Josh Pyorre | jpyorre@pyosec.com | pyosec.com

## Objectives and career goals

My interests involve network and computer security. I seek to improve the security of products, organizations, and people while working to increase my knowledge and skills to continuously provide high-quality expertise and solutions. I like to work on interesting problems both inside and outside the scope of my current role, often presenting findings at conferences, speaking in interviews, and applying solutions in creative ways.

## Work History

**Cisco Talos | Security Research Engineering Technical Leader**, 08/2022 - Present

- In this role, I am part of the DNS and Web team in Cisco Talos, where I help build next generation DNS and URL detection methods using machine learning, data analysis, AI/LLM technologies, and threat hunting.

**ZScaler | Principal Product Manager for Advanced Threat Protection** 12/2021- 08/2022

- Interfaced with customers and internal security research to translate customer needs into shaping the direction of the ZScalers primary product offering.

**OpenDNS/Cisco Umbrella | Senior Security Research Analyst**, 12/2014 –12/2022

- Managed a team of 7 analysts.
- Researched domains, IP addresses, malware and related indicators to protect customers from false-negative IOCs and to identify false-positives.
- Created customer reports, conducted log analysis and built automated systems to predict and mitigate threats.
- Presented at conferences and created public written content on threat activity.
- Produced a podcast called Root Access, for which I interviewed guests, narrated, and wrote music.
- Managed and completed SOC2 certification for the Security Research teams.
- Provided in-person and remote security research support to help close multiple large sales in Europe, Asia, and the US.
- Built systems to:
    - Discover domains associated with Ransomware as they were about to be used.
    - Predict and analyze malicious domains associated with various malware families.
    - Analyze false-negatives to discover actionable trends.
    - Automate customer report generation.
    - Threat hunt and Attribute threat Actor behavior.

**NASA, Dell Federal Services | Threat Analyst**, 08/2012 – 12/2014

TS Clearance (expired Dec, 2016)
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 defending against threats to NASA.

- Conducted research using data from private, government, and intelligence sources to discover potential threats and provide mitigating actions.
- Analyzed and triaged all agency phishing emails.
- Performed regular malware analysis, network forensics, report generation, and vulnerability and impact modeling.

**Mandiant | Incident Analyst** 09/2011 – 08/2012

- First of the initial team to build the MCIRT (Mandiant SOC), providing 24/7 monitoring and reporting for Mandiant clients.
- Provided security services to clients (Fortune 500, Federal government agencies).
- Reviewed and validated emerging threats, following established methodologies.
- Recommended process improvement.
- Assisted in growing new service line capabilities.
- Authored concise client-facing deliverables.
- Reviewed security-related events, assessing 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.
- Trained new employees.

**NASA, Dell Federal Services | Security Operations Supervisor**, 10/2010 – 09/2011

TS Clearance

- In Oct, 2010, the NASA SOC contract moved to Dell Federal Services.

**NASA, EyakTek, LLC | Security Operations Incident Analyst**, 10/2008 - 10/2010

Secret Clearance
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.

Responsibilities:

- Technical Manager for SOC personnel.
- Regular reporting of past and future threat trends to the NASA security community.
- Analyst training and mentoring.
- Creating documentation on systems and procedures.
- Designing and deploying the systems used by analysts.

- Reviewing and reporting on all documented incidents at all NASA centers.
- Analyzing network traffic, network flows, and IDS alerts.
- Interviewing job candidates.

Awards:

- NASA Group Achievement Award in 2009 for work in the field of IT Security
- NASA OIG award

**Technical Consultant**, 11/2007 – 10/2008

- 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 antivirus 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 of security policies.
- Worked with 3 other consultants to support 25 clients. Clients ranged from small to large organizations with over 100 users, including Point Blue, (prbo.org), Hamilton Family Center (hamiltonfamilycenter.org), Mother Jones (motherjones.com), Kickstart International (kickstart.org), Balance Hydrolics (balancehydro.com/), and Code for America (codeforamerica.org/)

**Hamilton Family Center | Technical Director**, 08/2002 – 11/2007

- Oversaw all aspects of the network and systems for 4 locations and 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, connecting them via Active Directory over VPN. Other tasks included upgrading the AD domain from Windows 2000 to 2003 and moving the email system from an external service to internally hosted Exchange Server 2003.
- I was also the technical advisor for a citywide homeless advocacy program sponsored by Gavin Newsom (San Francisco Mayor at the time).
- In November, 2007, I resigned as Technical Director and took HFC on as a client in my consulting business.

**Nonstop Logistics | System Administrator**, 06/2000- 08/2001

- Technical problem solving, Windows NT/2000 Server administration, user management/support, hardware configuration, database administration, and network maintenance.
- Provided 24/7 support to over 300 employees across the US.

**Scientific Learning Corporation | Field Service Engineer (N/E US)**, 10/1998 - 06/2000

- Technical lead in charge of implementation and customer support for the north-east US.
- Installed and configured company software, performed technical analysis of hardware and networks, and trained customers in public schools and private locations across the country.
- Provided technical support and training to Sales and Project Manager teams 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**, 2019

Built and configured systems to manage geo-location for use by operators in the US Special Operations.

## Education

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

## Certifications

SANS SEC573, Automating Information Security with Python
Malware and Memory Forensics with Volatility
Snort Certified Professional, Salesforce Administrator

### General Skills

Python, 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.

### Speaking and presentations

Active speaker and presenter at multiple conferences worldwide per year.
Visit https://pyosec.com for slides and code.