Luigi Martire

ESPERIENZA LAVORATIVA

01/2022 – ATTUALE – Benevento, Italia

THREAT RESEARCH TEAM LEADER | PRINCIPAL CERT OPERATOR | SENIOR INCIDENT RESPONDER – YOROI

Sono responsabile del team di Malware e Threat Research di Yoroi. Le mansioni principali prevedono il coordinamento del team in ambito Malware Research e di redazione di report pubblici e privati. Sono diventato il leader del team di Malware ZLab di Yoroi, laboratorio avanzato di analisi di minacce informatiche e di analisi malware. Scrivo, insieme con il resto del mio team, costantemente per i principali blog di cyber security italiana e molti dei miei articoli sono stati condivisi dalla principali testate giornalistiche nazionali e internazionali.
Sono anche uno dei senior Incident Responder nel momento in cui un cliente contatta Yoroi per la risoluzione di un incidente, a partire dalle fasi iniziali fino alla produzione di reportistica e di presentazione al Cliente.
Mi occupo della formazione dei nuovi analisti junior (partendo dalla formazione teorica, fino al training on the job degli stessi), sia di fornire supporto come analista di secondo livello e Incident Responder.
In sintesi:

- Malware Analysis Team Leader
- Security Research Team Leader
- Threat Intelligence Team Leader
- Principal Incident Responder
- Reverse Engineering
- Threat Research
- SOC L2
- SOC L3
- Addetto alla formazione

04/2022 – ATTUALE – Bologna, Italia

DOCENTE A CONTRATTO DI MASTER UNIVERSITARIO – UNIVERSITÀ DI BOLOGNA

Sono docente al Master di I livello in Cybersecurity dell'Università di Bologna denominato "Cybersecurity: from design to operations".
Mi sono occupato di insegnare il modulo di CERT Operation, dove si trattavano le materie di gestione delle attività CERT e poi approfondimenti molto verticali in Malware Analysis.

12/2019 – 03/2020 – Benevento, Italia

CORRELATORE TESI MAGISTRALE – UNIVERSITÀ DEGLI STUDI DEL SANNIO

Sono stato correlatore di una tesi magistrale in Ingegneria Informatica presso l'Università degli Studi del Sannio intitolata "Progettazione e sviluppo di un rilevatore automatico di tecniche di evasione nei malware".
L'obiettivo della tesi era quello di creare una antologia delle tecniche di evasione dei malware utilizzate dagli attaccanti e in seguito la progettazione di uno strumento che permettesse di automatizzare il processo di rilevamento di tali tecniche. Infine, sono state costruite delle indagini statistiche sui risultati ottenuti a valle dello studio di un dato numero di campioni malware.

14/10/2020 – 12/2021 – Benevento, Italia

PRINCIPAL CERT OPERATOR - SENIOR CYBER THREAT INTELLIGENCE ANALYST - REVERSE ENGINEER – YOROI

Mi occupo della operazioni CERT (Computer Emergency Response Team) di Yoroi, dove mi occupo di tre macro aree: Cyber Threat Intelligence, Malware Analysis e Incident Response.
Faccio parte del team di Malware ZLab di Yoroi, laboratorio avanzato di analisi di minacce informatiche e di analisi malware. Scrivo, insieme con il resto del mio team, costantemente per i principali blog di cyber security italiana e molti dei miei articoli sono stati condivisi dalla principali testate giornalistiche nazionali e internazionali.
Ho effettuato analisi su minacce attribuibili a gruppi hacker governativi (tra cui APT28, APT29, MuddyWater) o legati al cyberspionaggio.
Ho effettuato analisi avanzate sulle minacce intercettate dalle sonde aziendali sui clienti, fornendo indicatori di compromissione e regole Yara necessarie ad aggiornare i sistemi di rilevamento e, eventualmente, a bonificare le macchine infette.
I report pubblici prodotti da me sono disponibili su : https://yoroi.company/blog con il tag "ZLAB".
Ho curato l'immagine di ZLab sui social, in particolar modo Twitter, rapportandomi con altri analisti malware indipendenti o appartenenti ad altre aziende e partecipando ad analisi collaborative su minacce di interesse per la comunità.
Infine, sono coinvolto quotidianamente a prestare supporto agli analisti L1 del servizio SOC (Security Operation Center) offerto dal gruppo Yoroi. Mi occupo sia della formazione degli analisti junior (partendo dalla formazione teorica, fino al training on the job degli stessi), sia di fornire supporto come analista di secondo livello e Incident Responder.
In sintesi:

- Malware Analysis
- Incident Response
- Security Research
- Threat Intelligence
- Reverse Engineering
- Threat Research
- SOC L2
- SOC L3
- Addetto alla formazione

01/01/2019 – 13/10/2020 – Benevento

SENIOR MALWARE ANALYST E THREAT RESEARCHER – CYBAZE SPA

Sono il principal Malware Analyst e Threat Researcher di Cybaze. Faccio parte del team di ZLab di Cybaze, laboratorio avanzato di analisi di minacce informatiche e di analisi malware. Scrivo, insieme con il resto del mio team, costantemente per i principali blog di cyber security italiana e molti dei miei articoli sono stati condivisi dalla principali testate giornalistiche nazionali e internazionali.
Ho effettuato analisi su minacce attribuibili a gruppi hacker governativi (tra cui APT28, APT29, MuddyWater) o legati al cyberspionaggio.
Ho effettuato analisi avanzate sulle minacce intercettate dalle sonde aziendali sui clienti, fornendo indicatori di compromissione e regole Yara necessarie ad aggiornare i sistemi di rilevamento e, eventualmente, a bonificare le macchine infette.
I report pubblici prodotti da me sono disponibili su : https://yoroi.company/blog con il tag "ZLAB".
Ho curato l'immagine di ZLab sui social, in particolar modo Twitter, rapportandomi con altri analisti malware indipendenti o appartenenti ad altre aziende e partecipando ad analisi collaborative su minacce di interesse per la comunità.
Sono responsabile del corso di formazione in malware analysis fornito da Cybaze (https://cybaze.it/la-formazione-del-gruppo-cybaze-i-nostri-docenti/).
Infine, sono coinvolto quotidianamente a prestare supporto agli analisti L1 del servizio SOC (Security Operation Center) offerto dal gruppo Cybaze. Mi occupo sia della formazione degli analisti junior (partendo dalla formazione teorica, fino al training on the job degli stessi), sia di fornire supporto come analista di secondo livello e Incident Responder.
In sintesi:

- Malware Analysis
- Threat Research
- SOC L2
- SOC L3

- Addetto alla formazione

Indirizzo Benevento, Italia

10/2019 – 12/2019

CONSULENZA IN AMBITO PENETRATION TEST – CONSULENZA PRESSO TIM

Sono stato tre mesi in consulenza presso il Cliente di in qualità di team leader di un gruppo di penetration testers. Mi sono occupato della gestione delle commesse da parte del Cliente, con la qualifica di Team Leader Penetration Tester.
Nello specifico, mi sono occupato di gestire le richieste dei task dei test da compiere, dell'assegnazione ai vari tester. Il mio compito, oltre la gestione , prevedeva che portassi a compimento anche il mio test, controllare l'andamento degli altri, ed infine effettuare l'ultima review dei report prodotti non solo da me, ma anche dal mio team, prima della consegna, la quale spettava a me.
I test erano sia di tipo infrastrutturale che applicativo. Quindi ho utilizzato l'intera toolchain presente in Kali Linux.

Indirizzo Roma, Italia

01/2019 – 13/10/2020

PENETRATION TESTER – CYBAZE SPA

Ho effettuato test di penetrazione nei confronti delle infrastrutture informatiche dei clienti, avvalendomi di strumenti professionali quali Nessus, Acunetix e l'intera suite fornita da Kali Linux.
Ho effettuato delle valutazioni del rischio a cui le infrastrutture informatiche dei clienti sono esposte e fornito dei piani di rientro per la mitigazione delle vulnerabilità riscontrate.
Ho effettuato delle gap analysis tecniche delle infrastrutture informatiche dei clienti rispetto ai requisiti richiesti dal nuovo regolamento europeo (GDPR).

Indirizzo Benevento, Italia

10/2018 – ATTUALE

DOCENTE A CONTRATTO – LINK CAMPUS UNIVERSITY

Docente a contratto della Link Campus University Roma. Sono stato incaricato di effettuare docenza per l'insegnamento in master sia di primo che si secondo livello in Cyber-Security.
Le docenze erano relative a:

- Malware Analysis
- Vulnerability Assessment & Penetration Testing

Indirizzo Roma, Italia

01/2019 – 06/2019

DOCENTE E PREPARATORE PER LA CYBER CHALLENGE – UNIVERSITÀ DEGLI STUDI DEL SANNIO

Dal Gennaio 2019 al Giugno 2019 sono stato docente e istruttore della squadra dell'Università degli Studi del Sannio per la competizione nazionale della Cyber Challenge.
Durante l'attività, ho provveduto a formare i componenti del team nelle seguenti tematiche:

- Vulnerabilità
- Risk assessment
- Malware Analysis
- Network defence
- Network Attack
- Etical Hacking
- Capture The Flag

Indirizzo Benevento, Italia

02/01/2018 – 31/12/2018

MALWARE ANALYST & THREAT RESEARCHER – CSE CYBSEC ENTERPRISE SPA

- Malware analysis
- Threat research
- Penetration testing

Indirizzo Roma

01/07/2017 – ATTUALE

MALWARE ANALYST E SECURITY SPECIALIST – ISWAT - LAB

- Malware Analysis
- Vulnerability Assessment e Penetration Test

Indirizzo Benevento, Italia

ISTRUZIONE E FORMAZIONE

ABILITAZIONE ALLA PROFESSIONE DI INGEGNERE SETTORE INFORMAZIONE – Univerisità degli Studi Del Sannio

12/2015 – 13/12/2018 – Benevento

LAUREA MAGISTRALE IN INGEGNERIA INFORMATICA – Università degli Studi del Sannio

Tesi in "Sicurezza e Delle Reti e dei Sistemi Software" dal titolo "Analysis and Characterization of current attacks profiles captured through Honeypots".
Votazione 110/110 e Lode.

Indirizzo Benevento

09/2012 – 12/2015 – Benevento

LAUREA TRIENNALE IN INGEGNERIA INFORMATICA – Università degli Studi del Sannio

Tesi in Misure Elettroniche dal titolo "Progettazione e sviluppo di un sistema basato su piattaforma aerea per il rilievo e la misurazione dei sinistri stradali".
Votazione 106/110.

Indirizzo Benevento

2007 – 2012 – Avellino

DIPLOMA DI MATURITÀ CLASSICA – Liceo Classico "Pietro Colletta"

Indirizzo Avellino

COMPETENZE LINGUISTICHE

Lingua madre: **ITALIANO**

Altre lingue:

	COMPRENSIONE		ESPRESSIONE ORALE		SCRITTURA
	Ascolto	Lettura	Produzione orale	Interazione orale	
INGLESE	C1	C1	C1	C1	C1

Livelli: A1 e A2: Livello elementare B1 e B2: Livello intermedio C1 e C2: Livello avanzato

PATENTE DI GUIDA

Patente di guida: B

COMPETENZE ORGANIZZATIVE

Competenze organizzative

- Ottima esperienza nella gestione di progetti (acquisita in ambito didattico).
- Ottima capacità di Problem-Solving.
- Attitudine naturale a lavorare in gruppo.
- Abilità di leadership essendo diventato Threat Research Team Leader.

COMPETENZE COMUNICATIVE E INTERPERSONALI

Competenze comunicative e interpersonali.

- Spirito di gruppo (derivante da una serie di progetti portati a termine in ambito didattico e nel lavoro in team).
- Ottima capacità di comunicazione (acquisita in ambito didattico, essendo docente).

COMPETENZE PROFESSIONALI

Competenze professionali

- Spiccata capacità di Reverse Engineering (sviluppata nelle attività di malware analysis)
- Analisi Forense (sviluppata nelle attività di ricostruzione degli attacchi malware)
- Competenze di mentoring (come analista malware, SOC L2 e docente a contratto, sono responsabile della formazione delle nuove risorse)

LICENZE E CERTIFICAZIONI

24/10/2022 – 31/10/2026

GIAC Reverse Engineering Malware - GREM

GREM holders have demonstrated the knowledge and skills to reverse-engineer malicious software (malware) that targets common platforms, such as Microsoft Windows and web browsers. Professionals holding the GREM know how to examine inner-workings of malware in the context of forensic investigations, incident response, and Windows system administration.

https://www.credly.com/badges/52e1b0ea-38b0-4c14-b7f4-43440c736bb2

04/2020
Autopsy 8-Hour Online Training

Rilasciato a Basis Technology

ID Credenziale: 16364663

https://www.credential.net/16bf69f1-294f-41e4-9895-28ada5e7aaaa

07/2020
Certificate of Completion: ICSI | CNSS Certified Network Security Specialist

Rilasciato da: ICSI (International CyberSecurity Institute), UK
ID Credenziale: 20779351
https://www.credential.net/3d2dbd47-ae38-4715-9a57-9d22a6986c75

Intro to DFIR: The Divide and Conquer Process

Rilasciato da: Basis Technology
ID Credenziale: 6d4qatrc3b
https://dfir-training.basistech.com/certificates/6d4qatrc3b

Autorizzo il trattamento dei miei dati personali presenti nel CV ai sensi dell'art. 13 d. lgs. 30 giugno 2003 n. 196 - "Codice in materia di protezione dei dati personali" e dell'art. 13 GDPR 679/16 - "Regolamento europeo sulla protezione dei dati personali".