CURRICULUM VITAE

Leonard B. Simon, MS, CISSP

LinkedIn: https://www.linkedin.com/in/leonardsimon/

Statement of Teaching Philosophy

As an educator, I believe that every person deserves the opportunity to learn, to grow, and to change their world. I am driven to educate the cyber security workforce of tomorrow. This is a critical field that is short of knowledgeable talent. My experience and education can help train the workforce that we need to be aware of the threats we face and know how to deal with them quickly and effectively. I enjoy talking about the topics of information security and cybersecurity. I can talk for hours about it and enjoy seeing the students get as hooked as I am about it. Teaching these topics is challenging, especially when it comes to technical or more logical topics of Information Security and Cybersecurity, so I make sure students feel my drive and energy. One element of teaching that continues to interest me is how each student absorbs information differently and the challenge of finding the best way for each student to learn. I strive to understand as much about them as possible to provide the best learning environment. Applying my years of practical experience, I have the key ability to create immediate relevancy. Students enjoy learning why a certain theory matters and how it can be practically used in the real world.

A good teacher respects and supports a wide diversity of students and their needs while maintaining balance and fairness. I strive to provide an environment where students feel comfortable expressing their needs and opinions and believe that their fellow classmates will benefit from their individual ideas and experience. I tell my students the first day of class to, “always keep yourself marketable”. Knowledge is something no one can take away from you and it’s a very powerful thing to have. Keep moving forward in your career by leaning as much as you can from the brightest people around you. I teach based off the power of those words. Helping students work through challenges that distract them from being engaged and to learn something new requires the teacher to continuously connecting with the student. The instructor’s job in the classroom is to create a supportive environment that allows students to relate the course material to the issues that matter personally to them. I am committed to teaching students the concepts using innovative methods, mentoring those who desire to be mentored, and helping each student achieve their educational goals.

Personal Attributes

18 years of expertise with small businesses and corporations with security, networking, web design, programming, web hosting, Internet marketing, technical support and the development of functional and secure systems.

Highly qualified educator with over five years of teaching and course design experience.

Detail oriented professional with extensive management experience in the cyber security field.

Extensive background in the SAAS & mobile technologies, programming, database management and the development and implementation of content, services and features for various web projects.

Apply a variety of teaching styles and adapt instruction to students with diverse learning styles.

Ability to excel in a demanding, outcome-oriented, and dynamic work environment.

Proven teaching strategies that promote student success.

Skilled in many disciplines such as enterprise security, cybersecurity, information security, information assurance, and risk management.

Formal Education

DIT, Information Assurance & Cybersecurity Expected 2020
Capella University, Minneapolis, MN

MS, Management Information Systems & Security 2012
Nova Southeastern University, Davie, FL

BS, Information Technology 2009
Florida International University, Miami, FL

Licenses and Certificates

Cyberark Certified Sales Professional 2017

Cisco Certified Network Associate (CCNA) 2017

Certified Ethical Hacker (CEH) 2016

Check Point Certified Security Master 2016

Check Point Sandblast Administrator 2016

Symantec Sales Expert Plus – SMG, SEP, DLP, CCS 2016

Security + | Network + | A+ | i-Net+ 2015

Certified Information Systems Security Professional (CISSP) 2015

Cybersecurity Fundamentals Certificate (ISACA) 2015

ITIL Foundations 2015

Symantec Sales Expert (SSE) - Endpoint Protection MCP 2015

Microsoft Certified Professional 2009

Educator Experience

Adjunct Professor 2016 - Present
American Public University, Charles Town, WV

Teach various online information security courses for the School of Science, Technology, Engineering, and Math.

Utilize assignments like research papers, current events, discussion posts all related to information security.

Assisted in the development and redesign of several cybersecurity courses.

Courses Taught:

ISSC471 - IT Security: Auditing
Describe and apply information security systems compliance requirements, laws, standards, and framework to create IT infrastructure security audit plans and reports for supporting business, systems, and enterprise continuity. Describe and apply information security systems compliance requirements for User Domain, Workstation and various Network Domains, Remote Access Domain, and Systems and Applications Domains. Enumerate and recommend the qualifications, ethics, and certification organizations for IT security auditors.

ISSC361- Information Assurance
Explain the differences of the various information security domains based on the information security common body of knowledge and to categorize and solidify future security goals. Apply information security principles to create information assurance policies, procedures, and standards for fulfilling investigated gaps. Evaluate an organization's rating for current required security compliance standards.

ISSC364 - IT Security: Access Control and Authentication
Describe Access Control and Authentication Policies, Procedures, Standards, and Guidelines for Information Systems and Information Assurance. Apply access control and authentication security principles to assess access risk, physical security, social engineering and human behavioral considerations, and create a plan to mitigate for security solutions. Apply security principles with encryption and cryptography methodologies to implement access control systems.

ISSC362 - IT Security: Attack and Defense
Apply security techniques and tools to identify and enumerate common characteristics, processes, and methods that could be used in attacks against systems. Evaluate systems for early detection and identification of possible issues, viruses, and attack mechanisms that could impact their security and functions. Apply security-breaching principles to show how an adversary could take advantage of systems' vulnerabilities to launch an attack against them.

ISSC363 - IT Security: Risk Management
Identify and rank the various organizational assets that could be vulnerable to possible network security breaches. Compare and contrast intrusion detection tools, techniques and prevention capabilities on firewalls, routers, switches, sensors, scanners, servers, services, and systems. Evaluate tools, techniques, methods, and components for intrusion prevention network assessment and enumeration, application vulnerability assessment, and corresponding risk assessments, and security assessments of remote maintenance services. Develop an assessment plan to identify, attack, and penetrate intrusion prevention based network systems.

Adjunct Professor 2012 - Present
Florida International University, Miami, FL

Teach various information technology and security courses.

Explain the importance of user and asset security as well as teaching them the concept of role based access within the product which restricts users to sections of our product based on their IT automation role.

Lead in-class lectures to students explaining the Patch Management module of Kaseya, which allows customers to manage their Microsoft patches throughout all of their management endpoints.

Conduct hands on demonstrations on how the patch management module works.

Receive consistent high scores from student evaluations due to high course satisfaction.

Chosen to be included on the FIU's College of Engineering and Computer Science 30th anniversary brochure as an example of an accomplished and successful FIU CEC SCIC Alumni.

Courses Taught:

CNT4403 - Network Security
This course provides an in-depth understanding of the concepts of computer and network security. It covers basic cryptography, including symmetric and public key cryptosystems as well as key management and distribution and user authentication. It introduces digital signatures, hash functions, message authentication firewalls and intrusion detection, and operational issues. Students are also introduced to topics such as Physical Security, OS Security, Malware, Network Security, Web Security, Security Models and Distributed-Applications Security.

CIS4431 - IT Automation

Students learn about IT Automation and the software used to accomplish tasks that can assist administrators in the IT field. The course is primarily based on Kaseya software and the students get a chance to not only learn the concepts of IT Automation and the suite of IT Automation tools Kaseya has to offer but students are also given the chance to become Kaseya Certified (Technical or Administrator).

Articles and Research

Simon, L. (2017, October 16). Creating a Mature Cybersecurity Program Requires Going Back to the Basics. InCyberDefense. Retrieved from https://incyberdefense.com/leonard-simon/creating-cybersecurity-program-basics/

Simon, L. (2018, March 29). Hotel Networks, Breakout Time, and Speed of Response, Oh My! Compuquip CyberSecurity https://www.compuquip.com/blog/hotel-networks-breakout-time-and-speed-of-response-oh-my

Industry and Professional Experience

Senior Security Engineer 2015 - Present
Compuquip Cybersecurity, LLC Coral Gables, FL

Design, implement, monitor and troubleshoot detailed system security architecture for customers within various industries.

Develop technical solutions and new security tools to help mitigate security vulnerabilities.

Design secure networks, systems and application architectures.

Plan, research, and develop security policies, standards and procedures.

Configure and troubleshoot security infrastructure devices.

Deploy technologies using industry standard best practices.

Perform network assessments and vulnerability scans using industry standard tools.

Compile written comprehensive reports for mitigating risk and vulnerabilities found.

Effectively communicate network security issues to peers and management.

Kaseya Overall 2009 - 2015

U.S. Support & Security Manager
Miami, FL

Collaborate with upper management and executives on strategic initiatives, operational and departmental tasks.

Managed and enforced team member access to many physical (server rooms) and logical systems as well as creating, disabling and managing role-based access to them.

Ensured confidentiality when working with team members' salaries and other PII.

Executed vulnerability scans against Kaseya public IP addresses of their global offices and worked with security team on triaging the findings.

Managed (created, modified, and revoked) user access to many key systems within the organization.

Created, modified, and revoked user access to VMs on ESXi 5.5 box.

Managed endpoint security issues/troubleshooting.

Coordinated physical access to the Miami office server room and office via proximity cards and remote user access to internal Active Directory domain.

Responsible for managing user access to all internal systems and configured role-based access.

Assisted customers and employees on how to setup 2FA via AuthAnvil module.

Conducted soft-skill and security awareness training in addition to product training on 365Command.

Information Security Council & Computer Security Incident Response Team 2014 - 2015
Miami, FL

Manage external and internal information security incidents to ensure proper procedure is executed and communication is relayed to all appropriate parties.

Conducted quarterly vulnerability scans of Kaseyas 12+ offices public IP addresses globally using Nessus Vulnerability scanner.

Oversaw all operations to ensure HVAC system was fully operational for the server room.

Triaged, assessed, and communicated potential vulnerabilities within our web-based product via customer support tickets.

Reported and documented serious security vulnerabilities or incidents.

Performed root cause analyses and incident handling for security issues with our web-based product.

Configured, deployed, and maintained Security Onion throughout our internal network, including reviewing and triaging Snorby IDS alerts.

Patch Release Coordinator 2011 - 2015
Miami, FL

Assisted senior development team with managing the release of our major product releases for customers via the agile development scrum release cycle.

Responsible for making sure the U.S. support team has the list of patches to validate and someone is assigned to the task.

Assisted lead engineers with the transition from waterfall development methodology to agile development scrum methodology from a support perspective as well as trained the support team on the transition.

Worked in conjunction with lead engineers and developers on weekly basis as the lead support contact/liaison between support and engineering teams discussing general and security related issues.

Mitigated vulnerabilities of failed patches for our web-based and mobile based products.

Streamlined cipher suites (RC4 and SSLv3) to ensure that the product only used the stronger systems.

Transitioned and trained support team members with the transition from waterfall development methodology to agile development scrum methodology.

Supported and liaised with support and engineering teams to address general and security related issues.

Senior Support Engineer 2009 - 2011
Miami, FL

Provided email/phone support for Kaseya's IT automation products ranging from agent deployment to advanced scripting.

Suggested best practices for their business to save them additional time and money as well as advised them on security issues to mitigate vulnerabilities.

Assisted customers by providing support to the various "modules" Kaseya offers for IT Automation as OEM products from several 3-party vendors.

Conducted weekly SSL scans via Qualys SSL Labs of customer's environments to gauge the strength of their web server, which run Kaseya's web-based software.

Assisted customers to configure the asset inventory module, Discovery, on a domain (via Domain Watch) or on a workgroup (via LAN Watch).

Navigated discussions with consumers to assist them in choosing which assets they would like to deploy an agent to automatically.

Supported customers with configuring the SMTP outgoing mail server within the Kaseya product so they are notified of alerts and changes within the system.

Aided customers configuring routers, firewalls (Sonicwall, Fortigate), switches (Cisco) in order for Kaseya Agent on the endpoint to check in to the central monitoring server or to reduce latency on the remote control (desktop) or VPN connection

Received Kaseya Certified Administrator (KCA) and Kaseya Service Desk Certified Administrator (KSDCA Certification

IT Operations Manager 2008 - 2009
Locations for Hollywood, Miami, FL

Designed, implemented and maintained website with a PHP/MySQL database backend.

Executed all major decisions on IT infrastructure and additional support that were crucial to the project.

Monitored and administered Web/Email/MySQL servers and services all running on Red Hat Enterprise Linux servers to ensure operational and security efficiency.

Collected over 8,000 users within the first year.

Test Engineer Intern 2007 - 2007
Citrix Systems, Inc., Ft. Lauderdale, FL

Tested Citrix Presentation Server software on various Windows operating systems.

Responsible for a 2,000 sq. ft. data center for Citrix software testing purposes which housed several PC environments, including, configuring Cisco switches, proxy servers, printing servers, TWAIN racks, smart card racks, and Secure Gateway racks.

Affinity Internet Overall 2002 - 2006
Ft. Lauderdale, FL

Dedicated Technical Support Specialist 2005 - 2006

Assisted enterprise level dedicated hosting customers with complex server issues, including web server, databases, and email optimization.

Logged in via SSH to customer machines to correct the issues they were having on the server.

Senior Technical Support Specialist 2002 - 2004

Assisted Customers with email, website and hosting account issues over the phone which required login via SSH to correct issues on their servers remotely.

Peer Coach, Quality Response Team

Responsible for monitoring and evaluating 20 Technical Support Representatives and provide them feedback on their quality of technical support.

Technical Support Trainer

Developed training curriculum for new hires.

Instructed Training Seminars for new hires and trained over 160 employees.

Knowledge Base Manager

Responsible for monthly update of the FAQ sections of the company website.

Updated FAQ per representatives and customers feedback.

Hostway Corporation Overall 2004 - 2005
Chicago, IL

Dedicated Technical Support Specialist

Assisted Customers with email, website and hosting account issues over the phone which required login via SSH to correct issues on their servers remotely.

Technical Support Trainer

Trained new hires as well as existing employees on customer service basics and technical aspects of the support position.

Entrepreneurial Experience

Business Made Social 2017 - Present
Miami, FL
www.businessmadesocial.com

Owner of a social media marketing company.

Help businesses gain awareness and market share via social media through platforms like Facebook, Instagram, Twitter, Pinterest and more.

Lenernet Hosting Solutions 2000 - 2010
Boca Raton, FL

Owner of a web hosting company.

Provided shared and dedicated web hosting services to customers all over the world so they can get their websites online.

Educational Training

Engaging the First-Year Student Certification Training 2017
American Public University System

Business and Technical Training

Technical Training and Professional Development Overall 2016 - Present

Lean Six Sigma Green Belt

SANS ICS410: ICS/SCADA Security Essentials

Offensive Security Certified Professional (OSCP) - Official Course

Imperva Web Application Security 12.0

Imperva SecureSphere System Administration 12.0

Imperva Partner Training - WAF, Database, Incapsula, Skyfence

Checkpoint Certified Security Master (CCSM) - Official Course

Symantec Messaging Gateway v10.5 Technical Sales Training

Symantec Endpoint Protection v12.1 Technical Sales Training

Symantec Endpoint Encryption v11 Technical Sales Training

Symantec Data Loss Prevention v14 Technical Sales Training

Symantec Control Compliance Suite v11 Technical Sales Training

Operational Security (OPSEC) for Control Systems - U.S. Department of Homeland Security

Cybersecurity for ICS - Mapping IT Defense-In-Depth Security Solutions to ICS

Cybersecurity for ICS - Influence of Common IT Components on ICS

Cybersecurity for ICS - Differences in Deployments of Industrial Control Systems

Cybersecurity for ICS - Determining the Impacts of a Cybersecurity Incident

Cybersecurity for ICS - Cybersecurity within IT & ICS Domains

Cybersecurity for ICS - Cybersecurity Risk

Cybersecurity for ICS - Current Trends (Vulnerabilities)

Cybersecurity for ICS - Current Trends (Threats)

Cybersecurity for ICS - Common ICS Components

Cybersecurity for ICS - Attack Methodologies in IT and ICS

CyberArk Essentials Technical Training

CyberArk Certified Sales Professional Training

CyberArk - Privileged Account Security (PAS) Fundamentals

Checkpoint Sandblast Administrator Training

Checkpoint Certified Security Expert (CCSE) - Official Course

Checkpoint Certified Security Administrator (CCSA) - Official Course

Blue Coat Technical Sales Professional - Network + Security + Cloud Training

Memberships and Affiliations

Information Systems Audit and Control Association (ISACA) 2015

International Information System Security Certification Consortium (ICS2) 2015

Conferences Attended

Symantec Knights Conference February 2018

A four–day working summit with an exclusive group of your industry colleagues.

Opportunity to participate in meetings with Symantec executives.

ISC2 Security Congress September 2016
Orange County Convention Center

The goal of ISC2 Security Congress is to advance security leaders with invaluable education, networking and career advancement opportunities to all levels of security professionals.

Residencies and Colloquia

Capella University Residency February 2018
Dallas, TX

Awards and Honors

Order of the Blue Knights (Symantec Knights) 2017

Highly Competent Subject Areas

Software and Security Systems:

Microsoft Office Suite
CheckPoint Firewall, IPS, VPN, Endpoint, App/URL Filtering, Threat Prevention and Extraction
Cisco Switches/Routers/Wireless Controllers and Access Points
BlueCoat ProxySG, SSLv, CAS, ASG, Reporter, Management Center
Symantec SEP, DLP, SMG, CCS, VIP
Imperva Web Application Firewall, Database Firewall, Incapsula, Skyfence
Cyberark
Cylance
Fortinet
Infoblox
Bradford Network Access Control
Bit9 / Carbon Black
Kaspersky Security Center
Nessus
Qualys Vulnerability Management
F5

Learning Management Systems:

Blackboard
Canvas
Moodle
Sakai

Subject Matter Expert:

Management Information Systems
Information Security

Database Systems
Security Technology
Security awareness and training
IT Automation
Computer and Network Security
Security Technology
Enterprise Security
IT Auditing
Information assurance
Access control and authentication
Attack and defense
Risk management
Cybersecurity
SIEM

References

Upon Request