**Omar Chaaban**

**Union City, CA 94587**

**[Chaabano@yahoo.com](mailto:Chaabano@yahoo.com)**

**Please visit my publications page at:** [**https://www.linkedin.com/in/ochaaban**](https://www.linkedin.com/in/ochaaban)

I have published 13 articles which can be accessed in LinkedIn –Look for my most popular publication that has 1240 hits “Ethical Hacking & how to penetrate your network like hackers do Part I”

*I am interested* ***in Permanent position with the right opportunity*** *- Relocation would be acceptable for certain areas across the US or international*

**Summary:**

**Most Expertise SME** in Identify deficiencies and provide recommendation for solutions against the most powerful global cyber-attacks .**I have successful records of detecting the most serious cyber intrusions** such as **zero-day-attack and spy base exploit tool kits hidden in ADS (Alternate data stream) since 2012**, in addition to internal threats. My logo is **“Aware & Protect”** where I could develop PowerPoint presentation for technical and non-technical audiences called CSIR Metrics & Executive reporting.

I have developed and written 16 pages white paper called “**Security Controls, new mitigation for cyber intrusions”** which Provides a recommendation from minimum to maximum security controls for information systems categorized in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems .**This documentation is derived from multiple sources, cases study and personal events handled by me at many organizations I have worked for such as the NSA, DoD, DHS, The US Treasury and private companies.**

**Conclusion** based on numerous studies I have collected that the 16 pages white paper for security controls & cyber security is that if organizations have implemented them, **it will reduce the cyber intrusions by % 85.** Following common and uncommon procedures listed in the white papers **will reduce cyber intrusions by another % 14.**

* **IT SEC Subject Matter Expert SME-** acted as a liaison between various Infrastructure teams and the

management for both Lab and non-Lab biopharmaceutical environment in testing and evaluating new security related technology products. In addition, analyze current security deficiencies and provide solutions. Develop PowerPoint presentation to show the deficiencies and solution proofs as best practice following cases study by SANs organization, NIST, Department of Homeland Security, National cyber security database center, United kingdom and Australia cyber security prevention.

* **Security Controls**- Architect and implementation of Administrative, Logical and Physical controls.
* **CSIR**- Cyber Security incident Response Follow standard incident response phases includes ,Preparing for review, identify the event, contain, eradicate, recover, lessons learned.
* **Overseen DLP Integration Project**: I was the lead in overseeing testing and implementation of McAfee DLP
* **New approach for risk assessment to respond to the global cyber hacking**. The NSA-Nation-Exploit Stolen Tools which were released for free download in the Dark Web is an evidence to how dangerous these exploit tools are, two major global cyber-attacks for the last two months had attacked more than 150 countries. Developing new CSIR Cyber Security Incident Response to minimize such threats which most likely continue as cyber organized hackers keep changing and manipulating these exploit tools to escape detection by firewalls, IDS and IPS.
* **Cloud Security**- Experienced with cloud security especially while working for the US government and private large organization that use FedRamp framework, the latest Compliance NIST 800-171 among others.
* **Coaching IT teams to help in securing the infrastructure**- Providing routine and emergency technical security briefings to the Infrastructure, application, Desktop support, R&D research and development, managers, directors teams about current and expected cyber-attacks based on intelligence I collect from reports I generate from many applications such as PAN (Palo Alto Networks), Cisco Networks, Mimecast for email reports, Orchestrator such as McAfee for DLP ,antivirus and running scripts in Splunk for the top 10 OWAP such as injections, Botnet, command and control, cross-site scripting, brute-force attacks, remote code execution, TLS evasion, SMB (Server message block) and others.
* **Cyber security intelligence**, collect data throughout the globe about the latest cyber security intrusions, vulnerabilities including traveling to the countries where these intrusions are being launched from such as China, Russia, Ukraine and many other countries. In addition of collecting intelligence from the **DARK WEB** for cyber hackers trends and monitor stolen digital certificates auctions. Provide solutions to the Cyber Threats
* **Using ITIL model**, completed two years planning and execution IT security global operations and infrastructure hardening to an estimated 100 medium to large companies owned by AIG groups. Administered and improved global remote access to more than 163 countries.
* **Applied innovative**, outside-the-box thinking to protect 1.8 million highly sensitive files, executing immediate remediation for access control to protect organization assets. Laid down newly developed files, groups and folders security .
* **Couching** various infrastructure teams in security hardening and best practice.
* **Risk, compliance & Governance** following The US Government mandate act FISMA, NIST 800-53, NIST 800-171, PCI-DSS, HIPAA, and international standards.
* **Design and documentation for projects**: using SmartSheet application to document project timeline implementation with attachments of maps and other proofs of work done. Using power point presentation to provide visualise design for non-technical audience.
* **Last Audit Approver-** Audited an estimated 30,000 new servers **(both Windows and \Unix Linux OS)** and 20,000 existing servers at AIG using audit applications and automation.
* **Implemented security policy** and access control to folders and files. Security information and event management (SIEM).
* **Experience with major security frameworks (e.g. FedRAMP, ISO 27001 series, SSAE 16, PCI DSS, HIPAA, NIST 800-53, NIST 800-171, International standards, etc.)**
* **Penetration testing**. Ethical hacking by attacking the network from the inside and outside. Remediation would be applied upon discovery of vulnerabilities and policy would be updated based on the new testing results.

**Technical skills**

* Cyber security intelligence research which includes Intelligence gathering and prevention.
* Servers security –Windows & Linux server scans
* NIST 800- 53
* NIST 800-171 (Access Control, Identification & Authentication, Media Protection Physical Protection, System & Communications Protection, System & Information Integrity)
* CSIR Metrics (Cyber Security Incident Response Metrics Executive Report)
* SalePoint Identity Management. (Not Application installation)
* PAN Palo Alto Firewalls
* Microsoft SCOM infrastructure
* Threat, incident, compliance and risk management/ legacy policy and regulatory change management
* Threat Intelligence- Monitor Trends hackers activities and digital certificates auction in the Dark Web
* Virtualization Hyper-V & VMware
* **Dell Secure Works**- Logs that are generated by Palo Alto networks firewalls get analysed by Dell Secure Works, they raise incidents, I analyse and validate the incidents in Splunk if they are applicable to the infrastructure and send them to various groups to be remediated. **Example of type of attacks that raise incidents:** DDoS attacks, remote code execution, TLS evasion , SSL attack, brute force attack, cross site scripting, code injections, web site attacks, wildfire malware, application layer attack, backdoor and botnet, most dangerous but rare zero-day-attacks, ransomware, etc.
* cyber security network EMC RSA envision archer governance, risk and compliance
* Qualysguard Vulnerability Scan
* last server audit approval Windows and Linus OS
* blade logic compliance & patching
* Security information and event management (SIEM). Check point, MacAfee Orchestrator, Splunk Intelligence, & ManageEngine SIEM Tools
* Splunk Infrastructure administration and log analysis
* McAfee Orchestrator

**Professional Experience:**

**Global IT Threats Research with colleagues at Stanford University – Palo Alto, Ca March 2012- Present**

**Pharmacyclics an Abbvie company at Sunnyvale, CA…………………………………Feb 2017-June 2017**

**Senior IT Security Engineer- Subject Matter Expert**

* Lead and SME Sr. security engineer in both operations and projects overseeing all related securities operations and projects throughout the Infrastructure Lab and non-Lab machines.
* Worked with AbbVie large security team to follow the parent company policies and apply similar security practices.
* Analysing & remediation for 3rd party risk assessment and penetration testing reports an estimated 600 pages to direct the IT company’s team to apply remediation for critical and high as priority and followed by medium and low if I determined they apply to the infrastructure. I was the liaison engineer between the management and the IT teams such as the infrastructure, the networks, desktops, applications, R&D research and development, the Webs teams, and Labs management.
* Overview the IT Security operations making sure escalated incidents have been remediated in timely matter. Run routine scripts in Splunk for OWAP top ten exploits and double check if the SOC team has remediated exploits.
* I designed and completed Cyber Security Incident Response Metrics report following **Abbvie CSIR report**. The Metrics helps the company understand the overall company’s security posture, incidents intakes vs response time. Major findings, conclusion and recommendations with supporting graphs.
* **Risk ,compliance & Governance** Team lead for implementation of the following The US Government mandate act FISMA, NIST 800-53, NIST 800-171, PCI-DSS, HIPAA, and international standards. (e.g. FedRAMP, ISO 27001, SSAE 16, PCI DSS, HIPAA, NIST 800-53, NIST 800-171 etc.)
* I also was involved in collecting intelligence through Splunk advanced enterprise intelligence, the trends from the CSIR report, the type & methods of cyber-attacks cyber hackers are using.
* **Involved in immediate** remediation of the NSA exploit tools remediation by making sure firewalls can block the latest exploits while security patching was underway.

**Philips Andover, Massachusetts & Netherland Advanced Security Analytics Engineer 05/2016-07/2016 short contract**

I was a Member of MIT team researchers performing and developing Advanced Security Analytics for Philips in Amsterdam, Netherlands and North America in Andover ,Massachusetts.

Conducted application penetration testing of business applications which majority of them were integrated to hospitals.  
Compliance HIPPA, NIST 800-53, CIS, PCI and International Standards.

Performed functional testing of security solutions like RSA two factor authentication, Novel single sign on, DLP and SIEM. Proficient in understanding application level vulnerabilities like XSS, SQL Injection, CSRF authentication bypass, cryptographic attacks, authentication flaws etc.

Skilled using Burp Suite, NMAP, Qualysguard, Nessus, and many open source penetration testing applications.

**San Francisco Bay Area offsite cyber security short project Jun 2016 – Dec 2016**

**Pacific Networks – San Francisco & Hercules, CA**

**Act as a subject matter expert** on identifying early signs of intrusions to the cyber security and incident responders.

* Sub-Contractor to many medium to large clients- IT Infrastructure and Security assessment, vulnerability scans, subject matter expert in hardening the security of the infrastructure, provide penetration testing both white and black box exploits, exploit validation, proof and present how to fix the exploits.
* Write and present documentation for educating privilege access engineers and end users on how to protect their machines from today’s sophisticated exploits and cyber intrusions.

**The Pentagon and Enhance Cyber Security (Live Hacks Testing to nine Pentagon sites) Feb 2016 to May 2016 -Remote Work performed at different States from Texas to Virginia**

* The Pentagon Cyberwar fare testing’s simulation to enhance my expertise in the field of ethical hacking, cyber security and how organization could protect them currently and against next generation exploits.
* In April 2016, The Pentagon had sent me an invitation to hack their systems. I accepted the invitation and followed the pentagon guidelines.
* I started the testing in April and completed it in May 2016. I ran penetration testing against the pentagon major sites such as the DoD sites, Military sites, Archives sites, The Pentagon media sites, the health sites, and database sites and many other sites.
* List of some of the work, what I have done in IT Security and Performing penetration testing, Reconnaissance, Enumeration, scanning, cross site scripting XSS, remote code execution, path traversal, redirect/forward attack, failure to restrict URL access, cross-site request forgery, buffer overflow. Certain testing attacks were not allowed such as performing SQL Injection, LDAP injection, other injections, social media.

**American international group global services AIG –Fort Worth, Texas 01/2014 - 12/2015**

**Senior global IT security operations, Incident Response & Reports, compliance, risk and cyber security Solution Architect**

* Lead in Facilitating command center global IT security and remote access operations, spanning five continents, 162 countries, and 1,128 locations.
* Defined and utilized the integration principles of security (authentication / authorization), orchestration, and choreography. My role was with 40% architectural design, 30% Tech Leadership, and 30% Lead IT SEC operation and investigation.
* Risk and compliance following The US Government mandate such as FISMA, NIST, PCI-DSS, HIPAA, and international standards.
* Output Audit Details from logs and polices in web services execution. Worked on rotation duty as system support in the weekend.
* Drive seamless function be overseeing multiple responsibilities simultaneously, including compliance, threat, incident, and risk management; compliance intelligence; and enterprise governance, risk, and compliance.
* Support most AIG domains including DMZ domains.( estimated 300 domains)
* Security information and event management (SIEM) are being used 24x7 to protect AIG more than 300 domains, the investments and treasury.
* Last Audit Approver- Audited an estimated 30,000 new servers (both Windows and \Unix Linux OS) and 20,000 existing servers using audit applications and automation.
* Some of these applications were Qualys, Nessus, BladeLogic, Foundstone and RSA Envision, Archer. Splunk Intelligence, ManageEngine SIEM.
* Performed vulnerability scans and reporting to an estimated 50,000 servers Globally. Open emergency incident upon discovery of exploits for immediate remediation.
* Optimize workflows by delivering feedback and recommendations regarding applications improvement.
* Swiftly provide third-level support to address challenging issues regarding global remote access; solve complex problems, directing assisting the executive support team.

privilege accesses and are strictly monitored through MS SCOM, envision, solar winds, MacAfee and many other application tools.

**Us department of homeland security (Short Term project due to funding) 08/2013 - 11/2013**

**Federal networks and security integration, cyber security -Dallas, Texas & Virginia**

* Effectively supported The US Department of Homeland Security’s Cyber Security Infrastructure and related processes.
* Facilitated multiple data centers in Virginia, Dallas, and other cloud-hosted locations. Symantec, SIEM, MacAfee solid core firewall. Forensics. Security information and event management (SIEM). Penetration testing identifies and prioritizes security risks in all DHS (department of homeland security data centers. Monitor the whole infrastructure, computers, servers, routers, switches and other important devices using SIEM tools).
* Risk and compliance following The US Government mandate such as FISMA, NIST, PCI-DSS, HIPAA, and international standards.
* Some of these tools used were Nessus, RSA envision, FoundStone which include logging in to SQL server to pull out reports for analysis.
* Audits Approver for new servers (both Windows and \Unix Linux OS) and existing servers using audit applications and automation.

**XO Communications Senior infrastructure engineer- SCOM 2012 design & developer (Part time while working with the DHS) 07/2013 – 09/2013 Dallas, Texas**

* Xo communications provides network services and cloud hosting for small and medium sized companies, enterprises, national and us government accounts.
* Infrastructure senior IT engineer and cyber security expert. SCOM 2012 design, development and implementation including SNMP ,provide support in
* Microsoft system center operation manager 2012 base on ha level and fail over that the infrastructure monitoring application will not go down. Multiple domains with highly secured DMZ gateways, develop application management packs based on the company specification .
* Risk and compliance following The US Government mandate such as FISMA, NIST, PCI-DSS, SOC2, HIPAA, and international standards.
* time availability and health status.
* Headed SCOM 2012 design, development, and implementation. SIEM tools.

**DynCorp international\_ contracts with the NSA, US Department of Defense, the state department, DHS, and NASA – Fort Worth, Texas 09/2012 - 06/2013**

**Senior infrastructure engineer - IT security senior**

* Informed Microsoft and MacAfee of a new and unknown virus to drive anti-malware and security warnings.
* Adeptly supported the main data center infrastructure, encompassing multiple government organization locations
* Developed and installed special anti-hacking and spam alerts to file servers in real time, facilitating in stopping hackers from downloading sensitive files.
* DLP data loss protection. Monitor and analyse DLP alerts generated by RSA envision.
* Security information and event management (SIEM). SCOM alerts and customize alerts management. I served as a domain Admins and IT Security, Cyber Security , event management and forensics specifically to the department of defence during their
* Operations in Kandahar and Iraq. I worked closely with top Microsoft ,MacAfee cyber security and forensics engineers to remove
* Risk and compliance following The US Government mandate such as FISMA, NIST, PCI-DSS, SOX, and international standards.

**Us department of the Treasury, Bureau of Engraving, Western & Eastern currency facilities 08/2011 - 08/2012 – Fort Worth, Texas & Washington, DC.**

**Senior systems engineer MCITP EA / infrastructure administrator / SCOM\_IT Security**

* Applied high level of security with infrastructure security implementation, successfully passing the U.S. Department of justice (DOJ) US Inspector General’s (OIG) highest requirements and audits.
* Complete infrastructure and security operations; windows 2000, 2003, 2008 r2; 2012 non- beta version in development environment; SCOM 2007 r2 sp1, SCCM, 2007, SCOM 2012, hyper-v SVCMM 2007,2012,Administered SIEM tools.
* Swiftly and efficiently resolved server issues during breaks in communication between locations.
* Risk and compliance following The US Government mandate such as FISMA, NIST, PCI-DSS, SOC2, HIPAA, and international standards.
* Improved uptime data center through effective collaboration with the infrastructure team.
* Provided comprehensive support of the Washington DC, eastern currency facility and the Fort Worth, Texas western currency facility, including SCOM infrastructure, server configurations in data center, high-level support ticket resolution, and bottleneck infrastructure resolution.

**Computer generated solution- New York, New York 02/2011 - 06/2011**

**Enterprise system administrator consultant / IT security Consultant**

* MCITP Enterprise System Engineer; MCP Security consultant.
* Infrastructure and IT security analyst. Security information and event management (SIEM). Manage engine service desk plus security suite.
* Audits Approver for new servers Windows OS and existing servers using audit applications and automation.

**Infrastructure administrator \ IT security at Wal-Mart 02/2011 - 05/2011**

**Lead systems Security Engineer - Millbrae, California**

* Security Operation Center, Risk and compliance following The US Government mandate such as FISMA, NIST, PCI-DSS, HIPAA, and international standards.
* Supported multiple datacentres in numerous Wal-Mart locations, including data center infrastructures with a focus on Microsoft server 2008, Dell, HP servers, EMC San, and third-level support.
* Audits Approver for new servers (both Windows and \Unix Linux OS) and existing servers using audit applications and automation..

**Bay area air quality control management 06/2010 - 12/2010**

**Senior systems engineer - San Francisco, California**

* Executed a production system two-year layout. Systems: windows servers, IT security, SIEM tools including Dr Management.
* Conducted active directory windows 2008 R2 installation and configuration, VMware, and migrating virtual machines. Install and configure it security monitoring tools. Setup .beach manages 102 cities in the San Francisco bay area air quality control.
* Audits Approver for new servers Windows OS and existing servers using audit applications and automation.
* Risk and compliance following The US Government mandate such as FISMA, NIST, PCI-DSS.

**California business machines 12/2006 - 04/2010**

**Infrastructure IT Security manager San, Mateo, California**

* Performed system migration and windows servers deployment, it security, and configuration for onsite medium to large-size companies, local governments, hospitals, and organizations. Cyber security tools such as: MacAfee, Symantec ,RSA security tools.
* Risk and compliance following The US Government mandate such as FISMA, NIST, PCI-DSS, HIPAA, and international standards.
* Provided support as a contractor to various Bay Area Police Departments and Hospitals such as Burlingame police department, San Mateo Police Department, San Mateo General Hospital.

**Visigenic software- San Mateo, California 01/2001 - 02/2005**

**Senior system engineer - infrastructure IT Security architect**

* Served as an infrastructure engineer with new team to build new servers and IT security for the company on windows-based operating systems. IBM, hardware and software application management. Install configure and monitor IT security tools .
* PKI, Identity and Access Management, designing and implementing security policies and

Compliances. Also responsible for engineering aspects of the company’s Public Key

* Infrastructure (PKI) and encryption services support both internally and externally

**System and technical support engineer 01/1996 - 02/2001**

* Served as a systems and technical support engineer to build new servers and it security for the police department on windows-based operating systems. IBM, UNIX, hardware and software application support. Install configure and monitor it security .

**Education & professional development**

* Bachelor of Science in Engineering, San Francisco State University

**Certifications:**

* MCSA Microsoft certified solutions associate server 2008, Microsoft
* MCP Database Administrator SQL Server 2008, Microsoft
* Cyber Security issued by The Department of Home Land Security and FEMA
* Microsoft Certified Technology Specialist - Network infrastructure
* Microsoft Certified Technology Specialist – Application Infrastructure
* Microsoft Certified Technology Specialist - Active Directory – configuration
* Microsoft Exchange server 2010 – configuration.
* Qualysguard Certified Specialist vulnerability management, Qualysguard
* MCSA enterprise administrator windows server 2008, Microsoft

**Latest certifications:**

* ITIL V3 foundation in IT service management - Obtained in 2016
* CompTIA Security+Ce certification Expiration Dec 2018
* Administering windows server 2012 with active directory course completion.