ELENCO TEMI BORSE DI STUDIO

Aggiornato al 15/01/2023

Temi finanziati da Reiss Romoli srl

R1: “Tecniche di Machine Learning applicate alla Cyber Security”

Con l’uso del Machine Learning il processo di rilevamento del malware è più perseguibile, scalabile ed efficace rispetto agli approcci tradizionali, che richiedono l'intervento umano. Il lavoro di tesi esplorerà le metodologie analitiche e statistiche che possono essere adottate, sia per Intrusion che per Vulnerabilty detection. L’obiettivo sarà quello di realizzare una applicazione capace di automatizzare almeno alcune fasi della Cyber Security Assessment

R2: “Next Generation Firewall”

NGFW (Next Generation Firewall), i firewall di nuova generazione (3a generazione) costituiscono delle vere e proprie piattaforme integrate di network security. Esse combinano le funzionalità proprie di firewall tradizionali (traffic filtering) con funzionalità avanzate quali la DPI (Deep Packet Inspection), Application Firewalling, IDS/IPS e, nelle versioni più recenti, anche funzionalità di Machine Learning e/o Intelligenza Artificiale al fine di migliorare l'efficacia delle proprie rivelazioni, ad esempio, tramite Behavioural Analysis o suggerendo proattivamente politiche di sicurezza. Si individueranno alcuni scenari di rete simulati, per cimentarsi nel deploy e nella configurazione di dispositivi NGFW all'interno di tali scenari, ricorrendo a strumenti sia Open Source che proprietari, mettendo anche in luce differenze, punti di forza e debolezza.

R3: “Ansible, Puppet, Chef - sistemi di automazione a confronto “

Il lavoro è centrato sulla analisi, lo studio e il confronto delle potenzialità di diversi sistemi di automazione, in particolare Ansible, Puppet e Chef.
I sistemi dovranno essere messi a confronto in modo da individuare i punti di forza e di debolezza su tematiche inerenti la gestione delle configurazioni di environment di rete, il deploy di applicazioni e servizi e la gestione di sistemi operativi.
Nello specifico, andranno valutate le loro caratteristiche, mettendo a confronto i meccanismi di funzionamento, le relative performance e le feature in generale sotto vari punti di vista e in diversi contesti.

R4: “Zero Touch Provisioning in ambienti Edge Cloud”

L’obiettivo dell’approccio Zero Touch Provisioning, è quello di ridurre, fino a “portare a zero” con l’ausilio di tecnologie di automazione, la necessità di interventi manuali durante il deployment di funzioni di rete e piattaforme QoE virtualizzate. Si dovrà partire da uno studio di dettaglio di ZTP: delle sue potenzialità, dei possibili casi di studio ad esso connessi, nonché delle tecnologie e degli strumenti di automation necessari allo scopo. Tra i casi di studio analizzati si andrà quindi ad approfondire quello dell’Edge Cloud Computing.

R5: “OSINT : metodologie, tecniche e applicazioni “

L'open source intelligence (OSINT) è il processo di identificazione, raccolta, elaborazione, analisi e segnalazione delle informazioni, ottenute da fonti pubblicamente disponibili. E rappresenta uno strumento interessante per l’analisi del mercato, la valutazione della concorrenza, la raccolta di indicazioni per lo sviluppo del business. La tesi si concentra su un settore specifico di mercato, vengono esaminati casi specifici classificati come più rappresentativi del mercato stesso, cercando di raccogliere tutte le informazioni che il web mette a disposizione su di essi.
I risultati ottenuti, per ogni categoria di analisi, vengono via via commentati e contestualizzati per ottenere una visione di insieme dell’ambito di mercato cui si è fatto riferimento.

Dominio ICT Aerospazio Abruzzo
c/o Università degli studi dell’Aquila
SS 17 Ovest, loc. Boschetto di Pile
67100 – L’Aquila – Italia
segreteria@ictaerospazio.abruzzo.it

ELENCO TEMI BORSE DI STUDIO

Aggiornato al 15/01/2023

Temi finanziati da Leonardo Spa

L1: Vulnerability Intelligence

Lo studente dovrà analizzare strumenti e metodi per l'erogazione di un servizio automatico di vulnerability intelligence che possa aggregare informazioni riguardanti vulnerabilità per rappresentare correttamente il livello di rischio dell'organizzazione. Altre attività sperimentali possono riguardare lo sviluppo di un orchestratore di scansioni, ovvero uno strumento, che permetta di schedulare e notificare l'avvio delle attività interagendo in modo automatico con vari tools commerciali specializzati nell'erogazione di VA.

L2: Strumenti di mitigazione delle vulnerabilità legate al fattore umano in ambito Cyber Security

Il fattore umano è uno dei principali vettori di attacco utilizzati dai criminali per ottenere accesso ai sistemi e ai dati delle aziende. I lavori di tesi in questo ambito dovranno individuare e proporre soluzioni per mitigare questa vulnerabilità, focalizzandosi sugli aspetti di formazione.
Nel dettaglio, lo studente dovrà riportare qual è lo stato dell'arte degli strumenti per la formazione e individuare e sperimentare le nuove soluzioni che si stanno affermando sul mercato. Inoltre, sulla base di quanto visto sopra, dovrà proporre un framework di servizi che vada a coprire tutti gli aspetti ritenuti più importanti per mitigare al meglio il fattore umano.
Lo studente sarà supportato durante il lavoro di tesi e sarà possibile modulare l'obiettivo durante lo svolgimento.

L3: Analisi delle minacce storiche per lo sviluppo di strumenti predittivi in ambito Cyber

Scopo di questo tema di tesi è quello di realizzare un tool/algoritmo basato su machine learning, rete neurale o algoritmo predittivo che permetta, basandosi sui dati collezionati e sull'osservazione dei trend relativi alle minacce (vettori di attacco, tipologie di malware, vulnerabilità sfruttate), di poter prevenire e fronteggiare nuove minacce. Per esempio: lo studio dell'evoluzione degli attacchi di phishing, la detection di attacchi 0day, analisi e rilevamento comportamenti anomali (behaviour analysis) . Lo studente sarà supportato durante il lavoro di tesi e sarà possibile modulare l'obiettivo durante lo svolgimento.

L4: Strumenti di astrazione tecnologica in ambito Real Time Security Monitoring

Scopo di questo tema di tesi è quello di realizzare e sperimentare metodologie di data analytics/ data fusion da applicare ai dati provenienti dai vari sistemi di sicurezza in uno in un SOC.
La tesi sarà prettamente sperimentale e dovrà prevedere la definizione e lo sviluppo di uno unse case che tenga in considerazione diverse sorgenti dati. Scopo dello sviluppo è quello di offrire ad un operatore/analista SOC/CSIRT un layer operativo che possa supportarlo nel svolgere le consuete analisi ed operazioni di sicurezza (triage, attack detection, threat hunting, reporting, dashboarding, detection engineering). Lo studente sarà supportato durante il lavoro di tesi e sarà possibile modulare l'obiettivo durante lo svolgimento.

L5: Sperimentazione di metodologie in ambito data analytics su attività di Red Teaming

Le attività di red teaming sono caratterizzate dall'utilizzo di un ampio spettro di tools con cui gli analisti devono interfacciarsi e dai quali ricevono un'ampia varietà di dati da analizzare e correlare. L'obiettivo delle attività di tesi in questo filone è quello di analizzare il flusso di lavoro dell'analista per individuare e implementare soluzioni che possano automatizzare o migliorare parti del processo, come ad esempio la fase di discovery, reporting o analisi e correlazione dei dati anche attraverso l'analisi di dati storici. Lo studente sarà supportato durante il lavoro di tesi e sarà possibile modulare l'obiettivo durante lo svolgimento.

Dominio ICT Aerospazio Abruzzo
c/o Università degli studi dell'Aquila
SS 17 Ovest, loc. Boschetto di Pile
67100 – L'Aquila – Italia
segreteria@ictaerospazio.abruzzo.it

L6: Threat Hunting Automation

Spesso l'attività di Threat Hunting è limitata da IOC (indicatori di compromissione) e tiene poco in conto attività comportamentali (TTP, Tecniche Tattiche e Procedure).
Scopo di questo ambito di tesi è quella di, a partire da una dataset di telemetrie raccolte, definire una serie di regole statiche su un log collector (es. elastic search) che estraggano delle "features comportamentali" riconducibili al TTP Mitre. Tali features possono essere la base per creare modelli automatizzati di rilevamento compromissioni. Libera scelta dello studente è esplorare modelli di machine learning adatti (es. linear regression, classificatori, etc) e creare i training set più adeguati. Lo studente sarà supportato durante il lavoro di tesi e sarà possibile modulare l'obiettivo durante lo svolgimento.

L7: Data Protection

Sperimentazione e sviluppo di metodologie e tecnologie in ambito Data Protection. La data Protection, nella sua accezione più generale include oltre a tematiche tradizionali della data security (protezione da furto/accessi non autorizzati) anche la protezione del dato da eventi che possono portarne alla perdita o al danneggiamento (data vaulting). Tesi su questa tematica avranno l'obiettivo di approfondire le tecnologie, le problematiche e le best practice esistenti per garantire la sicurezza, la privacy e la compliance dei dati.
Su questa tematica, rivestono particolare importanza gli sviluppi tecnologici nelle aree del Cloud Computing, degli Algoritmi Quantum – safe e nella crittografia omomorfica, su cui si baserà la protezione dei dati delle future infrastrutture IT. Lo studente sarà supportato durante il lavoro di tesi e sarà possibile modulare l'obiettivo durante lo svolgimento.

L8: Cyber Security for Aereospace

Sperimentazione e sviluppo di metodologie e tecnologie in ambito Aereospace. I sistemi e le infrastrutture utilizzati in ambito aereospace stanno diventando sempre più interconnessi tra loro e con le infrastrutture tradizionali, aumentandone sensibilmente il perimetro di esposizione alle minacce cyber.
Le attività di tesi su questa tematica avranno l'obiettivo di identificare e sperimentare tecnologie, metodologie e standard normativi utilizzati nei sistemi spaziali per garantire la loro resilienza alle intrusioni informatiche. A seconda della tipologia di tesi, e in accordo con le altre attività di ricerca e sperimentazione in essere, dovranno essere simulate e sperimentate tattiche, tecniche e procedure applicabili sui vari componenti dei sistemi aerospaziali (es. software di terra e di bordo, infrastrutture di comunicazione, supply chain). Lo studente sarà supportato durante il lavoro di tesi e sarà possibile modulare l'obiettivo durante lo svolgimento.

L9: Cyber Security for automotive

Sperimentazione e sviluppo di metodologie e tecnologie in ambito Automotive. La trasformazione in atto nel settore dell'automotive protesa verso guida autonoma, auto elettriche e auto connesse pone in primo piano il problema della Cybersecurity. La cybersecurity di un veicolo passa per la protezione dell'intero ecosistema, a partire dai sistemi di bordo fino alle infrastrutture remote utilizzate per la gestione e l'aggiornamento.
Le attività di tesi su questa tematica riguarderanno l'approfondimento degli standard, delle tecnologie e delle best practice attuali, oltre che quelli in fase di sviluppo. A seconda della tipologia di tesi e, in accordo con le altre attività di ricerca e sperimentazione in essere, saranno effettuate attività sperimentali nelle quali dovranno essere simulati dispositivi e componenti dell'ecosistema automotive per testare le principali tecniche tattiche e procedure utilizzate dagli attaccanti. Lo

Dominio ICT Aerospazio Abruzzo
c/o Università degli studi dell'Aquila
SS 17 Ovest, loc. Boschetto di Pile
67100 – L'Aquila – Italia
segreteria@ictaerospazio.abruzzo.it

studente sarà supportato durante il lavoro di tesi e sarà possibile modulare l'obiettivo durante lo svolgimento.

L10: Crisis Management Platform

I lavori di tesi in questo ambito dovranno individuare e proporre soluzioni innovative per la gestione di incidenti e crisi in ambito cyber.
Nel dettaglio, lo studente dovrà riportare qual è lo stato dell'arte degli strumenti per la gestione incident per poi individuare e sperimentare una soluzione tecnologica che possa supportare i processi aziendali e le attività operative in maniera completa e flessibile, in accordo con i principali framework e best practices internazionali in ambito incident management. Lo studente sarà supportato durante il lavoro di tesi e sarà possibile modulare l'obiettivo durante lo svolgimento.

Dominio ICT Aerospazio Abruzzo
c/o Università degli studi dell'Aquila
SS 17 Ovest, loc. Boschetto di Pile
67100 – L'Aquila – Italia
segreteria@ictaerospazio.abruzzo.it