Contact

www.linkedin.com/in/antoniojohnnymartinelli (LinkedIn)
linktr.ee/admin (Personal)

Top Skills

Security
Active Directory
Troubleshooting

Languages

English (Native or Bilingual)

Certifications

Certified Information Systems Security Professional (CISSP)
Certified Information Systems Security Professional (CISSP)
A+
Apple Certified Desktop Technician
Apple Certified Portable Technician

Honors-Awards

SANS SEC560 CTF Winner
2nd Place - BSides Chicago\Detroit 2013 CTF
Eagle Scout

Antonio "Johnny" Martinelli, GIAC, CISSP

Startup pro putting Chicago on the World stage as a new technological center by supporting local technology R&D communities while remaining a popular Thought Leader at the forefront of the Information Security realm.
United States

Summary

Professional spokesman, and seasoned team leader, with robust Information Security certifications, and hands-on expertise. I work well with both Fortune 500 corporate enterprises as well as Small-to-Medium Business environments where Information Security requirements need to be designed, implemented and optimized to operate as a critical, independent infrastructure that goes well beyond checkboxes and compliance. I can be your Security Evangelist, speaking internally to support your team members network security objectives, or publicly, on your company's behalf, covering today's hottest Information Security topics.

Experience

GRIMM (SMFS, Inc.)
Director Of Information Security Training
February 2020 - Present (2 years 3 months)
United States

Community Leadership
Community Leader & International Speaker
August 2002 - Present (19 years 9 months)
International

COMMUNITY LEADER:

• Core Coordinator for BurbSec, the nation's most famous information security networking organization

• Founder of BurbSec East, which exceeded the attendance levels of BurbSec Prime in less than 1 year

• Regularly propositioned to take over ownership of the famous ChiSec meetups

• Volunteered countless hours assisting individuals with resume generation, networking and career advancement
• Director of Entertainment and Social Media for Circle City Con in Indianapolis, Indiana
• Regularly assisting with and presenting at various smaller information security and general educational groups such as ISSA, InfraGard and Evolve Security Academy
Regular organizer of non-infosec outings for the local infosec community to build and encourage comradery outside of a formal business or networking setting

INTERNATIONAL SPEAKER:
• Presented over 20 seminars at over 50 conferences & gatherings in 6 countries on the topics of Privacy, Information Security, personal management and career advancement
• Presented multiple times at such prestigious conferences as Hackers on Planet Earth (HOPE), DerbyCon, Thotcon and Hackfest Canada
• Keynote Speaker for BSides Las Vegas and GrrCon in 2017
• One of the primary contributors to the TSA Master Keys leaks of 2015 & 2016
o Created the first 3D-printed TSA key designs to actually work
o Featured in many high-profile technical publications, including Gizmodo, SC Magazine, PC Mag, Engadget and TechCrunch
o Featured in several primary news outlets, including The Hill, Daily Mail, Fox News and Vice
o Appeared several times on the Fox News channel in various local outlets

Kasada
Director of Field Engineering (North America & Europe)
October 2018 - October 2019 (1 year 1 month)
Greater Chicago Area

DIRECTOR, FIELD ENGINEERING (North America & Europe):
• Led field engineering team in understanding threat modeling and secondary revenue generation (i.e. ad revenue) in order to better comprehend the strategic goals of large enterprise customers
Established and audited Field Engineer KPIs in order to accurately measure team performance and justify headcount
• Integrated a cloud-based reverse proxy automation detection solution into a wide array of customer environments, by working with many CDN providers, including Cloudflare, Cachefly, Cloudfront, Akamai and others

• Architected and presented custom integration solutions based on customer infrastructure
• Assisted with every step of implementation, working with various engineers and administrators client-side to ensure and secure functionality
• Acted as technical lead for pre- and post-sales calls for high-profile clients
Wrote Python and JavaScript-based automation scripts to increase field engineering team task efficiency
Presented research and educational materials under the Kasada banner at various industry conferences and seminars

INFORMATION SECURITY ADVISOR:
• Worked to prioritize and security features in development pipelines, such as Single Sign-On and Role-Based Access Control
• Launched development of the company's first Information Security Program:
• Educated leadership in core Information Security concepts in order to facilitate informed decisions, such as Maturity Levels, Time-Based Security, IAM, Security in SDLC, etc.
• Led dev team leads in the understanding of PCI, ISO27001 and NIST 800-53A compliance standards, and the processes and purpose behind internal gap assessments in order to prepare for external auditing
• Created initial drafts of the company's first Business Continuity Plan
• Educated leadership and department heads in the purpose and execution of a proper Business Continuity, empowering each to effectively move down the path towards a proper plan

Uptake

Security Researcher

October 2017 - October 2018 (1 year 1 month)
Chicago, IL

SECURITY RESEARCHER:
• Perform targeted, hands-on research related to the digital security of Operational Technology (OT) and Internet of Things (IoT) devices
• File resulting vulnerability reports with the applicable public organizations (ICS-CERT, Mitre,
etc.)
• Develop and present on research findings and topics at industry conferences
• Source build out a Security Research Lab, complete with physical and virtual OT network simulations
spanning Oil & Gas, Water Treatment, Electrical Grid, Mining verticals
• Reverse-engineer OT control protocols

LEAD OT PENETRATION TESTER:

• Owner and Developer of Uptake's OT Penetration Testing Execution Framework, based heavily off Mitre ATT&CK and PTES

• Perform physical and cyber security assessments against OT client networks, in locations such as water treatment facilities, mining, manufacturing, rail, and Critical Infrastructure

PRODUCT DEV – UPTAKE CYBER SECURE:

• Function as a consultant for the overall design and roadmap of the Uptake Cyber Secure appliance and SaaS platforms, an IDS focused on detecting anomalous activity inside the data streams of industrial OT networks

• Function as a security consultant for the IoT and Data Science teams regarding development of the Uptake Cyber Secure appliance and SaaS platforms

MARKETING, LEAD GENERATION & SALES ENGINEERING:

• Assist as a technical lead on sales calls with potential clients

• Convert acquaintances in the OT space into customers for the Uptake Cyber Secure platform

• Advise Brand and Marketing on technical content and presentation of marketing materials to ensure an
accurate message and proper brand representation

• Present as a representative of the Uptake Security Research Team at industry conferences, Universities, and
local meetups in order to spread knowledge of Uptake's functions and offerings

• Work with Brand to develop logos and swag for the Uptake Security Research Team

RedLegg

Senior Information Security Consultant & Penetration Tester

May 2015 - October 2017 (2 years 6 months)

Greater Chicago Area

PENETRATION TESTING:

• Perform and/or oversee physical and/or digital security assessments using Mitre ATT&CK and PTES frameworks, with tasks including:

o SoW generation, testing, and reporting of final deliverables, including IT Risk-based reports aimed at technical personnel, as well as Business Continuity-based reports aimed at The Business and Upper Management
o Debriefing with clients, including in-depth discussion of remediation priorities, maturity goals and scheduling of additional assessments
• Perform and oversee tasks related to social engineering campaigns:
o Devise both Phishing and Vishing scenarios, websites and dialogue scripts to be used during mass social engineering risk assessment campaigns
o Execute dynamic social engineering attacks en masse, logging targets and responses
• Develop and record security awareness “webinars” to be presented live to hundreds of attendees, or pre-recorded for on-demand distribution

GOVERNANCE, RISK & COMPLIANCE (GRC):
• Assist with development or enhancement of client internal security policies, including incident response programs
• Perform gap assessments to determine client compliance with industry standards and best practices, required regulatory standards such as NIST, SOX or PCI, and/or internal policies

TEAM LEADERSHIP:
• Mentor and assist in the development of staff members in all skill sets, including technical, communication and personal management
• Assist with delegated managerial tasks to improve personal managerial skills and mentality

MARKETING, LEAD GENERATION & SALES ENGINEERING:
• Assist as a technical lead on sales calls with potential clients providing concise information to technical questions as well as provide general technical advice
• Develop and present on modern information security topics at public and private industry conferences

OfficeMax Corporate HQ
Senior Information Security Engineer
April 2011 - May 2015 (4 years 2 months)
Naperville, IL

INCIDENT RESPONSE:
• Member of Information Security Incident Response Team
• Rotating SOC shift to maintain Incident Response skillset

• Security Event Monitoring and Investigation using HP ArcSight and Splunk
• Primarily responsible for supporting and training offshore SOC analysts in Manila and Warsaw
• Investigating security policy (PCI, PII, SOX, internal, etc) violations
• Investigating corporate data leakage incidents

SOFTWARE \ APPLIANCE \ PROCESSS ADMIN:
•Primary Admin for the Following:
• Web Domain Portfolio Management (Via CSC)
• Symantec\VeriSign & Trustwave Managed PKI for SSL Certificates
• Motorola Air Defense Wireless Intrusion Detection System
• NetApp Decru DataFort Enterprise Encryption System
• McAfee Email Gateway (IronMail) appliances
• McAfee Web Gateway and Web Reporter appliances
• FireEye inline malware detection appliance
•Secondary Admin:
• McAfee Enpoint Protection \ ePolicy Orchestrator (ePO)
•McAfee EEPC & SafeBoot Encryption Agents
•McAfee VirusScan Enterprise
•McAfee Host Intrusion Prevention v7 & v8

DOCUMENTATION, METRICS & REPORTING:
• Generate team metrics for Executive \ Board review & analysis
• Monitor access removal for high-risk associate terminations and lost equipment
• Maintain departmental MediaWiki to ensure thorough and up-to-date information is available to all InfoSec associates

NOTABLE ACCOMPLISHMENTS:
• Engineered GPU-based password auditing (cracking) system and associated remediation processes and tasks to ensure password policy compliance in an enterprise with over 3000 service accounts managed by several dozen teams.
• Replaced aging BlueCoat explicit proxy system with Web Gateway setup, adding PAC-based autoconfig and Cisco WCCP support.
• Engineered a method for manually rolling out a critical firmware update to over 1200 remote WIDS sensors using TCL and TFTP.

Nextend, LLC
Systems Engineer
February 2007 - November 2010 (3 years 10 months)

• Engineered and maintained an assembly-line-style, PXE-based IT Asset Recovery system for the purpose of serving diagnostic, data eradication and disk imaging software to hundreds of workstations simultaneously, while incurring zero licensing costs using free, open-source software such as CentOS and Clonezilla. This allowed for a massive reduction in technical workforce, increasing productivity by 700% while reducing payroll expenditure by approximately 53%.
• Deployed this system from the ground up (from running Cat5 to configuring network equipment to spinning up servers) to multiple warehouse locations
• Managed endpoint protection on audit line servers by way of antimalware software, local firewalls (Windows or IPTables) and Full Disk Encryption
• Engineered and wrote scripts for large-scale, Solaris-based NAS systems for the purposes of scripted data eradication on customer drivers, per DoD standards and beyond.
• Ensured network segmentation for protection against potential threats by implementing and maintaining routing tables and switch ACLs on all diagnostic / auditing lines

Butler International
Network Technician
June 2006 - March 2008 (1 year 10 months)

Decommissioned DSL installations for Limited Brands stores which were being moved or remodeled. This included Victoria's Secret, Pink, Bath & Body Works, C.O. Bigelow, La Senza, White Barn Candle Co. and Henri Bendel locatrions

Worked with Verizon Network Operation Centers to perform installation of DSL equipment in Limited brands stores using Juniper and US Robotics network hardware.

Performed site surveys of entire indoor and outdoor shopping malls to prepare for migrating from an ISDN credit card system to DSL. This included making measurements and taking large amounts of digital pictures, and providing these to engineers via FTP.

Micro Center
6 years 7 months

Service Manager
September 2005 - February 2007 (1 year 6 months)

Verifying billing procedures, client interaction and notification, and managing parts receiving and distribution.

Analyzing daily and weekly reports to devise and implement action plans for addressing shop needs in a drastically dynamic environment.

Coordinated technician training by setting requirements and timelines for all technicians, thus maintaining the proper number and level of certified technicians for retaining various OEM service authorizations.

Wrote several Standard Operating Proceedures which were instituted for company-wide use.

Backup for both Operations and Sales management. Keyholder for all secure areas of the building, including outside doors.

Technical Support Representative
June 2005 - September 2005 (4 months)

Physically maintaining and expanding the building's Cisco-based network, including modifying network maps, submitting requests and changelogs to corporate office, and integrating additional servers, switches and routers, as well as upgrading existing ones.

Facilitating face-to-face technical support on all aspects of computer and networking setup and diagnostics.

Troubleshooting and repairing store equipment such as point-of-sale units, register drawers and signature pads, as well as impact and thermal printers.

Lead Service Technician
August 2000 - June 2005 (4 years 11 months)

Troubleshooting and repair of PowerPC (Macintosh), x86 & x64-based computers, along with peripheral devices, including scanners, printers and fax machines.

Most Productive Technician for every fiscal year

Completing a location record of over 4900 work orders in the 3.5 years served as a technician. This includes the assembly of over 100 custom-designed computers