Allegato 4

Borse di Formazione
Sportello parco
Sviluppo del capitale umano innovativo e qualificato nel Parco scientifico e tecnologico della Sardegna
Sportello parco

PROGETTO FORMATIVO
La sicurezza informatica

Soggetto Proponente

Ragione sociale	Abissi Srl
Sede legale - Indirizzo	Via Togliatti 78 – Sestu (CA)
Telefono	+39 070 22079
Fax	+39 070 7961511
Responsabile legale e Referente aziendale	Luca Savoldi
Indirizzo mail	luca.savoldi@abissi.eu
Sede operativa e della borsa di formazione	Pula – Parco scientifico e tecnologico
Indirizzo	Loc. Piscinamanna – 09010 Pula (CA)
Telefono	+39 070 22079
Sito Internet	www.abissi.eu
Tutor aziendale	Luca Savoldi
Indirizzo mail	luca.savoldi@abissi.eu
Telefono	+39 070 22079

1.OBIETTIVI DEL PROGETTO FORMATIVO

La figura che si intende formare è un Esperto di Sicurezza Informatica sia in termini generali che sicurezza intesa come sicurezza di rete e sicurezza applicativa.
In dettaglio, al termine dei 12 mesi di percorso formativo, il borsista avrà acquisito delle competenze relative alle più importanti best practice e standard internazionali per l'IT Risk & Security Assessment, Compliance and Governance. Ad esempio approfondirà il NIST 800-30 (Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology) lo standard OWASP, Application Security Verification Standard, integrato con metodologie proprietarie di Abissi.
Inoltre avrà familiarità con metodi di Penetration test (quali ad esempio l'Open Source Security Testing Methodology) ed avrà sviluppato competenze in reportistica tecnica. Inoltrè conoscerà le maggiori vulnerabilità informatiche a cui sono esposte le infrastrutture critiche, le Apps e più recentemente le reti di Internet of things. Completano il quadro la conoscenza delle soluzioni di Fraud Management, SOC/SIEM, I&AM, Data Security&Protection, Tokenisation, Encryption, PKI, ecc.

2. COMPETENZE DI BASE RICHIESTE

Il candidato deve essere in possesso di una laurea in Informatica, Ingegneria informatica, Ingegneria elettronica, Matematica, Fisica o materie similari.
Verrà considerata alternativa alla laurea un'esperienza pregressa di minimo 2 anni in almeno uno dei seguenti contesti:
- Sviluppo software con almeno due dei seguenti linguaggi di programmazione/scripting: - Shell script, Perl, Python, Ruby, Lua, asm, C, C++, Java, C#, JavaScript, SQL, Go, Swift.
- System Networking Administrator.
- IT System Administrator con approfondimento dei diversi sistemi operativi.

Costituiscono titolo preferenziale:
- Esperienze pregresse nei seguenti ambiti: Vulnerability Assessment, Penetration Testing, Web Application Penetration Testing, Exploit Development, Malware Analysis, Wireless Assessment, Development, System Administration.
- Conoscenza dei principali software di sicurezza informatica: nmap, Nessus, Metaspoit, BurpSuite, SQLMap, Beef, IDA, WinDBG, ImmunityDBG, AirCrack, Wireshark.

E' obbligatoria la conoscenza della lingua inglese parlata e scritta di almeno livello B1 ed è richiesta una grande passione e curiosità per la sicurezza informatica.

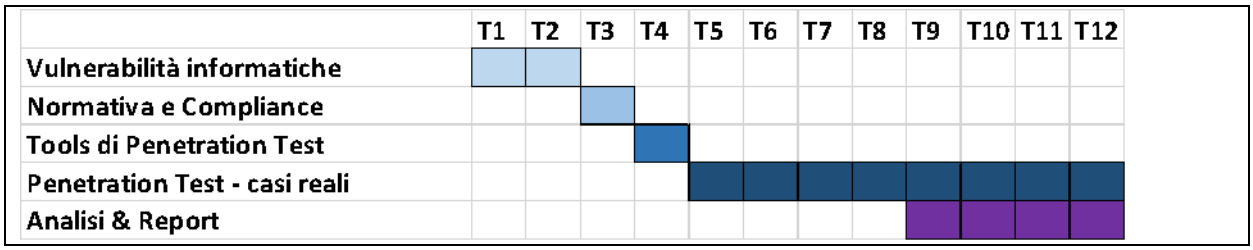
3.INDIVIDUAZIONE DEL CONTESTO LAVORATIVO E SPENDIBILITÀ DELLE COMPETENZE ACQUISITE E IN FUNZIONE DEL CONTESTO

I danni da Cyber Threat sono aumentati di oltre il 300% negli ultimi 24 mesi e le spese delle aziende per la sicurezza informativa sono aumentate mediamente del 25% per anno. Questi pochi numeri spiegano per quale motivo le richieste di esperti di Cybersecurity sono aumentate esponenzialmente negli ultimi anni.
Gli esperti di Cybersecurity sono attualmente molto richiesti da aziende come Abissi, cioè aziende che vendono servizi di sicurezza informatica a clienti quali Alitalia, Magneti Marelli, BNP, oppure direttamente da aziende di grandi dimensioni quali ad esempio Tiscali o Saras oppure la Pubblica Amministrazione. In quest'ultimo tipo di azienda vengono assunti per la gestione della sicurezza informatica, infatti recentemente la Commissione Europea ha obbligato le aziende di questo tipo a dotarsi di questa figura in azienda.
E' importante inoltre notare, che a fronte di una richiesta così alta, non esistono a tutt'oggi corsi di laurea o postlaurea specialisti per questo settore, per cui la formazione è fatta in azienda ed eventualmente con le certificazioni del settore.

4.MODALITA' DI ATTUAZIONE DEL PROGETTO FORMATIVO

La formazione sarà prevalentemente on the job in affiancamento con il personale di Abissi (sia nel laboratorio di Pula che in quello di Sestu, più eventuali visite dal cliente) e qualora ce ne fosse l'opportunità e l'esigenza si provvederà a selezionare opportuni corsi o eventi attinenti all'attività del borsista. In particolare si valuterà l'opportunità di procedere con le seguenti certificazioni OSSTMM Professional Security Tester (OPST), OSSTMM Professional Security Analyst Accredited Certification altamente qualificanti per le attività di cyber security.
Il percorso formativo della durata di circa un anno prevede che il borsista introdotto nel team di lavoro maturi le prime conoscenze di base relative alle maggiori e più frequenti vulnerabilità informatiche sia relative alle infrastrutture critiche, che alle App che a nuovi domini applicativi quali quello dell'Automotive e dell'Internet of things. Per meglio comprendere ed analizzare la problematica, oltre al mero studio, al borsista verranno sottoposti dei casi reali provenienti dalle richieste dei clienti di Abissi. Questa attività ha una durata stimata di 2 mesi.
In seguito per circa 1 mese l'attività del borsista di concentrerà su normativa di riferimento e compliance, anche in questo caso sempre partendo da casi reali ed affiancato dal team. Dopo questa prima fase più di studio, della durata di circa 3 mesi, inizierà la parte più pratica, in particolare con l'applicazione delle varie metodologie di penetration test, sia quelle più conosciute a livello internazionale sia quelle sviluppate da Abissi stessa. Questa seconda fase della durata totale di 9 mesi si svilupperà il primo mese (T0+3) con degli esercizi ad hoc di penetration test in modo da prendere dimestichezza con i tool ed affinare le tecniche di analisi dei risultati dei test, mentre i successivi 8 mesi vedranno il borsista impegnato nel testing su casi reali provenienti dalle commesse e dai clienti di Abissi. Inoltre negli ultimi 4 mesi all'attività di testing si aggiungerà quella di reporting, cioè l'analisi dei risultati dei test ottenuti e scrittura della reportistica relativa.

5. Gantt



6. INDICATORI DI MONITORAGGIO

I risultati principali delle attività di cyber security sono riportati sotto forma di report per il cliente che riportano metodo utilizzato, normativa di riferimento, test effettuati ed analisi dei test con suggerimento di eventuali azioni correttivi o policy da applicare.
Il borsista inizierà a fare questo tipo di reportistica a T0+8, questa reportistica verrà considerata come output principale del progetto formativo perché da un lato riassume tutti i vari aspetti della cybersecurity che sono stati approfonditi durante il percorso formativo, dall'altro comprende anche una parte di analisi che consente di capire l'autonomia ed il grado di expertise raggiunto dal borsista. La reportistica letta e valutata dal personale esperto di Abissi, sarà lo strumento principale per evidenziare eventuali carenze formative e/o decidere eventuali approfondimenti o chiarimenti.
Negli ultimi 4 mesi quindi si procederà con una modalità trial and error volta a migliorare la formazione del borsista e a valutare l'efficacia delle attività formative svolte.