guidelines.
- Conducted research and investigation into concepts and techniques that enhanced processes to ensure flexibility to anticipate and accommodate changes in cybersecurity policy and directives.
- Conducted reviews of current security analysis tools and provide analysis for decision consideration of incorporation to improve the process.
- Chief scientist for a Defensive Cyber Operations (DCO) Integrator supporting a classified federal agency.
- Applied advanced principles of engineering and management to solve problems involving the development of complex technologies.
- Oversaw and managed design and development processes as they related to the engineering of products utilizing principles and technology of physics, mathematics, engineering, and related physical sciences.
- Utilized technology to optimize all phases of work to include requirements management, modeling and simulation, risk analysis and formal trade study tools.
- Conducted research to identify leading or designing edge and breakaway technologies.
- Researched and reported important shifts in technological landscape and implications to the enterprise.
- Actively exposed high-level risks and communicated the risk trade space and mitigation strategies.
- Collaborated with management across the enterprise on research and development relevant to long-term objectives.
- Anticipated needs and concerns of the technical community and brought about resolutions.
- Used influence within technical and intelligence community to mitigate issues including the authoring of trade studies and position papers.
- Influenced the development of technical opportunities leading to new business.
- Took immediate and decisive action in dealing with technical, performance, and threatening issues.
- Directed development of technical strategies and teaming strategies across divisions.

- Resolved issues with new Tanium application servers provided for the new Tanium implementation.
- Managed Tanium modules Index, Connect and Patch.
- Edited Sensors for Linux, MacOS and Windows within the Tanium Platform.
- Created pre-requisite system check and functional testing for Tanium.
- Managed Tanium software utilization with Tanium Product Team and clients requiring reports from Tanium.
- Provided Tanium support for the new AWS cloud solution implementation.
- Managed network Tanium usage issues with various teams.
- Created saved question using Interact, creating action groups, computer groups when necessary, scheduling actions and deploying packages for the upgrade process for Tanium.
- Managed issue resolution with Tanium Application Vendor and DoD Tanium management team.
- Performed Tanium binary upgrades and coordinates with the various teams for outages.
- Worked with Tanium Application Vendor on possible enhancements to improve function and user experience.
- Configured Tanium reports for Cyber Risk and exports to the UDL (NSA Unified Data Library) and Warp Core (Palantir Foundry).
- Worked Tanium tickets within ServiceNow and resolving issues in a timely fashion
- Resolved issues involving Tanium clients installed on all Windows and Unix servers
- Managed Threat Response - Recorder, Index, Engine(Detect) and Incident Response, Using Tanium Interact to build questions and managed endpoints, analyze their answers and deploy actions to endpoints.
- Executed Threat Response Migration and Upgrade for Tanium.
- Managed Tanium APP server, Module Server and Trace Zone Server.
- Created Threat Response Profiles, exclusions, filters and Intel. Upgrading Threat Response to latest versions with hot fixes for Tanium.
- Managed Tanium Index exclusion tags.
- Performed Trace Module Upgrading Tanium Trace Module and documenting the process for knowledge transfer in both the workstation and server environments.
- Created Trends Boards for monitoring Trace Upgrade progress.
- Investigated problems and troubleshoot Trace Module issues for Live Trace Session Connectivity, create snapshots and upload evidence from endpoints for Investigations.
- Investigated failed package deployments using the Tanium sensors in the Tanium Console.
- Built Tanium Client package for standalone endpoint deployment in Linux MacOS and Windows using VMWare to build virtual Test Systems for Tanium Core Platform testing, managing systems, Linux, Windows at the NIPR, SIPR, and JWCIS level.
- Lead large proposals with identification of cross business unit strengths and technical shortcomings.
- Provided proposal teaming recommendations to shore up any shortcomings for optimum win probabilities.
- Drove the development of business opportunities that lead to new Line of Business or Division creation.
- Exceptional leadership skills.
- Defined key mission critical business application solution portfolios including the clients SAP ecosystem (ECC6, BW, BO, Enterprise Portal, CRM, SRM, PI and GRC) and its accompanying sub-systems (incl. JDA Supply Chain, Hybris E-Commerce, Recipe management and Dispensing systems).
- Recognized internally and externally as an expert in my field.
- Microsoft ERP Dynamics AX System Architect/Administrator with demonstrated expertise in installation, configuration, administration and Production Servers maintenance of Microsoft ERP Dynamics AX 2012 R3/R2/2009 and MS SQL Server 2014/2012/08/05/2000 Active/Passive Cluster/dispersed, Always-On and Oracle 11g/10g/9i.
- Lead solution planning and design efforts for enterprise-scale, complex Microsoft 365 opportunities.
- Played the critical role in solution design, configuration, process engineering and roll out of our AX ERP implementations.

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

- Dynamics NAV implementations experience.
- Exceptional ability to apply or develop highly advanced technologies, principles, theories and concepts.
- Demonstrated ability to communicate issues, impacts, and corrective actions.
- Exceptional ability to easily and effectively communicate technical topics to a diverse audience.
- Demonstrated ability to clearly report relevant information.
- Exceptional ability to understand and apply project leadership principles including SPI/CPI, Earned Value, Cost Account Management (CAM), and Statistical Process Controls for large complex programs.
- Demonstrated ability to anticipate technology, process, and skill needs.
- Demonstrated proactive leadership and has name recognition throughout both the enterprise and customer organizations.
- Ensured the solution portfolios were managed by a combination of internal teams and external managed services providers.
- Created an environment in which impact of technology on the business was clearly recognized.
- Responsible to Plan, direct and oversee full life cycle Implementation of Microsoft ERP Dynamics AX 2012 R3/R2/2009 and Database Infrastructure design and management Operation, leading projects, cost saving and meeting goals.
- Implementation and administration of Microsoft ERP Dynamics AX Axapta 2012 R3/R2/2009/4.0 on SQL Server, AOS Cluster/Load balancing, Enterprise portal EP load balancing reporting extensions and analysis Service extension, Setting up AIF, DMF and workflows.
- Designed and developed solutions for external customer's enterprise-wide cyber systems and networks.
- Designed, architected, engineered, installed, and administered ArcSight Enterprise Security Manager (ESM), Event Broker, ArcMC, Logger, Investigate, User Behavior Analysis (UBA), and Data Lake integration that had 300,000 events per second (EPS) and yearly data storage was 20 petabytes (PB).
- Ensured system security needs were established and maintained for operations development, security requirements definition, security risk assessment, systems analysis, systems design, security test and evaluation, certification and accreditation, systems hardening, vulnerability testing and scanning, incident response, disaster recover, and business continuity planning.
- Developed road maps describing the evolution of all enterprise solution portfolios from current state to future state.
- Provided analytical support for security policy development and analysis.
- Successfully designed and Implementation of Microsoft Dynamics AX 2009/2012 R3/R2 ERP system on Microsoft SQL 2012/2008 Cluster environment with Always-On.
- Dynamics AX AOS/Enterprise portal load balancing, administration and performance and optimization.
- Designed and integrated new architectural analysis of cybersecurity features and related existing system to future needs and trends.
- Embedded advanced forensic tools and techniques for attack reconstruction.
- Provided engineering recommendations and resolved integrations and testing issues.
- Interfaced with external entities including law enforcement, intelligence and other government organizations and agencies.
- Network expert responsible for providing thought leadership and subject matter expertise around a wide range of cybersecurity technologies.
- Experience securing multi public cloud environments.
- Defined and advocated the principles of application integration, and the use of middleware tools and standards.
- Excellent understanding/working knowledge of the public cloud infrastructure and services in Amazon Web Service (AWS), Oracle Cloud Infrastructure (OCI), Microsoft Azure: (IAM, VPC, KMS, CloudWatch, Systems Manager, S3, RDS, Route53, Lambda, AWS Config, Azure PaaS, Azure IaaS, Azure Saas, Azure networking, Azure Security Center, etc.)
- Expertise in Dynamics AX administration and Performance troubleshooting.

- Solid ability to actively assess existing cloud implementations, identifying security issues/ prioritizing fixes and delegating to junior technical resources appropriately.
- Oversaw the design, development of messaging type interfaces between applications, and oversaw the operational management of data flows between integrated applications.
- Vastly experienced working within an environment using DevOps and CI/CD.
- Designed and implemented Microsoft SQL 2014/2012 4 NODEs with Always-On and Multi node cluster/multiple instances on Microsoft Windows 2012/2008 R2 enterprise.
- Designed and implemented Enterprise SharePoint environment for Dynamics AX enterprise portal, SSRS reporting services extension and SSAS analysis services integration extension.
- Engineered and implemented public/private cloud security tools and techniques to ensure the ongoing security and compliance of all public/private cloud implementations.
- Direct experience with engineering, deploying, managing and supporting various security solutions including firewalls, IDS/IPS solutions, endpoint security, authentication systems, log management, content filtering, vulnerability scanning tools, etc.
- Protracted experience designing secure networks, systems and application architectures.
- Established identity management solutions and processes to facilitate secure access to business applications and information.
- Strong understanding with web related technologies such as web applications, web services, and service-oriented architectures along with network/web related protocols.
- Performed Dynamics AX Security Development and customization.
- Deployed and configured AIF/DMF.
- Demonstrated personal initiative in maintaining a continuous high level of professional knowledge in areas of security and risk management.
- Oversaw the establishment of an Information Security function within the clients Business Services that will develop and maintain enterprise security and risk policies.
- Provided extensive technical knowledge and analysis of exceptionally complex problems that needed extensive knowledge of the subject matter for effective development and implementation of cybersecurity solutions.
- Developed, tested and deployed Legacy Data migration to Dynamics AX using Data migration framework and Data loading; Setting up Workflows.
- Architected database capacity planning for ERP databases Dynamics AX, SharePoint, Siebel Analytics and BizTalk Servers.
- Prepared alerts and warnings for executive management and military chain of command, wrote classified and unclassified technical white papers, and implemented measures per approved solutions.
- Interpreted higher headquarters' guidance in the development/maintenance of policies and procedures, while evaluating new and existing security technologies; developed, reviewed and updated cyberspace defense and incident management procedures, Operating Instructions, internal processes, and other agency CERT/CSSP documentation.
- Created, managed and continuously improved a catalogue of SAP offerings.
- Provided technical security engineering leadership to classified and unclassified projects and Risk Management Framework (RMF) teams.
- Responsible for ensuring the reliable performance of ERP systems, monitor server performance, AX SQL Tracing and finding bottleneck, setting up Performance counter for Dynamics AX and SQL Servers.
- Responsible for providing technical security engineering for projects involving software/hardware/network systems.
- Ensured projects containing new software were directed to the Software Assurance (SwA) team to perform commercial off the shelf (COTs) or code reviews required to receive approval for placement on the agencies approved software list and network infrastructure.
- Infrastructure design with a focus on implementing technologies that are STIG compliant.

- Developed, with customers, Industry Engagement Managers and Application Engagement Managers the overall roadmap.
- Implemented cybersecurity standards and how they affect implementation of new tools like cloud technology.
- Documentation development focused on Engineering Review Board technical briefings and Risk Management Framework (RMF) accreditation requirements.
- Conducted Defensive Cyberspace Operations (DCO) support activities on Air Force Space Control Network (AFSCN) mission system, Geosynchronous Space Situational Awareness Program (GSSAP) mission system or Military Satellite Communications (MILSATCOM) mission systems.
- Responsible to work with improvements, by participation in the development of the architectural principles, processes and standards.
- Performed all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction.
- Performed monitoring operations; reported cyber security events and anomalies; provided analysis and recommendations, Vulnerability Management (VM) and Malware Protection / Vulnerability Assessment and Analysis (VAA), Intrusion Analysis and Correlation Information, incident handling, mission operations transfer, exercise and assessment support.
- Worked with domain and technical architects to develop detailed solution-specific application, data and infrastructure designs.
- Continuous learner with a passion for innovation in cyber risk management to drive bottom-line business contributions (optimize security investments, avoid losses from security incidents, improve customer retention, enhance business decision-making, and reduce corporate liability).
- Evaluated and made recommendations for Department of Defense facilities within the National Capital Region (NCR) on achievable means of enhancing the communications networks and/or systems to ensure local distribution networks and supporting off-site commercial facilities had the capacity, survivability, reliability, and security to support the mission.
- Managed employees/contractors, direct/indirect at varying levels of the Project Management job family.
- Conducted technical vulnerability assessments of computer networks, telecommunications (plain old telephone systems, voice over IP, and secure telephone equipment), industrial control systems, land mobile radio, microwave, satellite, wireless, and other communication systems.
- Directly supported the mission assurance and defense critical infrastructure programs of the Pentagon, Raven Rock Mountain Complex (RRMC) and over 100 facilities.
- Supported the antiterrorism force protection division of a federal agency through robust risk-based antiterrorism assessments in communications/network infrastructure and cybersecurity operations using established Department of Defense, Defense Information Systems Agency, Joint Service Provider, National Security Agency, and Defense Threat Reduction Agency benchmarks.
- Supported the antiterrorism force protection division of a federal agency through robust risk-based antiterrorism assessments in communications/network infrastructure and cybersecurity operations using established Department of Defense, Defense Information Systems Agency, Joint Service Provider, National Security Agency, and Defense Threat Reduction Agency benchmarks.
- Provided antiterrorism planning and programming staff support to the five Department of Defense Agencies, Field Activities, Raven Rock Mountain Complex and Pentagon Facilities Antiterrorism Officers to ensure compliance with Department of Defense / United States Northern Command mandates, and to improve the effectiveness of their antiterrorism programs.
- Provided proactive support, through effective capacity planning and change management.
- Revised and integrated Department of Defense and United States Northern Command policies into the federal agency's antiterrorism program and plans for execution by the federal agency and the five Department of Defense Agencies, Field Activities, Raven Rock Mountain Complex and over 100 other facilities.

- Provided customer reach back support in order to improve Department of Defense Agencies and Field Activities for force protection and meet overall antiterrorism and force protection strategic goals.
- Assessed and performed systems utilization and headroom reports to assist in troubleshooting and performance tuning.
- Ensured the antiterrorism plans addressed the execution and expectation risk management processes (threat, criticality, vulnerability, risk assessment, force protection condition and terrorist incident response measures) for operational and supporting forces.
- Ensured the antiterrorism plan programs mandated threat and force protection working groups were facilitated for the stakeholder's tactical control to the federal agency for force protection, and in turn, the federal agency attended working groups facilitated by Joint Forces Headquarters – National Capital Region and United States Northern Command.
- Performed quality control of the developed/new solutions, development of improvement suggestions.
- Ensured the federal agency had a robust education and awareness program to provide antiterrorism training to the Department of Defense National Capital Region Community and timely dissemination of indication and warning messages.
- Reviewed communication plans, defense continuity plans, and other associated plans to provide feedback to improve the policies, procedures, and benchmarks.
- Evaluated and made recommendations on secure and non-secure high-speed digital data transmission, government satellite services, high-frequency radio, long-haul military and commercial radio, telephone, voice frequency circuitry, wireless, facsimile, video, and computer network inter-switch trunks.
- Provided day-to-day technical/professional assistance for projects and programs delivered beyond the completion date.
- Performed single-point critical node analysis of a facility's telecommunications, other communications systems, computer networks including supporting infrastructure (power, ventilation, fuel, fire protection, etc.)
- Provided recommendations to reduce or mitigate system vulnerabilities due to terrorist, manmade, or natural incidents.
- Prepared code documentation in support of program development.
- Created and maintained system specification and sub-system specification documentation.
- Worked with SAP Roadmap for S/4 and other new technologies like HANA and Dynamic Tiering to create strategy/direction.
- Built SAP applications using SAP development tools and frameworks.
- Identified threats or hazards that could impact the mission's communications architecture and use that data to assess the vulnerability and risk to those assets.
- Prepared, classified and unclassified, assessment team reports based upon vulnerabilities observed during assessments.
- Conducted other assessment areas defined by the subject matter expert benchmark matrix.
- Provided technical advice to the Post Balance Survivability Assessment / Joint Mission Assurance Subject Matter Expert.
- Assessed
    - Life cycle management of information systems
    - Cable management and labeling of information systems connections
    - Physical security of information systems
    - Any vulnerabilities in communication infrastructure and routing
    - Resiliency of servers, routers, switches, and power supplies
    - Maintenance, software patches, and serviceability of information systems
    - Department of Defense, Defense Information Systems Agency, and Joint Service Provider Information Assurance practices

- Recruited, developed, motivated, and retained diverse staff structuring them into teams that delivered results and savings.
- Responsible for developing and maintaining the overall service delivered by a Managed Security Service Provider.
- Worked with regional capability leads to ensure consistency of the overall global offering of a managed security service.
- Worked with software engineer, PMs and operations teams to manage the solution delivery.
- SAP/CRM customizing – maintaining business transactions, status profiles, and date profiles.
- Responsible for maintaining and ensuring standard solutions are implemented and delivered according to global portfolio direction.
- Proven record of department profitability and cost savings realized within various business enterprise settings.
- End to end planning and implementation of various network devices and business applications.
- International enterprise expertise in auditing, cyber security, business continuity, disaster recovery, and planning.
- Performed economic analysis, planned, programmed, and budgeted for information systems resource requirements.
- Developed strategic plans, policies, service levels, key performance indicators, metrics, and operating procedures.
- Oversaw incident response planning as well as the investigation of security breaches, and assist with disciplinary and legal matters associated with such breaches.
- Provide technical leadership to the enterprise for the cyber security program.
- Mentor and train others in cyber security in addition to training for other technical groups.
- Created enterprise security standards and guidelines.
- Managed process and acted in the lead role for the computer incident response team or computer emergency response team.
- Perform and create procedures for system security audits, penetration-tests, and vulnerability assessments.
- Established a Risk Management Framework (RMF) program that implements the role of Authorizing Official and Security Control Assessor.
- Strong SAP solution architecture skills in data and analytics.
- Seasoned understanding of SAP/CRM development environment, SAP transport system and general software development lifecycle.
- Strong ETL experience.
- Experienced working on opportunity management module of SAP/CRM that includes opportunities, activities, and RFCs.
- Maintained responsibility for the development of project goals and objectives, working closely with clients, developing an implementation plan, documenting and testing new processes and tools, and creating quality assurance checklists and methods for collecting quality metrics.
- Performed extensive research and analysis of the existing DIACAP-based command processes and leveraged a thorough comprehension of DoD cybersecurity policy drivers and chains of command as it relates to performing C&A.
- Initiate RMF processes and oversaw DODI 8510.01 (RMF) activities for assigned information systems to transition from DIACAP to RMF.
- Responsible for architecture, engineering, administration, deployment, maintenance, design, and documentation, of following information security tools in enterprise network:
    - Tenable ACAS scanner
    - Algosec firewall policy management
    - FireEye: CMS, MAS, HX, NX, EX
    - Cisco Sourcefire Firepower
    - Imperva WAF
    - WebSense / Forcepoint
    - Blue Coat Security Analytics Solera

  - McAfee NSM
  - Proteus / IPAM / Bluecat DNS address manager
  - Cisco Security Manager
  - IGMON
  - Forescout NAC
  - TACACS+ ACS server
- ArcSight Global Capability Leader for Hewlett Packard Enterprise and the development of versions 6.11.0 and 7.0.0 of ArcSight.
- Expert level understanding of Qradar implementation and its Integration with other network devices and applications and the troubleshooting work.
- Expert understanding to develop the complex use cases, Universal device support Modules on the QRadar SIEM.
- Expert level knowledge on creating the uDSM parser for the logs normalization in the SIEM tool.
- Utilized QRADAR for internal and external IDS, in addition to Cisco IPS.
- Instrumental in architecting, implementing and administrating a Security and Information Event Management (SIEM) solution to automate the correlation of I-Series, Windows and network devices.
- Defined and implemented standard recruiting strategies and a career management program
- Performed database tuning, configuration changes, sizing, and troubleshooting.
- Developed integration capabilities with 3rd party systems including network management and trouble ticketing applications.
- Install and maintain security infrastructure, including IPS, IDS, log management, and security assessment systems.
- Designed and setup the Splunk architecture.
- Configuring Indexers, Forwarders (Universal and Heavy), Search Heads, Deployment/Management Servers.
- Created dashboards according to the business needs using Advance XML.
- Wrote Splunk queries.
- Created applications on Splunk to analyze the Big Data.
- Development of Splunk queries to generate the Report.
- Dashboard creation in Splunk, running SPL queries.
- Developed various metrics in Splunk.
- Importing the data in Splunk through inputs.conf, props.conf and transforms.conf.
- Created Data Leakage Prevention (DLP) Reports through Splunk.
- Developed Splunk applications.
- Assessed threats, risks, and vulnerabilities from emerging security issues.
- Published security updates newsletter for technical groups.
- Developed scripts to maintain and backup key security systems.
- Configured solutions to match up with compliance.
- Expert ability to translate business requirements into solutions.
- Worked closely with Certification and Accreditation, Counter Intelligence, and Information Assurance Team.
- Coordinated and conducted security event collection, using a log management tool, initiated event management, enhanced compliance automation, and leveraged identity monitoring activities using the ArcSight platform.
- ArcSight subject matter expert.
- Used ArcSight ESM in daily operational work and managed the workflow of events to the appropriate business unit or corporate group.
- Identified cyber threats associated with vulnerabilities and risks via analysis.
- Extensive experience in:
  - Responding to targeted threat events
  - Writing custom parsers for NetWitness or other network forensic tools

  - Information security, incident response, investigation, and penetration testing
  - Computer forensics (host and network-based)
  - Performing open-source research to identify emerging threats
- Advised executive and senior leadership on monitoring and reporting best practices and then developed use cases on how to use ArcSight to achieve end state requirements.
- Provided technical architectural services for ArcSight ESM, logger, and connectors.
- Provided custom development of connectors (agents) using the ArcSight flex connector.
- Architected, engineered, administered HP ArcSight user behavior analytics v1.0, v1.1, and v5.0.
- Customized security content including filter/rule/report creation, signature categorization, and vulnerability mapping.
- Architected a distributed multi-manager architecture and deployment.
- Collaborated with personnel on troubleshooting and configuring networking devices, various platforms, and databases.
- Responsible for upgrades and patches for all components of cyber security systems.
- Developed content for a complex and growing ArcSight infrastructure, including use cases for dashboards, active channels, reports, rules, filters, trends, and active lists.
- Applied configuration management disciplines to maintain hardware/software revisions, content, security patches, hardening, and documentation.
- Architected the establishment, enhancement, and continual improvement of an integrated set of correlation rules, alerts, searches, reports, and responses.
- Coordinated and conducted event collection, log management, event management, compliance automation, and identity monitoring activities.
- Responded to day-to-day security requests relating to security operations.
- Tuned ArcSight performance and event data quality to maximize ArcSight system efficiency.
- Detected and analyzed cyber threat activity for the identification of advanced persistent threats and malware in real-time.
- Proactively researched emerging cyber threats.
- Applied expert understanding of hacker methodologies and tactics, system vulnerabilities and key indicators of attacks and exploits.
- Directly communicated to team members and executive leadership both quantifiable and qualifiable cyber risk to the enterprise and vendor partners through operational briefings and threat intelligence reports.
- Investigated and analyzed events related to cyber incidents.
- Planned, directed, and facilitated response and recovery activities, based on a mature understanding of data sources, in response to a cyber-threat incident.
- Provided optimization of data flow using aggregation, filters, etc.
- Developed custom flex connector as required to meet use case objectives.
- Life-cycle management of the ArcSight platforms too including coordination and planning of upgrades, new deployments, and maintaining current operational data flows.
- Applied configuration management disciplines to maintain hardware/software revisions, ArcSight content, security patches, hardening, and documentation.
- Provided guidance to security analyst and network engineering staff.
- Managed the establishment, enhancement, and continual improvement of an integrated set of correlation rules, alerts, searches, reports, and responses.
- Performed systems hardening to meet Department of Defense, Department of Energy, National Security Agency, Joint Service Provider, Defense Information Systems Agency, and National Institute of Standards minimum guidelines.
- Provided optimization of data flow using aggregation, filters, etc.

- Developed custom flex connector as required to meet use case objectives.
- Architected and managed the operation of ArcSight security information and event management systems to include ArcSight ESM, Oracle, connector appliances, smart connectors, logger appliances, Windows and Linux servers, network devices, and backups.
- Architected all aspects of security information and event management initiatives.
- Engineered the establishment, enhancement, and continual improvement of an integrated set of correlation rules, alerts, searches, reports, and responses.
- Coordinated and conducted event collection, log management, event management, compliance automation, and identity monitoring activities.
- Responded to day-to-day security requests relating to ArcSight operations.
- Tuned ArcSight performance and event data quality to maximized ArcSight system efficiency.
- Installed, upgraded, and backed-up connector appliances, logger appliances, and smart connectors
- Developed filters, rules and customized reports for ArcSight loggers.
- Architected, implemented, engineered, and administered log management, event management, and security monitoring.
- Defined and developed the processes required for command RMF security authorization package processing.
- Performed Information Assurance (IA) engineering and architecture, security testing, and Certification & Accreditation (C&A) for an unaccredited enclave environment to go live with Authority to Operate (ATO) accreditation.
- Provided architecture and all levels of support during all phases of systems engineering, software development, testing, deployment, and maintenance.
- Support included IA requirements definition/analysis, security engineering, security architecture development, security design, integration support, DIACAP documentation development, security testing, data base management systems, security infrastructure applications/tools/services, Multi-Level Security (MLS) systems, Cross Domain Solutions (CDS), Service Oriented Architecture (SOA) security, intelligence community security configuration guides (e.g., DISA STIGs/checklists, CIS benchmarks, etc.), automated security testing utilities/tools (e.g., DISA GoldDisk and SRR scripts, NESSUS, Retina etc.), DoDI 8500.2 IA controls, NIST Special Publications (800- series), and network devices.
- Responsible for areas such as identifying INFOSEC requirements, defining security aspects of system architectures, determining testing requirements and methodologies, and conducting analytical risk management activities related to the development of information systems.
- Performed engineering services that included but were not limited to the following: engineering studies and analyses; technology planning; systems architecture development; requirements development; concept development; systems design; system development and integration; test and evaluation; systems operation; control of systems and components; integrated logistics support; modeling and simulation; configuration management; Demilitarized Zones (DMZs); operating systems (Microsoft, Linux, Unix);security test and evaluation; security certification testing; independent verification and validation; penetration testing; auditing; ethical hacking; information assurance control testing and validation; information system security policy; information protection needs elicitation; technologies and applications relating to web services, service oriented architecture, intrusion detection/prevention, anti-virus, and firewalls; and systems acquisition and life-cycle management in compliance with current industry and government practices.
- Analytical support included research and development of cyber warfare concepts and strategies, particularly within the national security framework.
- Coordinated related intelligence community and DOD DISA federal department and agency IA planning activities and identification of policy, technical, and programmatic issues crossing organizational, functional, and program boundaries.

- Managed and participated in software, systems, and security engineering activities, such as: small and large scale systems and security engineering and development efforts; technology lab development for system and security application prototyping; architecture and infrastructure analysis; INFOSEC requirements definitions; technology evaluation and assessment; e-commerce, public key infrastructure (PKI) design and deployment; multi-level security technologies; intrusion detection and analysis; simulation and modeling; development of IA concepts and strategic implementation planning for Intel community CIO Office and DOD DISA organizations; web site and content design and development and integration of DIACAP IA policy and guidance system to serve as centralized and authoritative source of IA policy, legislation, directive; perform and conduct system-level designs, reviews, and risk management assessments; develop certification and test and evaluation, technical reports, and project plans; perform systems integration and monitoring of the implementation of processes, hardware and software solutions, and technical writing.
- Ensured credit card systems were built and operated in compliance with cyber security policies and Payment Card Industry (PCI) regulations.
- Outlined the information security controls, testing, and evaluation requirements for the Systems Security Development Life Cycle. (SSLDC).
- Provided Information Assurance activities in accordance with current DOD policies, National Institute of Standards and Technology (NIST), industry best practices and Defense Information Systems Agency (DISA) guidance.
- Ensured all pertinent information was obtained to allow the identification, categorization, incident handling and triage actions to occur in a time-sensitive environment.
- Analyzed network traffic and various log data and open-source information to determine the threat against the network, recommend appropriate countermeasures, and assess the damage.
- Acted as the point of contact for accepting, collecting, sorting, ordering, and passing on incoming information for the reported cyber events.
- Facilitated and expedited tracking, handling, and reporting of all security events and computer incidents in accordance with organizational procedures.
- Evaluated threats, vulnerabilities, and risk while supporting real-time security monitoring operations.
- Built, implemented and deployed data security solutions including IDS/IPS sensors and management consoles.
- Strong experience configuring and deploying Web Application Firewalls (Imperva).
- Installed, configured, maintained, audited, upgraded, updated security products (non-inclusive): proxy servers (BluecoatSG 300-9000), Infoblox, vulnerability scanners, and application scanners.
- Architected, designed, and deployed Data Loss Prevention (DLP) infrastructure.
- Performed operational support and maintenance of DLP infrastructure, including deployment, analysis, tuning, configuration, security administration and upgrading.
- Created and modified DLP detection policies and policy elements (response rules, directory groups, etc.)
- Monitored DLP infrastructure for health checks, connectivity, and availability.
- Architected, installed, configured, and maintained, the following McAfee products: Enterprise Policy Orchestrator (EPO), Virus Scan Enterprise, Data Loss Prevention (DLP), McAfee Agent, McAfee Endpoint Security (ENS), and Host Intrusion Protection (HIPS).
- Administered system policies, repairs, and deployments and maintain agents on EPO to support applications/tools not limited: EPO, Host Data Loss Prevention (HDLP), Endpoint Security (ENS), Virus Scan Enterprise, McAfee Agent, and Host Intrusion Protection (HIPS).
- Developed solutions for desktop support, server support teams, and supported business groups in the installation and maintenance of applications and servers concerning EPO.
- Recommended preventive, mitigating, and compensating controls to ensure the appropriate level of protection and adherence to the goals of the overall information security strategy.
- Developed access-controls, separation of duties, and roles.
- Conducted technical risk evaluation of hardware, software, and installed systems and networks.

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

- Tested installed systems to ensure protection strategies were properly implemented and working as intended.
- Lead incident response and recommend corrective actions.
- Communicated with personnel about potential threats.
- Lead forensic recovery and analysis.
- Maintained security of voice and data networks and equipment.
- Monitored and maintained physical and logical security and access to systems.
- Responsible for support of existing security policies and procedures, as well as creation and implementation of new security procedures.
- Performed risk assessment of partners and 3rd parties.
- Achievements include completing TruSecure enterprise certification, and development of incident handling procedures.
- Implemented global Public Key Infrastructure (PKI); Rolled out 100,000+ client certificates and 10,000+ server certificates.
- Brought about radical improvements in Key Management (KMS) reliability set up operations support group, metrics, and implementation plans.
- Responsible for product management, consultation, strategy, and standards.
- Established Certificate Practice Statement and Certificate Policy.
- Owned SSL Server OnSite certificate strategy and contract renewal.
- Integration Test Lab product owner for encrypted/signed email, Adobe digital signatures, etc.
- Expert in the system and application Certification & Accreditation (C&A) process including development of the System Testing and Evaluation (ST&E) plan, System Security Plan (SSP), Configuration management (CM), System Security Authorization Agreement (SSAA), Disaster Recovery Plan (DRP), Business Continuity Plan (BCP), Risk Assessment (RA), identification of the Major Application Metric under the general support systems, and mitigation procedures using the Plans of Action and Milestones (POA&M).

Dr. Stuart Makowski, WEC-SG (PO)

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

Client list (non-inclusive):

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

Dr. Stuart Makowski, WEC-SG (PO)

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

Dr. Stuart Makowski, WEC-SG (PO)

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

Technical Skills and Tools (non-inclusive):

3Com
ACAS
Active Directory
Acunentix WVS
AdAware
Aelita
AirCrack
AirDefense Enterprise
AirKismet
AirSnort
AIX
Algosec
Alien Vault
Angry IP Scanner
Ansible
Apache
Apithief
AppDetectivePro
AppScan
ArcSight
ArcSight ADP
ArcSight ESM
ArcSight Investigate
ArcSight Logger
ArcSight Network Configuration Manager (NCM)
Argus
ARPWatch
Arudius
AS/400
Audit
AWS
Azure
BAAN
Backtrack
Barracuda
BASE
BCP
BeEF
BIG-IP
Bluecat
Bluecoat
Breaking Point
BrightMail
Brutus
BSD
Budgeting
Burpsuite
Business Continuity
C&A
Cain and Able
Canvas
Cassandra
Cat 8/7/6/5/4/3
CentOS
Certificates
Check point
Check Point Software Technologies UTM-1
Check Point UTM-1
Chef
Cheops
Cheops-ng
Cisco
Cisco ASA
Cisco NAC Appliance
Cisco Security Manager
Cisco Systems VPN
Cisco Wireless Security Suite
Cisco Works
Citrix
Citrix Access Gateway
Citrix Password Manager
Client Server
Clusters
COBIT
Code Repositories
Code Workbook
COGNOS
Contour
CORE Impact
COSO
CouchBase
Crackert 11g
Crystal Reports
CyberArk
Dameware
Data Connection
Data Lineage
Data Loss Prevention
DB2
Dcfldd
DCID 6/3
Debian
De-Ice
DHCP
DIACAP
Digital Forensics Tool Testing
Disaster Recovery
DITSCAP
DLP
DNS
DNS address manager
DR
DSniff
Dumb terminals
Dynamix AX
Dynamix GP
EDI
E-Discovery
Entrust
ePO
ESX
Etherape
Ettercap
Event Broker
Exchange
F5
FAH
FAM
FDDI
Fedora
Fiber Optic
Fierce Domain Scanner
Findevil
FIPS

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

FireEye
Firepower
Firewalk
Firewall
FireWall-1
FISMA
Flex Connector
Forcepoint
Forescout NAC
Foundry
Foundry_ML
Foundstone
Fping
Fport
Fragroute
Fusion
Gauntlet
GFI LanGuard
GIS
GLBA
GroupWise
GuardianEdge Data Protection Platform
Hadoop Distributed File System (HDFS)
HBase
HBase
Helix
HIDS
HIPAA
HIPS
HITECH
HP Openview
Hping2
HP-UX
Identity Protection Authentication Service
IdentityGuard
IDS
Igmon
IIS
IKE
IKE-Scam
Imperva
Infrared scanners
Intermec printers
Internet Key Exchange
IPAM
IPS
IronMail
ISACA
ISECOM
iSeries
ISS
ITGA
JD Edwards
John the Ripper
Juniper Networks IDP
Juniper Unified Access Control
Kafka
Kali Linux
Kismet
Knoppix
L0PhtCrack
Lieberman
Linux
Linux Disk Editor
MAC OS X
Maltego
Management
MapReduce
Matplotlib
McAfee
McAfee Endpoint Encryption
McAfee Enterprise Firewall
McAfee NSM
McAfee Total Protection for Data
McAfee Vulnerability Manager
McAfee Web Gateway
MetaSploit
Microsoft Base Analyzer
Mu-4000 Security Analyzer
Multiplexers
MySQL
NAS
NBTScan
NBX
NDS
Nemises
Nessus
NetCat
NetIQ
NetScaler
NetStumbler
Netwib
Network Assessment
Network Security Toolkit
Netwox
Ngrep
NIACAP
Nikto
Nipper
NISPOM
NIST
Nokia
NoSQL
Novell
NST
N-Stealth
Nstrings
NTOP
Numpy
Object Explorer
ODBC
Office
Oinkmaster
OMB A-130
OpenBSD
Oracle
OS/2 Warp
OSSTMM
P0f
Palantir
Pandas
Paros Proxy
PBX
PCI
PCI-DSS
PEcarve

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

Penetration test
Penguin Sleuth Kit
PE-scrambler
Pestat
PGP
Pitbull OS
PIX
PKI
PMI
POA&M
PointSec Mobile, Media Encyrption, Full Disk Encryption
PPTP
Project
Proteus
Proventia Network Multi-Function Security (MFS)
Public Key Infrastructure
Publisher
Puppet
Pwdump
Qradar
QualysGuard
QualysGuard Vulnerability Management
Quiver
RA
RACF
RainbowCrack
Raptor
r-arrow
Ratinal AppScan
r-base
Red Hat
RedSeal
Remedy
Reports
Retina
RFID
Riak
Risk Management Framework
RKHunter
RMF
RootKit Hunter
Router
RSA
RSA Access Manager
RSA envision
SA Series SSL VPN Appliances
SAINT
Salt Stack
SamuraiWTF
SAN
Sanctuary
SAP
SARA
SAS70
Scanrand
Scapy
SCCM
SCE
SCO
SCOM
Seaborn
Security Analytics
Security assessment
Security Information & Event Management
Servers
Sguil
Shavlik NetChk Compliance
Short haul modems
Sidewinder
SIEM
Slackpack
Slate
Slickpack
Smart Connector
Smart terminals
Smoothwall
SMS
Snort
Snow Leopard
Socat
Solaris
SolarWinds
Solera
SonicWALL Distributed Wireless Solution
Sophos Email Security and Data Protection
Sophos Endpoint Security and Control
SourceFire
Sourcefire IPS
SOX
Spark
Spark
SPIKE Proxy
Splunk
Splunk Enterprise
SQL
SSAA
SSL VPN
SSP
ST&E
Storm
Sun Microsystems Identity Manager
SuperScan
Switches
Switches
Symantec
Symantec Control Compliance Suite
Symantec Data Loss Prevention (Vontu)
Symantec Mobile Security Suite for Windows Mobile
Symantec Network Access Control
Symantec Security Information Manager
Sysinternals
TACACS+ ACS server
Tanium
TCPDump
TCPtrsceroute
Tcpxtract
THC-Amap
THC-CUPASS

M: (833) TEN-ZERO
DrTenZero@TenZeroConsulting.com

THC-Dialup login hacker
THC-Flood Connect
THC-Fuzzy Finger Printer
THC-getVIP
THC-grenzgaenger
THC-HappyBrowser
THC-Hydra
THC-IPF
THC-IPv6 Attack Toolkit
THC-Keyfinder
THC-Leapcracker
THC-LoginHacker
THC-ManipulateData
THC-Orakel
THC-Orakel
THC-Parasite
THC-PBXHacker
THC-pptp-bruter
THC-PrintDates
THC-Probe
THC-rut
THC-RWWWShell
THC-Scan
THC-Shagg
THC-Snooze
THC-UnixHacking Tools
THC-vlogger
THC-Vmap
THC-WarDrive
The Coroner's Toolkit (TCT)
Thin Clients
TippingPoint IPS
Tivoli Access Manager
Tivoli Identity Manager
TOCNET
Top Secret
Tor
TradeStation
Trend Micro InterScan Web Security Appliance
Trinux
Tripwire Enterprise
UBA
Ubuntu
Unicornscanner
Unix
UPXfail
Verisign
Virtual Network Security Analyzer (VNSA) 1.0
Visio
VLAN
VMware
Vontu
VPN
WAF
Wavemon
Web Application Firewall
WebInspect
WebScarab
Websense Data Security Suite
Websense Email Security
Websense Web Security
Whisker
WikID
Wikto
Windows 10
Windows 2008
Windows 2012
Windows 2016
Windows NT
WinHEX
Wireless
WireShark
Workstations
WSUS
Xprobe2
X-scan
Yersinia
Yet Another Resource Negotiator (YARN)
z/OS
Zenmap
ZooKeeper