Josh Pyorre | jpyorre@pyosec.com | pyosec.com | (415) 608-9953

Objectives and career goals

My professional interests involve network, computer and data security. I aim to maintain and improve the security of organizations I work with while continuing to increase my knowledge and skills in order to provide the best quality of service possible.

Work History

Senior Security Research Analyst, December, 2014 – Present
Cisco Umbrella (previously OpenDNS), Remote and San Francisco, CA

As a security research analyst with Cisco Umbrella, I conduct research based on domains, IP addresses, malware and related indicators. My work includes report generation, log analysis and the creation of automated systems to predict and mitigate threats. Additionally, I work to be a thought leader by speaking at conferences, writing publicly and by producing a podcast (http://rootaccesspodcast.com). Some of my accomplishments in this role have been:

- Took on the role of manager of the analyst team from January – April, 2019, and continue to support the manager role when needed.
- Completed SOC2 certification for all systems and processes used by my team.
- Created:
    - A system to discover domains associated with Ransomware as they are about to be utilized.
    - Multiple systems to predict and analyze malicious domains associated with various malware families.
    - Automated report generation.
    - Automated analysis and blocking of phishing domains as they are reported.
    - Automation of common tasks performed by other researchers and analysts.
    - System to analyze false-negatives, looking for trends

Additional tasks:

- Hunting for threats, analyzing malware, domains, IP addresses, IOCs.
- Attribution of threat actors
- Writing, presenting, interfacing with marketing and sales departments.
- Meeting with customers when requested by other departments to assist with support or sales.
- Creating documentation on threat hunting, automation and various other processes.

Threat Analyst, August, 2012 – December, 2014
Dell Federal Services, NASA Ames Research Center, Moffett Field, CA

In August, 2012, I re-joined Dell Federal Services in its work with the Security Operations Center at NASA to become part of the team that mitigates threats to NASA by predicting future cyber-threats. I conducted research and work with multiple private and governmental agencies and intelligence sources to discover potential threats and take action to eliminate their effectiveness.
My work also included review and triage of phishing emails, malware analysis, network forensics, report generation and vulnerability and impact modeling.
For this position, I held a top-secret clearance.

Incident Analyst, Sept, 2011 – August, 2012
Mandiant, Remote, Virgina, San Francisco, CA, Redwood City, CA

At Mandiant, I provided vital security services to Mandiant clients (Fortune 500, Federal government agencies, etc.), reviewed and validated emerging threats, followed established methodologies, recommended process improvement, assisted in growing new service line capabilities, authored clear and concise client-facing deliverables, reviewed security-related events, assessed host-based indicators of compromise and network traffic to assist in generating new attack signatures and analyzed additional log, forensic, malware and other IR-related data. Other duties included training new team members on

Mandiant's primary product, MIR and writing documentation for various technical procedures. In this position, I was part of the initial team hired to build the MCIRT, which provided 24/7 monitoring and reporting for Mandiant clients.

Security Operations Incident Analyst and Swing/Mid Supervisor, Oct, 2010 – Sept, 2011
Dell Federal Services, NASA Ames Research Center, Moffett Field, CA

Security Operations Incident Analyst, October, 2008 - October, 2010
EyakTek, LLC, NASA Ames Research Center, Moffett Field, CA

In my work with the NASA Security Operations Center (SOC), I provided operational, development and research support for computer security initiatives, leveraging expertise in intrusion detection system monitoring, incident response, information assurance, computer security best practices, system hardening, vulnerability management, network data analysis and computer forensics. In this position, I was part of the initial team that built the SOC as the central location for security incident reporting for all of NASA.
In June, 2010, I was promoted from a Tier 2 Analyst to an Incident Manger.
In Feb, 2011, I was promoted to swing and mid-shift supervisor in addition to previous duties.
For this position, I held a secret clearance.

Primary duties:

- Regular reporting of past and future threat trends to the NASA security community
- Training and mentoring of analysts
- Creating documentation on systems and procedures
- Designing and deploying the virtual machines used by SOC analysts and related personnel
- Reviewing and reporting on all documented incidents at all NASA centers.
- Analyzing network traffic, network flows and IDS alerts.
- Interviewing potential job candidates.
- Managing swing and mid shift personnel.

Awards:
- NASA Group Achievement Award in 2009 for work in the field of IT Security

---

Technical Consultant, November, 2007 – October, 2008
EIS Consulting, *San Francisco Bay Area*

As a Technical consultant, I configured, installed and deployed network equipment, servers, computers and virtual machines with multiple operating systems. Work included designing and maintaining Active Directory domain environments, configuring and deploying group policy, deploying anti-virus servers and clients, Windows Update Server, Small Business Server, Exchange 2007, VPN endpoints and backup systems.
I also provided technical support and training for employees and ensured the correct implementation and maintenance of security policies. I worked with 3 other consultants to support 25 clients. Clients ranged from small to large organizations with over 100 users. Clients included Point Reyes Bird Observatory (prbo.org), Hamilton Family Center (hamiltonfamilycenter.org), Mother Jones (motherjones.com) and Kickstart International (kickstart.org). In this position, I acquired several new clients for the business.
References available upon request.

Technical Director, August, 2002 – November, 2007
Hamilton Family Center, *San Francisco, CA*

As Technical Director, I oversaw all aspects of the network and systems for 4 locations and for approximately 75 users. My work included technical planning, server and desktop implementation, maintenance and configuration as well as technical support, policy creation and user training. In this position I helped to open two organizational programs at new locations, connected the 4 locations over VPN, created an Active Directory WAN across the VPN, upgraded the domain from Windows 2000 to 2003 and moved the email system from an external service to Exchange Server 2003.

I was also the technical advisor for a citywide homeless advocacy program initiated by Hamilton Family Center and sponsored by San Francisco Mayor Gavin Newsom.
In November, 2007, I resigned as Technical Director and took HFC on as a client in my consulting business.

Work gap, November, 2001 to August, 2002
Due to company layoffs at Nonstop Logistics in late October, 2001, I was let go.
During my unemployment, I was actively seeking work in my desired field.

System Administrator, June, 2000 - October, 2001
Nonstop Logistics, *San Francisco, CA*

My work activities included technical problem solving, Windows NT/2000 Server administration, user management/support, hardware configuration, database administration, and network maintenance. I shared responsibilities with two system administrators to provide 24/7 support to over 200 users in San Francisco, 50 users in Atlanta, GA, 50 users in Milwaukee, WI, and 20 users in Buffalo, NY. Duties included occasional travel to other offices and training of system administrators in those locations.
While in this position, I assisted in an international upgrade from Windows NT to Windows 2000 server.

Field Service Engineer (N/E Territory US), August, 1998 - June, 2000
Scientific Learning Corporation, *Berkeley, CA and 70% travel to North-East US*

As a Field Service Engineer, I installed and configured company software, performed technical analysis of hardware and networks, and trained customers in public schools and private locations across the country. I was responsible for implementation and customer support in the north-eastern region of the US. I also provided technical support and training to the Sales Team and Project Managers on the use of internal company software and procedures.
In this position, I worked through political and technical obstacles to enable the integration of Scientific Learning's software and the New York City public school system network.

Consulting and Volunteering:

Elysian Labs, April, 2019

I built and configured a server to provide phone geo-coordinates for operators in US Special Operations. I continue to provide technical guidance as needed.

Balance Hydrolics, September, 2014

I was hired as a consultant to migrate two live web servers to virtual machines. The servers hosted multiple web sites, processed scientific data used to track rainfall throughout the year and provided internal functions to employees. The legacy systems were running CentOS and my access to them was only available via SSH. I built two CentOS virtual machines and reproduced the configurations for both servers while updating security controls and software versions. Configurations included modifying php scripts, tuning CRON jobs and batch scripts, installing and adjusting Tomcat, preparing the servers for data from sensors at multiple locations, replicating the websites and tuning the apache configurations for each site, fixing broken databases and applications in order to re-enable their use on the new systems, adjusting private and public DNS and providing a smooth transition from the old to the new servers. This work was completed over a 1 week period during my evenings and weekends.

I volunteer my time and security knowledge with several organizations. I have installed network sensors utilizing either Snort or Suricata IDS software at three locations, including two non-profits and one small business. Alerts generated by these systems are sent to a central database for each organization to review. Occasionally, I assist with incident response and mitigation and provide advice on security best practices.
Non-profits: Point Blue (http://www.pointblue.org/) and Hamilton Family Center

(http://www.hamiltonfamilycenter.org).
Small business: Code for America (http://codeforamerica.org/).

Education

I have completed courses and training in Ethical Hacking, computer forensics, network security, graphic design and Cisco Networking at City College of San Francisco. The majority of my professional skills have been self-taught, through work-sponsored training and learned while working.

Recent training:

- August, 2019: Cisco Green Belt Certification
- Sept, 2019: SANS SEC573, Automating Information Security with Python

Certifications

Malware and Memory Forensics with Volatility, Snort Certified Professional, Salesforce Administrator

General Skills

Programming, Automation, Packet and network flow analysis, IDS configuration, trending and pattern matching, Incident Response, simplifying documentation for complex systems and procedures, database configuration and management, Active Directory and group policy configuration, practical knowledge of common methods of network, system and user attack and compromise, MITRE ATT&CK and TTP mapping, Cuckoo/CAPE malware analysis configuration.

Software

Programming: Python 2/3
Security and network: ArcSight, Q Radar, Wireshark, TCPDump, TShark, Snort/Sourcefire/Suricata, MIR, Snorby/BASE
Programming: Python, Shell Scripting (Windows, OSX, UNIX/Linux)
Database and web: MySQL, Mongo, ELK, common web frameworks, Flask, HTML, CSS, JavaScript
Operating systems: Microsoft (All versions), OSX, Linux.
Other: VMWare, VirtualBox, Proxmox, Docker, and other virtualization software

Speaking and presentations

Presentations and code available at https://pyosec.com

Ransomware, Trends and Analysis
DeepSec, Vienna, AT, November, 2020
Exploitcon, Portland, OR, June, 2020

Malicious Cryptomining
QuBit Prague, Prague, CZ, April, 2019

Automating Threat Intelligence and Hunting
QuBit Sofia, Sofia, Bulgaria, November, 2018

We Pass the Costs to You, an Analysis of Cryptomining and CryptoJacking
SANS Webcast, May, 2018
https://www.sans.org/webcasts/pass-costs-you-analysis-cryptomining-cryptojacking-107565

Visualizing Botnets
DragonCon, Hong Kong, HK, December, 2020
Arctic-Con, Anchorage, AK, October, 2020
OpenLate, San Francisco, CA, October, 2018
SANS Threat Hunting Summit, New Orleans, LA, September, 2018
DeepSec, Vienna, Austria, November, 2017

The Future of the Internet (IOT, Law Enforcement and AI)
DeepSec, Vienna, Austria, November, 2017
Santa Clara City Government, October, 2017

Your Cloud is Bigger Than You Think
Midwest Cyber Security Conference, Milwaukee, WI, September, 2017

Behavioral Analysis with DNS and Network traffic
BSides Amsterdam, September, 2017
BSides Las Vegas, July, 2017
Info Security Intelligent Defense, London, May, 2017
DeepSec, Vienna, Austria, November, 2016
Infosec world, Orlando, FL, April, 2016

Building Intrusion Detection for Cloud Environments (Workshop)
BSides Portland, October, 2016 (source material posted on https://jpyorre.com)

Building the Next Generation Security Operations Center
BSides Austin, TX, April 2016
QuBit, Prague, CZ, April 2016
Cloud Security World, Boston, MA, June 2016

Building a Security Operations Center
DEFCON, Las Vegas, NV, 2010
Youtube link: http://www.youtube.com/watch?v=ZlOMmycpusw

How the NASA Security Operations Center Works
San Jose State, San Jose, CA, 2010

Securing Cloud Services
Bsides Austin, TX, 2015, Bsides SF, CA 2015, BSides Chicago 2015

Building a Better HoneyPot Network
DeepSec, Vienna, Austria
DerbyCon, Louisville, KY, 2015
NASA Ames Research Center, Moffett Field, 2015