europass

Luigi Martire

Sesso: Maschile

ESPERIENZA LAVORATIVA

[14/10/2020 – Attuale] **Principal CERT Operator - Senior Cyber Threat Intelligence Analyst - Reverse Engineer**

Yoroi

Città: Benevento

Paese: Italia

Principali attività e responsabilità:
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.
Altra attività di competenza è quella relativa all'emanazione dei bollettini di sicurezza quando vengono pubblicate nuove vulnerabilità con i relativi CVE da approfondire.
Questa mansione si colloca nell'ambiente del vulnerability management dei nostri clienti.
In sintesi:

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

[01/01/2019 - 13/10/2020] **Senior Malware Analyst e Threat Researcher**

Cybaze SpA

Indirizzo: Benevento, Italia

Città: Benevento

Principali attività e responsabilità:

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

[10/2019 - 12/2019] **Consulenza in Ambito Penetration Test**

Consulenza presso TIM

Indirizzo: Roma, Italia

Principali attività e responsabilità:

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.

[01/2019 - 13/10/2020] **Penetration Tester**

Cybaze SpA

Indirizzo: Benevento, Italia
Principali attività e responsabilità:
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).

[10/2018 - Attuale] **Docente a contratto**

Link Campus University

Indirizzo: Roma, Italia
Principali attività e responsabilità:
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

[01/2019 - 06/2019] **Docente e preparatore per la Cyber Challenge**

Università degli Studi del Sannio

Indirizzo: Benevento, Italia
Principali attività e responsabilità:
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

[02/01/2018 - 31/12/2018] **Malware Analyst & Threat Researcher**

CSE CybSec Enterprise SPA

Indirizzo: Roma
Principali attività e responsabilità:

- Malware analysis
- Threat research
- Penetration testing

[01/07/2017 - Attuale] **Malware Analyst e Security Specialist**

ISWAT - Lab

Indirizzo: Benevento, Italia
Principali attività e responsabilità:
- Malware Analysis
- Vulnerability Assessment e Penetration Test

ISTRUZIONE E FORMAZIONE

[09/2020] **Abilitazione alla Professione di Ingegnere settore Informazione**

Univerisità degli Studi Del Sannio

[12/2015 - 13/12/2018] **Laurea Magistrale in Ingegneria Informatica**

Università degli Studi del Sannio

Indirizzo: Benevento
Principali materie studiate/competenze professionali acquisite.:
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.

[09/2012 - 12/2015] **Laurea Triennale in Ingegneria Informatica**

Università degli Studi del Sannio

Indirizzo: Benevento
Principali materie studiate/competenze professionali acquisite.:
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.

[2007 - 2012] **Diploma di Maturità Classica**

Liceo Classico "Pietro Colletta"

Indirizzo: Avellino

COMPETENZE LINGUISTICHE

Lingua madre: italiano

Altre lingue:

inglese

ASCOLTO C1 **LETTURA** C1 **SCRITTURA** C1

PRODUZIONE ORALE C1 **INTERAZIONE ORALE** C1

PATENTE DI GUIDA

Automobile: 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 (derivante da progetti universitari sviluppati in team, di cui sono stato nominato 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

[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".