INFORMAZIONI PERSONALI

Dott. Ing. Tal Melamed

Tel Aviv (Israele)
+972.54.6234799 (ISR) | +39.0461.934480 (ITA)
tal@appsec.it
http://appsec.it

Data di nascita dicembre 1982 | Nazionalità Israeliana

Residenza Trento, Italy | Permesso di Soggiorno a tempo indeterminato

ESPERIENZA PROFESSIONALE

2013 – ad oggi

Director of Security Academy | Principal Security Consultant

AppSec Labs, (Israele)
https://appsec-labs.com

Ruoli principali

- **Direttore della Security Academy:** direzione dell'Accademia di AppSec Labs; responsabilità della ricerca scientifica e della creazione di nuovi contenuti per corsi di formazione nell'ambito della Cyber-Security. Erogazione su scala internazionale di corsi di formazione e attività di Training specializzati rivolti ad ethical hackers, sviluppatori, designers e architetti di sistema (per i dettagli dell'offerta formativa, si veda il sito: https://appsec-labs.com/training/).
- **Tech Leader:** direzione tecnica dei consulenti di sicurezza informatica di AppSec Labs; punto di riferimento per l'erogazione di informazioni tecniche per i consulenti di AppSec Labs e per le attività di revisione dei resoconti ufficiali per i clienti; gestione dei servizi clienti: valutazioni preventive dei servizi, riunioni iniziali, gestione delle relazioni tecniche, presentazione di resoconti e relazioni, riunioni con i dirigenti delle società clienti.
- **Consulente Principale:** consulenza per l'implementazione di Secure Development Lifecycle (SDL); individuazione e suggerimento di soluzioni a criticità in ambito di Software/Architecture Security e di Threat-Modelling; servizio offerto ai clienti di AppSec Labs (tra cui: *Intel*, *CheckPoint*, *IBM, Israel Aerospace Industries, NTT, HP, Wix, AVG, AT&T, LivePerson, Akamai, 888, Motorola, Israel Defence Force, Teva, Taboola, NCR, Verint*.).
- **Ricerca e Sviluppo (R&D):** attività di ricerca scientifica per nuove tecnologie, finalizzata alla produzione di nuovi dispositivi e set di strumenti per le piattaforme di Security Tests e del materiale didattico pubblicato da AppSec Labs.

Ambiti principali

- **Application Security:** direzione ed esecuzione di Security Tests (Black Box) e Code Reviews (White Box) in ambito di applicazioni Web e Desktop in conformità agli standards di riferimento e alle indicazioni OWASP e NIST, ecc.
- **Mobile Security:** direzione ed esecuzione di progetti di sicurezza per iOS, Android e WP (Hacking, Reversing, test di sicurezza e ricerca scientifica); sviluppo di piattaforme e di strumenti atti ad eseguire Security Tests per applicazioni Mobile (AppUse, iNalyzer).
- **IoT Security:** direzione di progetti nel campo di IoT Security e di Hardware Security. Analisi di PCB, di Serials e di Firmware; manipolazione di Flash/Chip; Hacking di Wireless, Radio Frequency (RF) e Bluetooth.
- **Malware Analysis:** attività di ricerca e analisi di applicazioni Malware e Anti-Malware in ambito Mobile; sviluppo e utilizzo di strumenti di analisi statica/dinamica e di Exploits; produzione di materiale didattico, finalizzato sia all'apprendimento teorico che ad eserscitazioni di carattere pratico (ad esempio: virustotal-api).

2011–2013 **Information Security Analyst**

Amdocs Ltd., (Israele)
http://www.amdocs.com

- Esecuzione di Penetration-Testing, in conformità agli standard di riferimento e alle indicazioni OWASP, per applicazioni organizzative sviluppate da Amdocs per uso interno e esterno.
- Attività didattica di sensibilizzazione alle problematiche in materia di sicurezza informatica rivolta a sviluppatori e managers dell'azienda; erogazione di presentazioni e lezioni sul tema della vulnerabilità e dei rischi nel campo dell'Application Security (impatto; possibili soluzioni; analisi di casi di studio e di incidenti di sicurezza informatica realmente avvenuti).
- Collaborazione attiva con gli sviluppatori, i project managers e gli architetti di sistema di Amdocs, per l'implementazione di principi e soluzioni di Application Security, secondo le esigenze specifiche dell'azienda.
- Progettazione e sviluppo di strumenti per Security Testing e automazione, al fine di agevolare e supportare il lavoro dell'unità di Application Security di Amdocs.

2009–2011 **Security Researcher**

CheckPoint Software Technologies Ltd., (Israele)
http://www.checkpoint.com/products/dlp-software-blade/

- Ricerca, progettazione e implementazione di contenuti di sicurezza per il sistema DLP (Data Loss Prevention), in ottemperanza ai requisiti degli standard PCI, HIPAA, PII, ecc., al fine di individuare e prevenire la trasmissione non autorizzata e data leak di informazioni riservate e sensibili.
- Creazione di Security Signatures sulla base di analisi degli algoritmi e della validazione degli standard ISO; sviluppo di modelli operativi idonei per il controllo della sicurezza informatica interna per prevenire la perdita di dati in movimento all'interno e all'esterno dell'azienda, secondo i protocolli HTTP/S, SMTP e FTP.

2006–2008 **Intelligence Analyst**

RSA, The Security Division of EMC, (Israele)
http://www.emc.com/security/rsa-identity-protection-and-verification/rsa-fraudaction.htm

- Attività di prevenzione di frode informatica per banche e istituzioni finanziarie internazionali (tra i principali clienti: Banco Posta, UniCredit, Intesa Sanpaolo, BofA, HSBC, Barclays, Citigroup, RBS, Chase, ING, E-Trade, ecc..).
- Analisi e monitoraggio di Trojans, Phishing, e delle attività fraudolenti a danno delle società finanziarie.
- Investigazioni forensi su Malicious Data/Websites per il recupero di dati finanziari rubati e il rintracciamento degli eventi e delle cause che hanno determinato uno specifico incidente di frode informatica.
- Ricerca di strategie di protezione contro le frodi informatiche da integrare nella Governance Security.

2004–2005 **Security-Operation Team Member**

Israel Aerospace Industries (IAI), (Israele)
http://www.iai.co.il/

- Gestione ed esecuzione delle strategie di sicurezza (sia sul piano fisico che della Cyber-Security) della società; monitoraggio costante della corretta gestione degli eventi, al fine di rilevare tempestivamente possibili minacce e contrastare in modo efficiente ogni possibile attacco o rischio.

2001–2004 **Caporale Maggiore Capo Scelto**

Israel Defence Force (IDF)
http://www.idf.il/

- Servizio militare della durata di tre anni nel Corpo di Fanteria della Brigata Golani dell'IDF.
- Comandante di plotone: responsabilità dell'amministrazione delle operazioni; raccolta e analisi di Intelligence; programmazione e gestione logistica delle operazioni; preparazione e training del plotone all'operazione per quanto concerne le caratteristiche logistiche, le modalità di azione, e le possibili minacce sul campo; creazione, direzione e analisi di simulazioni di scenari critici e di incidenti legati all'operazione e guida delle strategie di risoluzione sviluppate dal plotone.
- Istruttore del corso per comandanti: elezione per merito di eccellenza nel Corpo dei Comandanti della Fanteria; responsabilità della preparazione, gestione ed erogazione del programma di formazione e addestramento per il ruolo di comandante di unità operativa nelle brigate di Fanteria e Paracadutisti.

PROGETTI

ProKSy — A TCP Proxy with Java KeyStore Handling to Support SSL/TLS connections and bypassing Key-Pinning.
https://github.com/nu11p0inter/proksy

AppUse — Piattaforma per tests di Mobile Application Security in ambiente Android, con tools customizzati creati da AppSec Labs; la piattaforma, leader nel campo della Android Application Security, è fruibile gratuitamente.
https://appsec-labs.com/AppUse

iNalyzer — Framework per manipolare e alterare i parametri e i metodi delle applicazioni iOS; iNalyzer viene usato per testare applicazioni chiuse, permettendo di trasformare automaticamente un test Black-Box in uno Grey-Box.
https://appsec-labs.com/iNalyzer

Rainbow Maker — Strumento open-source per generare e operare Cracking di Hash Signatures.
http://sl.owasp.org/rainbow

Path Traverser — Strumento di Application Security ideato per testare eventuali attacchi Path Traversal e per identificare la presenza di vulnerabilità nei procedimenti di autenticazione/autorizzazione dei sistemi.
http://sl.owasp.org/pt

PUBBLICAZIONI

Tal Melamed, "An active Man-in-the-Middle Attack on Bluetooth Smart Devices," *International Journal of Safety and Security Engineering*, Vol.7, in stampa, atteso per il 2017.

CONFERENZE

http://appsec.it/talks

01-05/10/2017 — COSAC 2017 - 24th International Computer Security Symposium
Make it BLEed: Hacking BLE Applications (accettato)
http://cosac.net/

10-14/09/2017 — SECUREWARE 2017 - The Eleventh International Conference on Emerging Security Information, Systems and Technologies
Hacking Bluetooth Low Energy Based Applications (accettato)
http://www.iaria.org/conferences2017/ProgramSECURWARE17.html

06-08/09/2017 — SAFE 2017 - 7th International Conference on Safety and Security Engineering
An Active Man-in-the-Middle Attack on Bluetooth Smart Devices (accettato)
http://www.wessex.ac.uk/conferences/2017/safe-2017

04-08/08/2017 — SHA 2017
Hack-a-ble: Hacking BLE Smart Devices
https://sha2017.org/, https://media.ccc.de/v/SHA2017-230-hack-a-ble

28/06/2017 — BSidesTLV 2017
Break-a-ble: Hacking Your Smartphone with BLE
https://www.bsidestlv.com/

25-29/06/2017 — ICIMP 2017 - The Twelfth International Conference on Internet Monitoring and Protection
Hacking Bluetooth Low Energy Based Applications
https://www.iaria.org/conferences2017/ICIMP17.html

18/01/2017 — OWASP Israel January 2017
R U aBLE? BLE Application Hacking
http://sl.owasp.org/melamed17

19/09/2016 — OWASP AppSec IL 2016
Java Hurdling: Obstacles and Techniques in Java Client Penetration-Testing
http://sl.owasp.org/melamed16

ISTRUZIONE E FORMAZIONE

2007–2011 **B.Sc. Software Engineering**
Shenkar College of Engineering and Design, (Israele)

2016 Cryptography I @ Stanford University
Analisi di sistemi crittografici e del loro corretto utilizzo in applicazioni reali; esame di protocolli collaudati e analisi di errori in sistemi esistenti; studio delle tecniche di crittografia asimmetrica, ecc.

2016 Cybersecurity and Its Ten Domains @ University System of Georgia
Gestione del rischio, Governance, Compliance, Business Continuity e Disaster Recovery; crittografia; sviluppo della sicurezza del software; Access-Control, sicurezza di rete, architettura della sicurezza, operazioni di Cyber-Security; sicurezza fisica e ambientale.

2016 Software Security @ University of Maryland
Fondamenti di Software Security; analisi di importanti vulnerabilità del software, di attacchi, Exploits e delle relative strategie di difesa (tecniche di Testing avanzato e analisi del programma).

2016 Cybersecurity and the Internet of Things @ University System of Georgia
Minacce, politiche e strategie della Cyber-Security; problematiche inerenti alla privacy dei più diffusi prodotti di IoT.

2016 Usable Security @ University of Maryland
Principi di Interfaccia Uomo-Macchina (HCI); progettazione e sviluppo di sistemi sicuri con attenzione alla componente umana.

2016 Cybersecurity and Mobility @ University System of Georgia
Nuove sfide nella protezione dei dati; evoluzione delle minacce di Cyber-Security; scambi di dati critici; BYOB, sicurezza informatica efficace, strategie di prevenzione, sicurezza dei networks, ecc.

2016 Digital Risk: L'evoluzione business dell'Information Security @ ISACA Venice Chapter (IT)
Analisi e comprensione di come garantire al meglio l'Information Security nel mondo aziendale, tenendo conto non soltanto degli aspetti prettamente tecnologici, ma considerando anche altri aspetti importanti, quali: le caratteristiche del business da proteggere, i corretti processi organizzativi da adottare, l'adozione di un metodo e/o framework, la conoscenza delle relazioni aziendali, la conoscenza del livello di rischio del mondo esterno, la necessità di non fermarsi ai sistemi informativi aziendali.

2012 Mobile Application Hacking @ AppSec Labs
Architettura iOS and Android, modelli di sicurezza, FileSystem, analisi statica e dinamica, dispositivi e piattaforme per Ttesting. Modelli di minacce informatiche, metodi, strumenti, e metodo Ppen-Ttesting.

2011 Advanced Web Application Hacking & Pen-testing @ AppSec Labs
Hacking avanzato in Wweb Aapplication: metodologie e implicazioni giuridiche; elaborazione di dettagliati Security Reports; utilizzo della più comune gamma di tools nel campo della Web Application; Exploit e tecniche di difesa da attacchi informatici che sfruttano le principali vulnerabilità nel campo del laWeb Application.

2010 Network Hacking @ CheckPoint Software Technologies Ltd.
Tecniche di Network Hacking avanzate e moderne, basate su procedimenti standard di sicurezza e su principi di tecniche di evasione (ARP Spoofing, DNS Poisoning, TCP Hijack, SQL Injection, HTTPS Striping, ecc.).

2010 Network Hacking @ CheckPoint Software Technologies Ltd.
Tecniche di Network Hacking avanzate e moderne, basate su procedimenti standard di sicurezza e su principi di tecniche di evasione (ARP Spoofing, DNS Poisoning, TCP Hijack, SQL Injection, HTTPS Striping, ecc.).

2009 Certified Secure Developer @ CheckPoint
Input Validation, Buffer Ooverflow, problematiche di Format Sstrings/Iinteger Ssecurity, vulnerabilità di Privilege Escalation, gestione passwords, utilizzo sicuro di SSL/TLS.

2006 Threat Intelligence @ RSA, The Security Division of EMC
Metodologie, individuazione, Ttracing e strumenti per contrastare le minacce informatiche su Internet (Phishing, Trojans, Viruses, ecc.)

COMPETENZE PERSONALI

Competenze linguistiche
Lingua madre

Ebraico

Altre lingue

	COMPRENSIONE		PARLATO		PRODUZIONE SCRITTA
	Ascolto	Lettura	Interazione	Produzione orale	
inglese	C2	C2	C2	C2	C2
italiano	B1	B1	C1	B2	B1

Livelli: A1 e A2: Utente base - B1 e B2: Utente autonomo - C1 e C2: Utente avanzato
Quadro Comune Europeo di Riferimento delle Lingue

Competenze comunicative

Ottime capacità collaborative e relazionali in ambito personale e lavorativo, maturate durante o grazie a:

- la partecipazione a molteplici gruppi di lavoro tecnici per la gestione di progetti complessi;
- il ruolo di docente e Tutor in corsi di formazione in materia di sicurezza informatica rivolti a figure professionali multidisciplinari;
- il ruolo di istruttore e formatore in corsi militari, responsabile della trasmissione di conoscenze etico-militari e culturali e dello sviluppo delle competenze fisiche ed etiche degli attendenti;
- gli ottimi rapporti costruiti e coltivati negli anni con colleghi, collaboratori e clienti.

Competenze organizzative

Ottime capacità di leadership, di organizzazione e coordinamento di gruppi, maturate durante o grazie a:

- le fasi di progettazione e stesura di lavori tecnici di gruppo;
- le relazioni e rapporti con i colleghi e con il gruppo di networking;
- l'organizzazione, il coordinamento, il tutoraggio e l'erogazione di percorsi formativi rivolti sia a gruppi professionali che a singoli professionisti;
- l'organizzazione del materiale didattico dei corsi erogati e del relativo piano di lavoro.

Ottime capacità analitiche, investigative e di Problem Solving; prontezza nell'individuazione di soluzioni efficaci e pertinenti, sia in autonomia che in collaborazione con business partners.

Forte propensione al lavoro di squadra; valorizzazione della condivisione delle conoscenze; disponibilità, supporto e incoraggiamento per la crescita professionale dei colleghi.

Competenze digitali

- Conoscenza approfondita di Windows, Unix\Linux, ambienti OSX e della struttura del computer.
- Solida comprensione di Networking e protocolli quali TCP/IP e Client-Server Model.
- Ottima conoscenza del protocollo HTTP/S, di Web Servers e di applicazioni web.
- Ottima conoscenza dei principi, delle metodologie e delle tecniche/teorie della Cyber-Security e del panorama attuale degli attacchi informatici in diversi ambienti (Desktop/Web/Mobile/IoT).
- Competenza professionale nella programmazione dei linguaggi di scrittura Python, Java, C#, PHP, C/C++, SQL, Go, NodeJS, JavaScript and Bash/ Shell Scripting.
- Esperienza nell'uso di Scanner commerciali di sicurezza informatica: IBM AppScan, HP Fortify, Checkmarx, Tenable Nessus, Metasploit, sqlmap.
- Esperienza avanzata nell'uso dei più noti strumenti di monitoraggio della comunicazione: Burp, Fiddler, EchoMirage, ProKSy, Wireshark, tcpdump, Netcat, ecc.
- Esperienza nell'uso di strumenti di Reverse Engineering: OllyDBG, IDA, procmon, apimonitor, ILSpy, Dotfuscator, adb, FFDec, JavaSnoop, apktool, jadx/jd-gui, jbe/reJ, snoop-it, ecc.
- Esperienza nell'uso di strumenti di IoT Hacking: esptool, inspectrum, gattacker, btljuice, UART, bus pirate, GoodFet, Jtagulator, binwalk, Aircrack-ng, ecc.
- Buona padronanza dei requisiti normativi e del framework di best practice in materia di privacy e gestione della sicurezza delle informazioni (ISO27001, SOC, PCI, HIPAA, ecc.).