Joel Snape

+44 7735 058024

https://joel.sna.pe
joel@sna.pe

I am an experienced security professional, comfortable with both tackling hard technical problems and working across organisations and with customers to present complex issues in an understandable way.

I have a broad range of technical experience, with particular interests in reverse engineering, threat-intelligence and vulnerability research. I have been working most recently with a focus on the marine and offshore industry, researching both threat-actor activity and vulnerabilities in the protocols and products used.

I am motivated by difficult technical challenges, and enjoy learning about new technologies and the ways that they can be misused.

Key Skills

- Development in Python, C, C# and shell scripting.
- Malware reverse engineering and analysis.
- A deep-level understanding of networking and operating system technologies.
- Embedded device reverse engineering.
- Experienced technical writer and presenter
- Risk management, prioritisation and mitigation.
- Application and system security testing
- Mentoring and managing high-performing teams.

Experience

NETTITUDE - 2019 - PRESENT:

SENIOR RESEARCHER

I am responsible for delivering technical innovation across Nettitude's technical teams by solving complex problems. I have worked closely with our threat-intelligence team to streamline their processes and expand into new sectors; and with our red-team to apply my experience to mature our capabilities. Alongside this I have carried out vulnerability research and product assurance, both internally with a focus on maritime technologies and commercially across a range of platforms.

Key achievements:

- Malware reverse engineering, both for incident response and research.
- Designed and implemented automation pipeline for malware sample procurement, unpacking and initial analysis to streamline tracking and reporting processes.
- Researched and authored a range of publications, including technical reports and higher-level briefings, blogposts and news reports.
- Delivered commercial product and system security assessments, including TBEST red-team exercises.
- Developed innovative Linux and Windows implants for Nettitude's red-team

BT PLC. - 2012 - 2019:

HEAD OF DISCOVERY & ANALYTICS – 2016-2019

I established a new team to provide big-data and threat-hunting capabilities for BT's security operations. I was a strong technical contributor, alongside running the team, developing strategy and ensuring delivery commitments were met. I also worked with

stakeholders across the business to drive security improvements either arising from incidents or through the hunting work we carried out.

Key achievements:

- Established big-data team to deliver analytics and detection logic against large-scale datasets collected from BT's networks and data centres.
- Developed industry-leading threat-intelligence sharing programme; this provides UK-wide customer protection, and contributed to the UK government's 'Active Cyber Defence' strategy.
- Lead technical incident response for major incidents, including for two of BT's biggest customers where I co-ordinated across the customer, BT and sub-contractor environments to ensure successful remediation.

SECURITY LEAD - 2015-2016

I helped form a small team of technical specialists to provide a 'fourth-line' escalation point for our security operations department, and led technical incident response to advanced incidents. I was also responsible for writing security policies and providing design consultancy to new projects across the business.

Key achievements:

- Remediation of major customer network intrusion, involving reverse-engineering of firmware-level persistence techniques.
- Development of 'discovery' programme to understand and assess BT's internet inventory and exposure

SECURITY RESEARCHER – 2013-2015

I was a member of a team performing risk analysis, mitigation and escrow across BT's most critical networks. I was responsible for validation of source code deposits, risk analysis of network designs and hands-on vulnerability research.

PHYSICAL SECURITY SPECIALIST – 2012-2013

Developing and maintaining physical security systems to protect BT's 8500 global properties.

SOLIDWORKS UK 2007 - 2010 **QA INTERN**

Education

Durham University M.Eng (Hons) Electronic Engineering, first-class, 2012

The Perse School A-levels: A grades in Maths, Physics, Technology & English

CREST Certified Network Intrusion Analyst (CCNIA)
ISA/IEC 62443 IC32 - Industrial Control Systems Cybersecurity Fundamentals
Stanford Cryptography I
EC-Council CHFI

Reached final stage of Flare-On 7 (2020)

I have previously held security clearance.

Publications: https://joel.sna.pe/p Talks: https://joel.sna.pe/t