CHRIS J. TEODORSKI

Land O' Lakes, FL 34639 • (704) 615-1833 • chris.teodorski@gmail.com • www.linkedin.com/in/christeodorski/

Enterprise Information Security Professional

Security Engineering **Global Team Leadership** **Incident Management** **Cybersecurity Analysis**

Information security professional with expertise providing defensive security and proactive protection of Fortune 100 and government cloud-based and physical infrastructures. Dedicated to providing the technical expertise and decisive leadership necessary to fortify organizations' technical infrastructures, enhance their security posture, and protect valuable digital assets.

KEY ACHIEVEMENTS

+ Consulted on multiple projects at EMC2 / Virtustream to balance the go-to-market needs of the business with industry best practices and sound information security practices when deploying cutting-edge cloud services.

+ Developed process to automate discovery of rogue access points across geographically disparate locations where 'war-driving' was not practical, which saved PPG Industries a significant amount of expense and man hours.

+ Designed and implemented an open source SIEM based on Elasticsearch, Kibana, and Logstash and deployed the system on virtualized hardware, which provided EMC2 / Virtustream with enterprise-level security at extremely low costs.

PROFESSIONAL EXPERIENCE OVERVIEW

Manager, Information Security Engineer – EMC² / Virtustream	01/2015 – Present
Information Security Engineer – EMC² / Virtustream	05/2014 – 01/2015
Security Analyst III – Lowe's	02/2012 – 05/2014
Senior Security Analyst – PPG Industries	10/2008 – 02/2012
Team Lead, eBusiness Support – PPG Industries	06/2005 – 10/2008
Delivery Systems Administrator – Sapphire Technologies / DDI	10/2004 – 06/2005
Senior Network Administrator – Mahoning County	10/2003 – 10/2004
Systems Analyst, Intel Server Team – PPG Industries	10/2001 – 10/2003
LAN Design / Technology Analyst – Compex Corp / Dept. of Defense	09/2000 – 10/2001

EDUCATION

MS, Information Security and Assurance – Robert Morris University – Moon Township, PA	2009
BA, English Literature – Indiana University of Pennsylvania – Indiana, PA	1999

CERTIFICATIONS

Certified Information Systems Security Professional (CISSP)	Active
Offensive Security Certified Professional (OSCP)	Active
CompTIA Security+ and Network+	Active

SELECT TECHNICAL SKILLS

Operating Systems: Linux; Ubuntu; Debian; Red Hat; SuSE Windows
Networking: Cisco Enterprise Switches, Routers, and Pix Firewalls; TCP/IP; DHCP; WINS; DNS; HTTP; FTP; Apache; IIS;
Languages: Python; Perl
Security Tools: Metasploit; NMAP; W3AF; Burp Proxy; Nexpose; Nessus and Qualys Vulnerability Scanner; Trend Micro; Mcafee EPO
SIEM: RSA Envision; IBM QRadar; Splunk; RSA Netwitness; Elasticsearch; Logstash; Elasticsearch; Kibana

Chris J. Teodorski • (704) 615-1833 • chris.teodorski@gmail.com

PROFESSIONAL EXPERIENCE

EMC² / Virtustream – Tampa, FL 05/2014 – Present

Manager, Information Security Engineer (2015 – Present)
Information Security Engineer (2014 – 2015)
Lead a team of 7 analysts responsible for architecting, deploying, and supporting a portfolio of security tools (e.g. vulnerability management and assessment platform, SIEM tools, intrusion detection platforms, etc.) and provide incident response for 5 cloud service lines.

- Worked with various system administration teams to improve security posture and meet various compliance requirements, including PCI, HIPAA, and SOC 1/2.
  - Managed deployment of intrusion detection systems within the infrastructure as well as at the perimeter.
  - Ensured systems were hardened to a CIS level 1 and that all administrative activities are captured and auditable.
- Overcame the challenge of storing massive amounts of log data without driving up costs by leveraging a low-cost object store and a new methodology that enabled immediate retrieval of data.
- Replaced aging Cisco IDS sensors with Open Source technology based upon the Security Onion project, which significantly reduced costs while improving intrusion detection capabilities.

Lowe's – Mooresville, NC 02/2012 – 05/2014

Security Analyst III
Managed all incident response activities and SIEM management, with a focus on leading support and configuration of the RSA enVision SIEM. Conducted security assessment of international locations and assisted local support teams in resolving security issues. Mentored junior members of the team in assessing threats and identifying malicious activity on the network. Advised on development of information security policy documents.

- Provided technical expertise to the junior penetration testing team and assisted with custom Python scripts to automate time-consuming and repetitive tasks.
- Enhanced understanding of basic information security best practices among non-technical staff by developing and facilitating "lunch and learn" courses covering information security for both the workplace and the home / mobile computing environment.
- Proposed, designed, and deployed a custom honeypot management system utilizing easy-to-support open source tools to provide additional threat landscape information to the security operations team.

PPG Industries – Pittsburgh, PA 06/2005 – 02/2012

Senior Security Analyst (2008 – 2012)
Provided end-to-end security management and oversight of a global computing environment – 40K+ users, 1500+ Windows servers, and 100+ HP-UX and Red Hat Linux servers – for the Fortune 500 company with operations in 70 countries. Served as a technical resource for all incident response activities, Supported PCI, SOX, and HIPAA compliance. Managed business continuity and disaster recovery plans and testing. Served as Disaster Recovery Event Manager for all testing.

- Partnered in achieving PCI compliance by managing deployment of an application whitelisting technology to protect POS systems across 200+ stores.
- Wrote Perl and Python scripts to improve and automate resource intensive compliance and security tasks.
- Collaborated with development staff to drive adoption of secure coding methodologies and build security into the SDLC.

Team Lead, eBusiness Support (2005 – 2008)
Supervised a team of 6 on- and off-shore (India) systems analysts to support PPG's eCommerce environment, including primary support for various Microsoft web infrastructure components and 5000+ intranet and internet sites. Created and managed department budget. Served as primary interface between development community and infrastructure support teams.

- Served as Infrastructure project manager for the architectural design and deployment of PPG's next generation eCommerce environment, which utilized the latest Microsoft technologies and security practices.
- Co-chaired the company's eCommerce oversight committee, which is tasked with developing and preserving developer standards and best practices.

Chris J. Teodorski • (704) 615-1833 • chris.teodorski@gmail.com

ADDITIONAL EXPERIENCE

Sapphire Technologies / DDI – Pittsburgh, PA 10/2004 – 06/2005

Delivery Systems Administrator

Administered and maintained external facing, in-house developed HR applications and supported infrastructure servers. Managed and modernized the Quality Assurance lab. Recommended and implemented a portfolio of security best practices, including use of Group Policy objects to improve manageability, consistency, and auditing of security.

Mahoning County – Youngstown, OH 10/2003 – 10/2004

Senior Network Administrator

Supported the county's entire network infrastructure, including 28 remote locations. Improved and maintained security best practices and acted as a final escalation point for the help desk. Performed comprehensive security analysis and implemented numerous security best practices, including redesigning e-mail infrastructure to provide an additional layer of security.

PPG Industries – Pittsburgh, PA 10/2001 – 10/2003

Systems Analyst, Intel Server Team

Provided 24/7 server support for 300+ servers across North America, primary support for the corporate e-commerce environment, and back-up support for 3 additional continental Active Directory domains. Partnered with development community to resolve coding errors and environment issues. Established standards and best practices in the e-commerce environment.

Compex Corp / Dept. of Defense – Springfield, VA 09/2000 – 10/2001

LAN Design / Technology Analyst

Led project lifecycle, from research and testing through post-implementation troubleshooting, for deployment of Windows 2000 and Windows 2000 Directory Services for a large US Army client. Assisted client with disaster recovery following 9/11.

TEACHING EXPERIENCE

Robert Morris University – Moon Township, PA 05/2012 – Present

Adjunct Faculty

Developed and teach *Network Forensics and Intrusion Detection and Response* (INFS4180), a course required for the Bachelor of Science in Cyber Forensics and Information Security degree. Made the course accessible to more students by redesigning it to be offered online with a heavy concentration in online lab work.

SELECT TRAINING

SANS FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques	2016
SANS SEC542: Web Application Penetration Testing and Ethical Hacking (Challenge Coin Holder)	2016

SELECT AFFILIATIONS

Founder and Primary Organizer – BSidesCLT Security Conference	2013 – 2017
Contributing – W3AF Project	2009
Founder – Pittsburgh Information Security Users Group (PittSUG)	2009
Founder – Erie Linux Users Group (ErieLUG)	2007
Project Director at Large – Western Pennsylvania Linux Users Group	2005

SELECT SPEAKING ENGAGEMENTS

Presenter, *Drinking from the firehose: Logging at scale with ELK* – Defcon 813	2016
Presenter, *Kippo and Bits and Bits, SSH Honeypotting* – BSidesCLT Security Conference	2014 – 2015