Jason Schorr – jason@spyglassltd.com

Spyglass Security, New York City, NY 2018 to Present
Chief Operating Officer
● Designed, Architected, and Built Spyglass' Flagship Product DataDrifter[.xyz] SaaS platform (Node.JS, Python, ReactJS, redisDB, mongoDB, HTML/CSS)
● Managing daily operations and delivery at a small cybersecurity consultancy

Accenture, New York City, NY 2017 to 2018
Manager
● Led teams to deliver incident response, threat hunting, and strategic cybersecurity program development services within Accenture’s elite FusionX group

McAfee and Foundstone Professional Services , New York City, NY 2017 to 2017
Foundstone Threat Researcher
● Team Leader of the Threat Intelligence and Forensic Unit (TIF) for the City of New York. Responsible for responding to and investigating IT security related incidents.
● Subject Matter Expert and Trusted Advisor to New York City Cyber management structure and leadership.
● Cyber Threat Hunting operations, searching for Indicators of Compromise and other signs of hacking activity, responding to incident escalations from SOC.
● Analyze malware and weaponized documents, identify capability and functionality of malicious code and determine relevance and exposure to environment.
● Process documentation, run-books, flowcharts and instructions for both SOC and Threat Intelligence and Forensic teams.

FireEye, Inc. , San Francisco, CA 2015 to 2017
Consultant
● Steward of a client facing service offering focusing on network hunting and lead resource on all engagements.
● Developed and delivered internal network security hunt training focusing on methodology and mindset.
● Developed and maintained internal tools created to increase team productivity and increase internal chargeability.
● Perform on engagements that review Security Operations Center processes, procedures, use cases, playbook and incident response plans.

Sutter Health , San Francisco, CA 2015 to 2015
Senior Information Security Analyst
● Performed Security Risk Assessments on medical devices and software to be purchased and integrated into daily hospital use.
● Physical and operational security testing of area hospitals and

clinics, 25+ in the area.
● Conducted user education trainings on proper security practices and policy.

Apple Inc , Sunnyvale, CA 2014 to 2014
Security Engineer
● Daily analysis of security alerts from various appliances including Splunk Dashboards, WhiteHat, and QualysGuard.
● Lead web security engineer, handling discovery, disclosure, and remediation with development teams.
● Developed python tools to test for various disclosed 0-days, CVE-2014- 0160, and CVE-2014-3120

Cisco Systems, San Jose, CA 2013 to 2014
Information Security Analyst
● Analysis of daily security alerts from our Cisco and Sourcefire IDS utilizing various security tools and techniques.
● Worked on Sourcefire IDS tuning and policy writing including their cloud malware interface.
● Developed tools for fellow analysts to relieve pain points when performing email malware verification.

REDSPIN Inc, Carpinteria, CA 2012 to 2013
Security Consultant
● Performed HIPAA & FFIEC risk assessments.
● Extensive analysis of Nessus results, cisco ASA router, firewall, switch, and Windows Server configurations.
● Evaluated and performed physical engineering and social engineering assessments.

NASDAQ OMX, New York, NY 2010 to 2012
Systems Security Analyst III, Global Information Security
● Team leader for engineering, implementing, and supporting of the global Sourefire IDS
● Wrote policies, standards, baselines, guidelines and procedures for global security operations.
● Maintained multiple WAF's, SIEM solution, RSA Key Manager, BES server, Citrix server and VPN server.
● Performed corporate wide vulnerability assessments through the use of various tools and methods.
● Performed all aspects of an incident response lifecycle.

EDUCATION
BA Computer Science – CUNY Hunter College, NY