CURRICULUM VITAE

INFORMAZIONI PERSONALI

Nome	GIANLUCA
Cognome	OGLIETTI
Qualifica	Categoria D
Amministrazione	POLITECNICO DI TORINO
Incarichi attuali	Esperto di dominio (Servizio Cybersecurity & IT for Research)
Numero telefonico dell'ufficio	0110906698
Email istituzionale	gianluca.oglietti@polito.it

ESPERIENZE PROFESSIONALI E LAVORATIVE C/O POLITECNICO

Esperienze professionali (incarichi ricoperti)

01/12/2022 - Attuale **Politecnico di Torino**

Servizio Cybersecurity & IT for Research

Esperto di dominio (Servizio Cybersecurity & IT for Research)

Descrizione attività:

Componente del servizio "Cybersecurity & IT for Research" presso ISIAD con incarico di ED "Cloud Cybersecurity".

01/11/2022 - 01/12/2022 **Politecnico di Torino**

Infrastrutture Servizi Informatici e Amministrazione Digitale

Tecnico Amministrativo

Descrizione attività:

Componente del servizio "Cybersecurity & IT for Research" presso ISIAD con l'obiettivo di fornire supporto e consulenza sulle problematiche di sicurezza informatica (sia in ambito on-premise che in ambito cloud), di fornire supporto e consulenza sul controllo del traffico di rete, di collaborare con il Coordinatore della Sicurezza Informatica di Ateneo all'attuazione delle linee programmatiche sulla security e privacy, e di supportare i referenti informatici e gli incaricati della sicurezza informatica delle strutture dell'Ateneo (dipartimenti, centri, amministrazione, enti ospitati, ecc.) nella diagnosi e nella bonifica di sistemi attaccati o vulnerabili.

Elenco delle attività svolte:

- Installazione, configurazione e gestione dei sistemi di sicurezza perimetrali ed interni d'Ateneo.
- Progettazione, installazione, configurazione e gestione di sistemi multi processore ad elevate prestazioni per l'acquisizione e l'analisi del traffico di rete.
- Attuazione delle linee programmatiche di Ateneo su sicurezza e privacy.
- Monitoraggio del livello di sicurezza dell'infrastruttura IT d'Ateneo (portali web,postazioni client/server, infrastruttura di rete)
- Analisi dei log di Security & Compliance dell'ambiente cloud di Microsoft 365.
- Analisi ed utilizzo, ai fini di PoC, del prodotto Microsoft Sentinel come soluzione SIEM nativa del cloud Microsoft 365.
- Analisi, configurazione e gestione di differenti piattaforme software per la cifratura dei dati su piattaforme cloud proprietarie.
- Progettazione, realizzazione, configurazione e gestione dei canali cifrati sicuri VPN verso enti o ambienti cloud remoti.
- Condivisione di informazioni riguardanti nuove tipologie di attacco informatici o aggiornamenti di sicurezza critici.
- Supporto nella diagnosi, nella bonifica e nella riconfigurazione di sistemi IT vittima di attaccati informatici o potenzialmente vulnerabili.
- Supporto nell'analisi puntuale o sistematica di grandi quantità di log.
- Esecuzione di indagini di informatica forense.
- Recupero dati da supporti/dispositivi danneggiati.
- Cancellazione sicura di dati memorizzati su svariate tipologie di supporti o dispositivi.
- Supporto nell'analisi e nella ricerca delle cause di problematiche di funzionamento ("troubleshooting") sia a livello applicativo che a livello rete.

01/12/2017 - 01/11/2022 **Politecnico di Torino**

Information Technology

Tecnico Amministrativo

Descrizione attività:

Componente dell'"Unità di sicurezza IT" presso l'AreaIT con l'obiettivo di fornire supporto e consulenza sulle problematiche di sicurezza informatica (sia in ambito on-premise che in ambito cloud), di fornire supporto e consulenza sul controllo del traffico di rete, di collaborare con il Coordinatore della Sicurezza Informatica di Ateneo all'attuazione delle linee programmatiche sulla security e privacy, e di supportare i referenti informatici e gli incaricati della sicurezza informatica delle strutture dell'Ateneo (dipartimenti, centri, amministrazione, enti ospitati, ecc.) nella diagnosi e nella bonifica di sistemi attaccati o vulnerabili.

Elenco delle attività svolte:

- Installazione, configurazione e gestione dei sistemi di sicurezza perimetrali ed interni d'Ateneo.
- Progettazione, installazione, configurazione e gestione di sistemi multi processore ad elevate prestazioni per l'acquisizione e l'analisi del traffico di rete.
- Attuazione delle linee programmatiche di Ateneo su sicurezza e privacy.
- Monitoraggio del livello di sicurezza dell'infrastruttura IT d'Ateneo (portali web,postazioni client/server, infrastruttura di rete)
- Analisi dei log di Security & Compliance dell'ambiente cloud di Microsoft 365.
- Analisi ed utilizzo, ai fini di PoC, del prodotto Microsoft Sentinel come soluzione SIEM nativa del cloud Microsoft 365.
- Analisi, configurazione e gestione di differenti piattaforme software per la cifratura dei dati su piattaforme cloud proprietarie.
- Progettazione, realizzazione, configurazione e gestione dei canali cifrati sicuri VPN verso enti o ambienti cloud remoti.
- Condivisione di informazioni riguardanti nuove tipologie di attacco informatici o aggiornamenti di sicurezza critici.
- Supporto nella diagnosi, nella bonifica e nella riconfigurazione di sistemi IT vittima di attaccati informatici o potenzialmente vulnerabili.
- Supporto nell'analisi puntuale o sistematica di grandi quantità di log.
- Esecuzione di indagini di informatica forense.
- Recupero dati da supporti/dispositivi danneggiati.
- Cancellazione sicura di dati memorizzati su svariate tipologie di supporti o dispositivi.
- Supporto nell'analisi e nella ricerca delle cause di problematiche di funzionamento ("troubleshooting") sia a livello applicativo che a livello rete.

ALTRE ESPERIENZE PROFESSIONALI E LAVORATIVE

Esperienze professionali (incarichi ricoperti)

16/04/2007 - 30/11/2017

Datore di lavoro:
Politecnico di Torino

Ruolo:
Assegnista di Ricerca

Descrizione attività:

Componente dell'"Unità di sicurezza IT" presso il CeSIT e l'AreaIT con l'obiettivo di fornire supporto e consulenza sulle problematiche di sicurezza informatica e sul controllo del traffico di rete, e di supportare i Referenti Informatici e gli incaricati della sicurezza informatica delle strutture dell'Ateneo (dipartimenti, centri, amministrazione, enti ospitati, ecc.) nella diagnosi e nella bonifica di sistemi attaccati o vulnerabili.

Elenco delle attività svolte:

- Installazione, configurazione e gestione dei sistemi di sicurezza perimetrale d'Ateneo.
- Progettazione e gestione di sistemi dedicati all'acquisizione e all'analisi del traffico di rete.
- Attuazione delle linee programmatiche di Ateneo su sicurezza e privacy.
- Monitoraggio del livello di sicurezza dell'infrastruttura IT d'Ateneo (portali web,postazioni client/server, infrastruttura di rete).
- Condivisione di informazioni riguardanti nuove tipologie di attacchi informatici o aggiornamenti di sicurezza critici.
- Supporto nella diagnosi, nella bonifica e nella riconfigurazione di sistemi IT vittima di attacchi informatici o potenzialmente vulnerabili.
- Esecuzione di indagini di informatica forense.
- Recupero dati da supporti o dispositivi danneggiati.
- Cancellazione sicura di dati memorizzati su svariate tipologie di supporti o dispositivi.
- Supporto nell'analisi e nella ricerca delle cause di problematiche di funzionamento ("troubleshooting") sia a livello applicativo che a livello rete.

Pubblicazioni:

- 2015: Articolo su rivista "International Journal of Computer Science and Software Engineering" (IJCSSE): M. Mezzalama, G. Oglietti, E. Venuto, "IP packet capture on high throughput networks by using NUMA architectures" (ISSN 2409-4285 - 4:10(2015), pp. 248-255)

- 2013: Articolo in atti del Congresso Nazionale AICA – Fisciano, 18-20 Settembre 2013: M. Mezzalama, G. Oglietti, E. Venuto, "Sicurezza nelle reti: utilizzo di architetture multi-core per il monitoraggio del traffico IP" (ISBN: 9788898091164)

- 2011: Articolo in atti del Congresso Nazionale AICA – Torino, 15-17 Novembre 2011: M. Mezzalama, G. Oglietti, "Acquisizione del traffico IP da una rete ad elevato throughput utilizzando un sistema Open Source: tecnologie e problematiche" (ISBN: 9788890540646)

ISTRUZIONE E FORMAZIONE

Titoli di studio

Titolo:
Laurea in Ingegneria Elettronica

Università:
POLITECNICO DI TORINO

Data di conseguimento:
13/03/2007

Voto:
106

	Titolo: Perito Elettronico Industriale *Università:* Istituto Tecnico Industriale Statale "Q.Sella" - Biella *Data di conseguimento:* 16/07/1997 *Voto:* 60/60
Corsi di formazione svolti presso il Politecnico	*Titolo:* Tool GoPrivacy: funzionalità dei Registri di trattamento e Valutazione dei rischi *Data di conseguimento:* 27/05/2022 *Titolo:* Seminario formativo su Criminalità informatica e investigazioni digitali - Strategie e tecniche di prevenzione *Data di conseguimento:* 03/05/2022 *Titolo:* Seminario formativo di presentazione del nuovo modello organizzativo *Data di conseguimento:* 24/03/2022 *Titolo:* Formazione Specifica alla Salute e Sicurezza per i Lavoratori - Rischio Basso *Data di conseguimento:* 08/09/2021 *Titolo:* Privacy - Formazione per amministratori di sistema *Data di conseguimento:* 10/06/2021 *Titolo:* Pillole di Privacy e Cyber Security *Data di conseguimento:* 10/06/2020 *Titolo:* Salute e sicurezza sul lavoro: formazione aggiuntiva per videoterminalisti che operano in lavoro agile *Data di conseguimento:* 29/04/2020 *Titolo:* Workshop formativo su Microsoft Office 365 *Data di conseguimento:* 17/07/2019 *Titolo:* Formazione Operatore BLS-D finalizzato al rilascio dell'autorizzazione all'impiego del DAE *Data di conseguimento:* 20/03/2019 *Titolo:* Corso di formazione sull'utilizzo del defibrillatore semiautomatico *Data di conseguimento:* 08/03/2019 *Titolo:* Corso di Formazione Generale sulla normativa anticorruzione e sulle azioni di prevenzione attivate al Politecnico di Torino *Data di conseguimento:* 20/11/2018 *Titolo:* Incontro informativo/formativo sul Regolamento generale europeo sulla protezione dei dati, RGPD- UE 679/2016 *Data di conseguimento:* 14/06/2018

Titolo:
Corso di Formazione Generale sulla Sicurezza per i lavoratori ai sensi del D.Lgs. 81/2008 e coerente con l' Accordo Stato Regioni 21 dicembre 2011

Data di conseguimento:
18/01/2018

CAPACITÀ E COMPETENZE PERSONALI

Conoscenza delle lingue

Lingua	Comprensione (Ascolto)	Comprensione (Lettura)	Orale (Interazione)	Orale (Produzione)	Scrittura
Italiano	Madrelingua	Madrelingua	Madrelingua	Madrelingua	Madrelingua
Inglese	B1 - Utente autonomo	B1 - Utente autonomo	B1 - Utente autonomo	B1 - Utente autonomo	B1 - Utente autonomo

Capacità e competenze tecniche

- Sistema operativo Linux: installazione, configurazione client/server e ottimizzazione (ricompilazione di pacchetti software e del kernel di sistema)
- Sistema operativo mobile Android: utilizzo avanzato (linea di comando), debug e compilazione di ROM aggiornate per smartphone non più supportati
- Sistemi operativi Microsoft client (da Windows 95 a Windows 11): installazione, configurazione e ottimizzazione
- Sistemi operativi Microsoft server (da Windows 2003 a Windows 2022): installazione, configurazione e ottimizzazione
- Sistemi di sicurezza (Next Generation Firewall) di CheckPoint: installazione, configurazione, ottimizzazione e debug avanzato
- Sistemi di sicurezza (Next Generation Firewall) di Fortinet: installazione, configurazione, ottimizzazione e debug avanzato
- Sistemi NUMA (Non-Uniform Memory Access): installazione, configurazione e ottimizzazione dei processi che necessitano di elevate risorse di calcolo
- Conoscenza del linguaggio di programmazione C (livello approfondito) e C++ (livello base)
- Conoscenza dei linguaggi di programmazione Basic, Visual Basic, Python e scripting Bash
- Conoscenza dei sistemi di versioning del codice sorgente basati su tecnologia Git.
- Utilizzo approfondito del servizio GitHub da interfaccia web, da linea di comando o tramite GUI dedicate
- Conoscenza basilare dei principali linguaggi di programmazione utilizzati per la realizzazione di pagine WEB (quali HTML e PHP)
- Conoscenza dei protocolli utilizzati all'interno delle reti Ethernet (IP, TCP, UDP, ICMP, ecc)
- Conoscenza delle tecniche di acquisizione del traffico IP anche in reti ad alta velocità
- Capacità di analisi di acquisizioni di traffico IP al fine di identificare problemi o malfunzionamenti utilizzando software dedicati
- Conoscenza delle principali metodologie e dei principali software o necessari per effettuare il Vulnerability Assessment di postazioni client/server
- Conoscenza delle principali metodologie e dei principali tool da impiegare per individuare, analizzare e bonificare PC Windows/Linux compromessi
- Conoscenza delle principali metodologie e dei principali tool hardware e software da utilizzate durante le indagini di informatica forense
- Conoscenza dei tool hardware/software PC-3000 e Data Extractor utilizzati per il recupero dei dati memorizzati su Hard Disk (HDD o SSD) danneggiati
- Capacità di assemblare in modo ottimale un server o un PC installandone in modo appropriato le varie componenti
- Capacità di smontare un server o un PC con l'obiettivo di individuare eventuali problemi hardware
- Capacità di installare, configurare e gestire reti informatiche di piccole e medie dimensioni
- Capacità di utilizzare i più comuni apparecchi necessari per effettuare riparazioni su dispositivi elettronici (saldatori, programmatori EEPROM, ...)