FRANCESCO SCHIFILLITI

Profilo Professionale

Consulente senior di Cybersecurity con oltre 10 anni di esperienza operativa in Cyber Threat Intelligence, Digital Forensics e Incident Response. Supporta Board, Funzioni di Compliance e Forze dell'Ordine nella gestione di incidenti cyber ad alto impatto, nella valutazione strategica delle minacce e nella profilazione di adversary group. Comprovata esperienza nella progettazione e implementazione di strutture CERT/SOC, nella produzione di intelligence operativa e strategica, e nella consulenza per organizzazioni nei settori Difesa, PA, Telecomunicazioni, Energy e Financial Services.

fschifilliti@forensictech.it
+39 328 825 1955 (Mobile | WA | Signal)
Via G. Zuretti, 9 – 20125 Milano (Italia)
LinkedIn.com/in/fschifilliti

Esperienza Professionale

INDEPENDENT CONSULTANT — CTI & SECURITY ADVISOR

2015 – Presente | Milano, Italia

Consulenza in Cyber Threat Intelligence, Digital Forensics e Incident Response per società di rilievo nazionale e internazionale. Attività di Strategic Advisory e ruoli di CTO in residence per clienti enterprise. Progettazione di strutture CERT/SOC, produzione di intelligence operativa STIX 2.x, threat hunting, adversary emulation e sviluppo di programmi di formazione specialistica.

MANAGER — FORENSIC TECHNOLOGY & DISCOVERY SERVICES

2013 – 2015 | Ernst & Young, Milano

Manager nel gruppo Forensic Technology and Discovery Services. Responsabilità su ingaggi di Digital Forensics, Cybercrime investigation, Fraud Investigation e progetti eDiscovery per clienti financial services, telecomunicazioni e multinazionali.

MANAGER — INFORMATION SECURITY & FORENSICS

2001 – 2013 | Lombardia Informatica, Milano

Manager nel gruppo Information Security e Technical Leader per IT Forensics e Incident Response a supporto del sistema sanitario e della Pubblica Amministrazione regionale. Oltre 12 anni di esperienza nella gestione della sicurezza ICT per infrastrutture critiche healthcare.

Competenze Chiave

CYBER THREAT INTELLIGENCE

- Progettazione di Servizi di CTI e Deployment Setup
- Progettazione di Programmi CTI (CTI-CMM) end-to-end
- Intelligence Analysis & Reporting (operativa e strategica)
- Adversary Profiling, TTP Mapping (MITRE ATT&CK), STIX 2.x/TAXII Dissemination
- Threat Landscape Assessment e Risk Briefing per C-Suite
- Threat Hunting e Supporto all'Adversary Emulation

DIGITAL FORENSICS & INCIDENT RESPONSE

- Digital & Mobile Forensics (supporto Forze dell'Ordine e corporate)
- Memory Forensics e Malware Analysis/Reverse Engineering
- Incident Handling: Processi, SOP, Playbook, Coordinamento Operativo
- Data Breach Investigation e Cybercrime Investigation
- Supporto Post-IR
- Supporto ad attività di Red Teaming

SECURITY TESTING & ADVISORY

- Strategic Advisory e CTO in Residence per clienti enterprise
- Vulnerability Assessment e Penetration Test (infrastrutturale/applicativo)
- Progettazione architetture SOC/CERT e Processi di Sicurezza/Playbook
- Conformità alla Direttiva NIS2/NIST CSF, al Framework DORA
- Analisi e Produzione di Attack Surface Monitoring & Digital Risk Protection

Strumenti & Piattaforme

THREAT INTELLIGENCE PLATFORMS
EclecticIQ · ThreatConnect · OpenCTI · MISP · Maltego · Palantir

DIGITAL FORENSICS
Principali strumenti commerciali e open-source di Digital & Mobile Forensics

MALWARE ANALYSIS
Strumenti commerciali e open-source per reversing e analisi di codice malevolo

SECURITY TESTING
Strumenti commerciali e open-source per VA&PT infrastrutturale e applicativo

Formazione Accademica

LAUREA IN SCIENZE DELL'INFORMAZIONE

Università degli Studi di Catania | 1999

Lingue

Italiano
Madrelingua

Inglese
Buono (B2)

Docenza & Formazione Specialistica

Docente in Master universitari, corsi di perfezionamento aziendali e programmi formativi per reparti speciali di Forze dell'Ordine:

- Cyber Threat Intelligence — metodologie, framework, produzione operativa
- Digital Forensics & Incident Response — procedure, strumenti, chain of custody
- Malware Forensics & Analysis — statica, dinamica, reverse engineering
- Network & Web Application Security Testing — metodologie e strumenti

Settori Industriali Serviti

Telecomunicazioni / ISP & Energy| Difesa / Forze dell'Ordine | Studi Legali & Corporate Governance | Servizi Sanitari / Pubblica Amministrazione| Financial Services & Banking