Scott Russell Scheferman

The Woodlands, Texas, United States

linkedin.com/in/scottscheferman

scheferman@gmail.com 16199801337

Summary

Today's fast-moving threat landscape demands that we approach the problem with new perspectives and advanced capabilities which more than ever require data-driven, automated actions capable of preventing threats that now advance at the speed of computing itself.
As we blaze through the year 2020 and beyond, Mr. Scheferman provides our community candid strategic advice and thought leadership, bringing more than two decades of experience facing the cyber adversary, while presenting novel solutions and strategic guidance to C-Suite leadership. His often disruptive perspective is founded on current, real-world operational problem solving and direct customer interface, helping organizations best prepare for emerging threats most likely to cause harm to people, privacy, production and reputation.

Experience

Principal Security Technologist

SentinelOne

Aug 2019 - Apr 2020 (9 months)

Provides the community with strategic advice, disruptive thought leadership, and a renewed perspective designed to change our attitude in how we approach the threat. He accomplishes this through direct client engagement, significant speaking and panel engagements at major industry venues, authorship of numerous thought pieces aimed at key industry sectors and by interfacing with press and media journalists.

Example of disruptive thought leadership blog here:
https://www.linkedin.com/pulse/fresh-perspective-tired-brainwashed-self-defeating-scott-scheferman

Last speaking event prior to COVID-19 pandemic:
What Happens When Privacy and Malware Trends Converge? Welcome to “Privacy Warfare”
Trends in both Privacy and Malware are converging. Data science has propelled us towards a new era in which our identity is no longer just the static markers we are born with. Instead it is a meta-collection of data points that describe how we move through time and space, and predicts what our decisions, preferences and movements are likely to be. When it is possible to re-identify data after it has been anonymized and track our behaviours in both the physical and cyber realms, we arrive at a point of no return: all static data that identifies us has been stolen and combined, while all related meta-data is tied to our true identity. This begets a new era in which criminals and nation states will are able to target victims uniquely. Like their commercial counterparts, they will have the ability to accomplish this at scale, with the same algorithmically-enhanced efficacy. Looking further out, criminals may find new ways to extort us as organizations and individuals…by modifying (vs. stealing) our privacy data. The only thing worse than a doctor losing access to a patient record due to a ransomware attack, is one whom has access but cannot trust the data; or who does, and the patient dies. This is Privacy Warfare. https://www.rebootcommunications.com/event/privsec2020

Senior Director of Global Services, Strategic Advisor, Public Speaker

Cylance Inc.

Dec 2017 - Aug 2019 (1 year 9 months)

Promoted to Senior Director of Global Services. Focus on disruptive thought leadership, relevant research on the hyper-evolving threat landscape, significant public speaking, threat intelligence sharing across public and private trust groups, incident response client engagement success (with notable emphasis on destructive and extortion-based incidents, ransom negotiation, adversary identification and attribution, proof of life, etc).

Director of Global Consulting

Cylance Inc.

Jan 2016 - Nov 2017 (1 year 11 months)

Successfully directed Cylance's expert professional services team comprised of industry-leading experts armed with advanced AI-enabled technologies. Service areas included Rapid Incident Response, IOT/IIOT, embedded OSes, Medical Devices, Research and traditional Enterprise Security Services (Red/Purple teaming, compliance, risk, table-tops, playbooks, wireless, advanced physical, etc).

Ensured team utilization, hired and mentored dozens of consultants, provided executive / board level out briefings for VLE (Very Large Enterprise) clients, oversaw all engagements in region.

Absolutely smashed our bookings, revenue and margin numbers quarter over quarter for several years.

Solutions Architect, Office of the CTO

FireEye, Inc.

May 2014 - Dec 2015 (1 year 8 months)

Public Speaking, Threat Research, Blogging and technical white papers supporting sales enablement, GTM (go to market), marketing, and internal office of the CTO initiatives.

Initiated, performed and authored an eye-opening seminal report entitled "Storming the Ivory Tower" based on security test data from over 100 Colleges and Universities, all of which had been compromised. Briefed Education CISOs and boards on results and impact of the research report.

https://www.fireeye.com/current-threats/threat-intelligence-reports/wp-storming-the-ivory-tower.html

Actively briefed LE (Law Enforcement, FBI, State Authorities, Fusion Centers (via NFCA, InfraGard WIGs, more) on cyber threat actor TTPs (Techniques, Tactics and Procedures), IOCs (Indicators of Compromise) and related Incident Response impacts, lessons-learned, table-tops, RCA (Root Cause Analysis), playbooks, containment and high-level forensic considerations.

Led research effort enabling messaging to SLED (State, Local and Education) and Federal markets to compel organizations to recognize the presence and activity of Advanced Persistent Threats (APT's) already inside their organizations, and change their attitude from a reactive to a pro-active threat mitigation approach. Analyzed historical data from POC (Proof of Concept) engagements to discern the percentage of, and attribution / distribution of APT actors inside different verticals.

Advised major university CISOs on APT activity tied to Iranian, Chinese and Russian threat actors targeting medical, research and space exploration programs.

Supported both internal Threat Intelligence as well as community trust-group TLP (Traffic Light Protocol) sharing of active threats in the wild.

Actively provided consultation, insight and support for the FireEye internal office of the CTO.

Solutions Architect

Mandiant

May 2014 - Dec 2015 (1 year 8 months)

Worked closely with State, Local and Education verticals, including LE, IC, and critical infrastructure organizations. Curated and cross-shared relevant Incident Response Threat Intelligence with teams with in FireEye and Mandiant.

Curated content for public speaking engagements, tying together Incident Response and product/technology data insights into a single, cohesive message to SLED market.

Principal Security Consultant

Sentek Global

Aug 2008 - May 2014 (5 years 10 months)
Promoted from the Technical Lead for the Navy Certification Authority to the team Project Manager; successfully leading a team of 20 cyber security risk Liaisons serving the Navy CA. My team performed in-depth cyber security risk analysis of every GENSER system within the USN, covering every technology ranging from enterprise, ICS / OT, backbone, SaaS, PaaS, application hosting facilities, satellite control systems, weapons systems, submarines and more. (over 1200 systems per year analyzed via security testing from over 800 cyber Validators). In depth risk analysis performed down to the vulnerability-level of resolution. My role was deputized by the acting CA to effectively be the final cyber risk determination for every system analyzed, an incredibly high-profile, high-responsibility role.

As of early 2013, was the Commercial BD lead for Sentek, expanding their customer base to non-Federal organizations, focusing on Information (Cyber) Security, Cloud Security (SaaS, PaaS, IaaS, etc), Mobile Device Security, and security of Virtual Environments. Given role as Project Manager, assisting a commercial software company in secure code development (Secure SDLC), security testing, security awareness training and penetration (red team) testing of the development environment (physical, network, OSINT (Open Source Intelligence gathering)).

Other roles included performing as the Technical Lead for a pilot Mobile Device platform; designing the hardware and software suite, end-to-end security, and device management for a nation-wide community of highly-mobile recruiters. Technologies researched and deployed included virtualization, thin-app containers, DAR encryption, mobile device management, thin-client, wireless carrier solutions, physical and environmental security, identity management, rapid-prototyping.

Performed in-house duties at Sentek HQ ranging from IT procurement, enterprise security, security awareness training, mentoring of consultants and project lead.

Senior Security Analyst

Northrop Grumman

Mar 2006 - Aug 2008 (2 years 6 months)
Information Assurance (Cyber) PM (Project Manager) for several NG products and systems ranging from Tactical Data Networks, Radio Networks, Website/Databases, satcom, intel, cyber labs, and more.
Effectively worked with government sponsors of NG programs, security working groups, IPTs, testing organizations, CA's and DAA's (Certification Authorities and Designated Approval Authorities) to manage and ensure the successful Security Accreditation (successful configuration and implementation of cyber security controls) of given program. Worked internally with developers, CCB's (Configuration Control Boards, aka Stakeholders), and lab managers to ensure systems meet all DoD cyber security requirements prior to Validation Testing under DITSCAP / DIACAP.
Acted as a heavily matrixed multi-program NGIT consultant for NGMS out of San Diego, CA.

Product Manager

NT OBJECTives, Inc.

2005 - 2006 (2 years)
Messaged, pitched, and proactively secured initial $1,000,000 angel round of funding from six investors for this start-up company that successfully exited with an acquisition by Rapid7.

Responsible for the successful design, execution and feature integration, as well as Security of the SDLC (Software Development Lifecycle) overall, for the flagship product, NTOSpider.

Led a diverse team of multi-national software developers, QA (quality assurance) and early-stage product pitching, beta-customer feedback integration, and GTM strategy.

Senior Security Analyst

Booz Allen Hamilton

2000 - 2003 (4 years)

Provided Federal customers with expert consulting in the areas of Certification and Accredidation, Security Requirements, Policy, Planning, Implementation, Risk Analysis, Security Architecture, IA software evaluation & recommendation, Incident Response, Network Security Assessments, Web Application Testing, Pen Testing and more.

Provided security architecture review and recommendations for the Enterprise Security of a 360,000 seat (Currently a 1m+ device!) network; performing Cyber Risk Assessments on Network Design Architecture, S / SDLC (Security / Software Development Lifecycle), Data Center, more. Held Secret Clearance.

Directly advised DAA (Designated Approval Authority) with regard to IA (information assurance) issues surrounding system components. Provided whitepapers, tech research, and recommendation to Cetification Agent. Examples of work performed: Developed guidelines for mitigation of spyware and trojan threat to enterprise, conducted incident responses activities, developed security requirements for implementation into global enterprise. Others: Spam, Bot-networks, viruses, event logging/consolidation, VoIP cyber assessments, PKI, IPv6, physical security, covert channel discovery, ICS (Industrial Control System) PPS security (Ports, Protocols, Services), discovery and applied Rainbow Series guidance on legacy / mainframe systems.

Senior Information Security Analyst

Lucent Technologies

Jan 1999 - Jan 2000 (1 year 1 month)

Lucent Network Professional Services (NPS) division acquired International Network Services (INS).

Authored seminal paper for SANS: "TROJAN WARFARE EXPOSED": https://www.giac.org/paper/gsec/540/trojan-warfare-exposed/101280

Given 20% raise for outstanding performance in the field of cyber security. Helped define, create and deliver novel cyber security services in the network security space early on in the industry's evolution of cyber security. On winning team for internal CTF (Capture the Flag) (early version of purple teaming).

Senior Network Security Engineer

International Network Services

Jan 1998 - Jan 2000 (2 years 1 month)

Provided expert cyber security consulting services and led team engagements for myriad commercial customers. Example engagements included:

Fiber-Optic Telecommunications Company, Denver CO – Project Manager for 20 person tiger team for large-scale effort to ensure data integrity and cyber security for DS1 through OC12 circuits. Performed logical architecture analysis, risk-determination, threat-discovery and other security architecture services.

Global Shipping and Packaging Company – Performed security posture review, evaluating against the ISO17799 Security Standard domains. Evaluated physical security at HQ, Policies, Procedures, Contingency Planning, Disaster Recovery, Roles and Responsibilities, Server and Network Device hardening, Network Architecture, and Security Awareness.

International Chip Manufacturer – Performed sec assessment, including interviews with director level down to end user. Analyzed Security Policies, Roles and Responsibilities. Pen testing on key public servers. Efforts concluded with Business Impact Analysis (BIA) and lead to a full-scale network reconfiguration and hardening effort.

Mentored consultants and supported their penetration testing and ethical hacking engagements by collecting, archiving, categorizing, and pushing a CD-ROM image (website on a disk) of both white hat and underground cyber tools: "Shagghie's Shangrila". Nick named "Trojan Man" as result.

Education

Ripon College

BS, Economics and Philosophy (dual)

1992 - 1995

Licenses & Certifications

CISSP - International Information Systems Security Certification Consortium

54985

Certified Ethical Hacker (C|EH) - EC Council

NA

Honors & Awards

DEFCON.org Badge Hacking Contest Winner Defcon - www.grandideastudios.com

Jul 2008

From the DEFCON 14 Badge Hacking Contest. The winning Badge Hacking contest entry by Scott Scheferman called the Event Generator Ghoul (EGG). Scott modified the LEDs on his badge to serve as event generators into his analog synthesizer. He connected the hacked badge to his Cwejman synthesizer's envelope generator and LPF cutoff frequency modulation jacks via a 1/4" stereo plug. He also installed two piezo buzzers/tweeters onto the badge to verify his initial concept and for debugging purposes. More details of the DEFCON 14 badge at http://www.grandideastudio.com/portfolio/defcon-14-badge/

Skills

Information Security • Public Speaking • Thought Leadership • Evangelism • Security Incident Response • Cyber Threat Intelligence (CTI) • Data Privacy • Leadership • Cybersecurity • Security Consulting