

# LEONARD B. SIMON

**Insightful, results-driven IT security professional** with over 18 years of experience and notable success directing a broad range of corporate IT security initiatives while participating in planning, analyzing, and implementing solutions in support of business objectives.

---

## AREAS OF EXPERTISE

---

<i>Technical Training</i>	<i>Hosting Solutions</i>	<i>OWASP Top 10</i>
<i>Network Security Management</i>	<i>Cyber Security</i>	<i>Access Controls</i>
<i>IT Automation</i>	<i>Agile Development Cycle</i>	<i>Customer Service</i>
<i>Social Engineering</i>	<i>Intrusion Detection/Prevention</i>	<i>Cryptography</i>

---

## PROFESSIONAL EXPERIENCE

---

**Compuquip Cybersecurity LLC**, Coral Gables, Florida

Oct 2015 – Present

### Senior Security Engineer

Design, implement, monitor and troubleshoot detailed system security architecture for customers within various industries such as healthcare, government, manufacturing, technology, transportation, retail, financial, legal, hospitality, travel, and utilities.

- Develop technical solutions and new security tools to help mitigate security vulnerabilities
- Knowledge of risk assessment tools, technologies, and methods
- Experience designing secure networks, systems and application architectures
- Experience planning, researching and developing 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.
- Provide written comprehensive reports for mitigating risk and vulnerabilities found.
- Provide knowledge transfer and any required written documentation and diagrams to clients.
- Ability to communicate network security issues to peers and management

Hands-on experience with security systems including but not limited to:

- 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

**American Public University**, Charles Town, WV

Feb 2016 – Present

### Adjunct Professor in Cybersecurity at Science, Technology Engineering and Math College

Adjunct Professor for various online information security courses for the School of Science, Technology, Engineering, and Math where students are given assignments like research papers, current events, discussion posts all related to information security. Some of the IT Security-related courses taught are:

- IT Auditing
- Information Assurance
- Access Control and Authentication
- Attack & Defense
- Risk Management

**Notable Accomplishments:**

- Helped develop and redesign several cybersecurity courses

**Florida International University, Miami FL**

Aug 2012 – Present

**Adjunct Professor** for FIU's College of Computer Science and Engineering College.

Adjunct Professor for a Network Security core course as part of the IT Degree path to 25+ students per class. 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.

Also, the primary adjunct professor to 70+ students per semester in a senior-level college course called 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).

**Notable Accomplishments:**

- Popularity of this course has grown from one session per year to three sessions per semester
- Received consistent high scores from student evaluations for this course
- 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

**Kaseya, Miami, Florida**

Jan 2009 – July 2015

**U.S. Support & Security Manager** (July 2011 - July 2015)

Manage a support team consisting of 30+ support members in the U.S. ranging from tier 1 support through tier 3 which required the exercise of judgment, management decision-making, and discretion to ensure operations run smoothly. Work closely 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.

- Managed (created, modified, and revoked) user access to VMs on ESXi 5.5 box for internal testing among support team
- Assisted with endpoint security issues/troubleshooting (Definition Updates, Scans, Malware/Virus Management)
- Managed physical access to Miami office server room and office via proximity cards
- Managed (created, modified, and revoked) user access to internal Active Directory domain on the test domain via Users and Computers
- Managed (created, modified, and revoked) user access to many internal systems (License server, ticketing system, etc.) as well as configured role based access based the techs role. (Intern/Tier1, Tier 2, Tier3)
- Assisted customers and employees on how to setup 2FA via AuthAnvil module now offered to our customers so they can use this type of functionality when logging into their central Virtual Systems Administrator (VSA)
- Attended and contributed to weekly change management meetings to discuss changes to our SAAS servers across our infrastructure.
- Conducted soft-skill and security awareness training for the team members based on our support goals, missing and support/security policy
- Trained employees and customers on a product called 365Command that enabled user to manage large amount of Office365 accounts in an enterprise.

- Enforced company security policy by making sure no personal machines are brought to the office and connected to the network.
- Audited support team members machines periodically to make sure each had the required AV software installed, Kaspersky AV.

**Notable Accomplishments:**

- Built a support team of 11 support engineers to a team of 32 providing customers with a world-class support experience.
- Developed and budgeted a continued education program for support members.
- Developed a global training program for tier-1 support engineers, which increased support ticket closer rate 20%.
- Developed mini workshop training for support engineers to improve customer service and soft skills

**Information Security Council Member & Computer Security Incident Response Team Member (CSIRT)**

(January 2014 – July 2015)

Manage external (product-related issues like XSS, SQL Injection, etc.) and internal (security awareness training, access control, etc.) 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.

- Office lead to ensure HVAC system is operational for the server room. (Temperature, humidity, etc.)
- Triage/Assess/Communicate potential vulnerabilities within our web-based product via customer support tickets. (XSS, SQL Injections, etc.)
- Reported and documented serious security vulnerabilities or incidents as they came into the helpdesk from customers.
- Performed root cause analysis and incident handling for those security issues with our web-based product.
- Configured/Deployed/Maintained *Security Onion* throughout our internal network. Reviewed/Triaged Snorby IDS alerts

**Notable Accomplishments:**

- Created dozens of efficient processes/workflows for internal/external security incidents
- Increased security incident response time by 15%
- Provide information security awareness training (which also included OWASP Top 10) to global support and customer service teams
- Assist and monitor the implementation of an Intrusion Detection system “Security Onion” across the production environment as well as review logs.

**Patch Release Coordinator (July 2011 – July 2015)**

Assist senior development team with managing the release of our major product releases for customers via the agile development scrum release cycle. This included having the U.S. support team run additional regression testing apart from what the QA team performed. In charge of making sure the U.S. support team has the list of patches to validate and someone is assigned to the task. If patch validation was successful I would give go ahead to release patches to public. If patches failed I would assemble lead engineer of that particular module to assist with fix. Made adjustments to the cipher suites (removed RC4 and SSLv3) on the server side so servers with the Kaseya product will not use those weaker items when negotiated with client. 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 very closely 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. Lead the support team through regression testing when new releases came out (quarterly) to test the installation of our product as well as access controls (user logins and roles).

- Assisted in mitigating vulnerabilities of failed patches for our web-based products and mobile based products (Enterprise Mobility Management and BYOD)

- Made adjustments to the cipher suites (removed RC4 and SSLv3) on the server side so servers with our product will not use those weaker items when negotiated with client.
- 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 very closely 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

**Notable Accomplishments:**

- Increased communications between Kaseya and customers during release time (feedback, issues, etc.)
- Developed a testing environment for support to help validate patches for releases before release

**Senior Support Engineer** (June 2009 – July 2011)

Provide email/phone support for Kaseya's IT automation products ranging from agent deployment to advanced scripting. Work with Mac OS, Linux and Microsoft SQL Server 2005/2008/2012/Microsoft Server 2003/2008/2012 on a daily basis. Suggested best practices for their business to save them additional time and money as well as advised them on security issues to mitigate vulnerabilities. Working as a senior support engineer I assisted customers by providing support to the various "modules" Kaseya offers for IT Automation as OEM products from several 3-party vendors. Some of them being our Backup and Disaster Recover module (worked with our vendor Acronis and StorageCraft), our Endpoint Security modules called Kaseya Endpoint Security (worked with vendor AVG), Kaseya Anti-virus (worked with vendor Kaspersky) and lastly Kaseya Anti-malware (worked with vendor Malwarebytes). 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 with their Backup Disaster and Recovery plans via our BDR modules we offer. Assisted configuring offsite replication as well as the backup type differential, incremental and full backups.

- Assisted customers configuring the asset inventory module called Discovery which customer can use either on a domain (via Domain Watch) or on a workgroup (via LAN Watch). Both of these scan will scan the network for devices via nmap and other tools which will product a report of assets detected (machines, laptops, firewalls, routers, etc.). Customers can then choose which of those assets they would like to deploy an agent to automatically.
- Assisted customers configuring the SMTP outgoing mail server within the Kaseya product so they are notified of alerts and changes within the system.
- Assist 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

**Notable Accomplishments:**

- Had the highest number of resolved tickets among the team with superior quality and high customer satisfaction.
- Lead many presentations and meetings to increase the teams awareness and knowledge of the product.
- Received Kaseya Certified Administrator (KCA) Certification
- Received Kaseya Service Desk Certified Administrator (KSDCA) Certification.

**Locations for Hollywood, Miami, Florida**

Mar 2008 – Apr 2009

**IT Operations Manager** for start up company focusing on developing a centralized place where entertainment professionals search for places they can lease or rent for TV/movie productions.

Designed, implemented and maintained "real-estate" type website with a PHP/MySQL database backend. Made final decisions on IT infrastructure and additional servers that were needed for the website to run. Monitored and administered Web/Email/MySQL servers and services all running on Red Hat Enterprise Linux servers from an operational and security

perspective. Was required to login to the servers remotely via SSH as well as a custom web-based PHP/MySQL interface for administration.

**Notable Accomplishments:**

- Collected over 8,000 users within the first year

**Citrix Systems, Inc.** Ft. Lauderdale, Florida

May 2007 – Sept 2007

**Test Engineer Intern** for publicly traded Global Software Manufacturer.

Tested Citrix Presentation Server software on various Windows operating systems during internship program. Responsible for a 2,000 sq. ft. data center for Citrix software testing purposes which housed several PC environments. Setup of these PC environments included configuring Cisco switches, proxy servers, printing servers, TWAIN racks, smart card racks, Secure Gateway racks, and much more.

**Notable Accomplishments:**

- Internship was extended from 3 months to 5 months due to excellent performance and teamwork

**FIU College of Engineering and Computing**, Miami, Florida

Jan 2007 – May 2007

**Energy Systems Engineering Lab Intern** for local University

Worked closely with Energy Systems Lab members (graduate/undergraduate students) and collected information about their past/present/future research projects.

**Notable Accomplishments:**

- Was given the privilege of designing a website for the Energy Systems Lab members to collect their research and share knowledge.

---

## CERTIFICATIONS / TRAINING / ORGANIZATIONS

---

**CISSP** – Certified Information Systems Security Professional (ISC<sup>2</sup>)

**CEH** – Certified Ethical Hacker

**CCSM** – Check Point Certified Security Master

**Cybersecurity Fundamentals Certificate** (ISACA)

Check Point Sandblast Administrator

**CCSP** – Cyberark Certified Sales Professional

**CCNA** – Cisco Certified Network Associate (R&S)

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

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

**ITIL Foundations**

**Symantec Sales Expert (SSE)** - Endpoint Protection

**MCP** – Microsoft Certified Professional

---

## EDUCATION

---

**Doctor of Information Technology (DIT) in Information Assurance & Cybersecurity**

Capella University, Minneapolis, Minnesota

*Doctoral Student – 1/2018 - Present*

**Master of Science, Management Information Systems w/ concentration in Information Security, December 2012**

Nova Southeastern University, Davie, FL

**Bachelor of Science, Information Technology, April 2009**

Florida International University, Miami, FL