RAD S.r.l. via Achille Papa, 30, 20149 MI
info@radsec.it \ radsrl.pec@legalmail.it
P.IVA 10282620961 \ www.radsec.it

1. Introduzione a RAD

RAD S.r.l (RAD) nasce in Italia come start-up nel 2018 con l'obiettivo di focalizzarsi solo sulle tematiche di sicurezza informatica. Nel 2023 entra a far parte del gruppo Wind Tre SpA come società specializzata nella Cyber Security mantenendo l'identità costruita negli anni.

Il metodo di lavoro implementato in questi anni, basato sull'ascolto delle necessità del Cliente e sulla completa trasparenza, ci permette di implementare strategie di lungo periodo basate sulla condivisione degli obiettivi e di diventare la naturale estensione dell'azienda per cui lavoriamo. Il porre l'attenzione sulle reali necessità del Cliente, aiutando a trovare la migliore soluzione per il proprio contesto, ci ha spesso permesso di differenziarci dai competitor e ad instaurare con i nostri clienti rapporti duraturi basati sulla fiducia reciproca.

In questi anni RAD, grazie alla specializzazione dei fondatori e agli investimenti in formazione continua, è riuscita a definire un portfolio completo e competitivo nei principali ambiti della sicurezza informatica (Errore. L'origine riferimento non è stata trovata.). Queste scelte ci permettono di poter gestire le differenti necessità dei Clienti con risorse preparate e competenti nei diversi ambiti della sicurezza informatica.

Figura 1 - Portfolio RAD

THE CULTURE OF CYBER SECURITY

RAD S.r.l. via Achille Papa, 30, 20149 MI
info@radsec.it \ radsrl.pec@legalmail.it
P.IVA 10282620961 \ www.radsec.it

RAD ha tre modalità di affrontare il mondo della sicurezza, che diventano poi un circolo virtuoso per approcciare a questo vertical. Siamo un'azienda specializzata nel mondo della sicurezza informatica ed attraverso la CONSULENZA supportiamo i nostri clienti nella definizione della strategia Cyber più idonea al loro contesto e al loro business costruendo un vero e proprio percorso con la definizione di priorità utili per raggiungere il grado di maturità necessario per ridurre il rischio. A questo, affianchiamo le nostre competenze sulle tecnologie di mercato, occupandoci della parte di SYSTEM INTEGRATION delle soluzioni all'interno dell'ecosistema del cliente e spingendo le tecnologie ai loro limiti. Abbiamo diverse partnership con i principali e migliori vendor di settore.
Grazie all'esperienza sviluppata nel corso degli anni nell'ambito consulenziale e come system integrator oggi siamo in grado di dare supporto continuativo alle tecnologie che implementiamo o già presenti sul cliente offrendo SERVIZI GESTITI H24,

Abbiamo sviluppato competenze verticali e approfondite su partner e su una gamma selezionata di prodotti. Ci siamo specializzati attraverso certificazioni, sia in ambito tecnologico che commerciale. Di seguito viene riportata una mappatura delle nostre principali partnerhip suddivise per area:

THE CULTURE OF CYBER SECURITY

RAD S.r.l. via Achille Papa, 30, 20149 MI
info@radsec.it \ radsrl.pec@legalmail.it
P.IVA 10282620961 \ www.radsec.it

Di seguito è riportato un dettaglio dei nostri Competence Center:

Cyber Security Protection & Monitoring

Le aziende negli ultimi anni hanno investito molto e continuano ad investire nel perimetro della Cyber Security.

La maggior parte degli investimenti sono stati fatti in tool sempre più complessi e in tecnologie di sicurezza che agiscono su specifici perimetri ed attacchi; il proliferare di questi diversi tool presenta la necessità di strutturare multi dimensionalmente un monitoraggio efficace che tenga conto da un lato delle diverse tecnologie da integrare, dall'altro della complessità di gestione di allarmi che tali tecnologie possono generare.

Questo competence center in RAD agisce da ingegneria SOC portando avanti progettualità in ambito costruzione e definizione SOC e miglioramento delle infrastrutture di monitoraggio e gestione degli incidenti. Le persone all'interno di questo team gestiscono anche l'ingegneria interna del servizio SOC as a Service e coordinano gli analisti che nel quotidiano gestiscono gli incidenti presso i nostri clienti.

Se entrerai a far parte di questo team:

- Lavorerai sulle tecnologie SIEM per collezionare eventi da varie sorgenti e scriverai delle regole di detection per rilevare attività sospette
- Lavorerai su tecnologie SOAR per implementare automazioni atte alla gestione degli incidenti e la response ad essi
- Gestirai tecnologie Next Generation Antivirus ed Endpoint Detection & Response per proteggere al meglio gli endpoint di tutti i tipi
- Resterai continuamente aggiornato sulle principali tecniche di attacco utilizzate dagli attaccanti per essere sempre un passo avanti al loro

Incident Response

Il rischio è sempre basato sull'impatto, ma anche legato alla probabilità: se qualcosa può succedere, prima o poi accadrà ed al giorno d'oggi essere vittime di un attacco informatico ha una reale ed alta probabilità.

Nonostante subire un attacco, in alcune circostanze, possa diventare inevitabile, bisogna sempre considerare l'importanza delle misure di risposta e gestione dello stesso, è necessario focalizzarsi su come reagire, con quali strumenti e attraverso quali metodologie e processi;l'Incident Response è il processo organizzato e coordinato per identificare, contenere, mitigare e risolvere gli incidenti di sicurezza al fine di ridurre al minimo l'impatto sui sistemi e sui dati aziendali.

Se entrerai a far parte del competence center di Incident Response:

- Analizzerai e contestualizzerai gli incidenti identificati dal CSIRT e/o SOC e lavorerai su attacchi critici che impattano l'operatività dei nostri clienti, sfruttando anche sorgenti di Cyber Threat Intelligence.

RAD S.r.l. via Achille Papa, 30, 20149 MI
info@radsec.it \ radsrl.pec@legalmail.it
P.IVA 10282620961 \ www.radsec.it

- Svolgerai attività di analisi degli incidenti di cyber security effettuando analisi sulle piattaforme dei nostri clienti correlando opportunamente le informazioni.
- Lavorerai alla definizione di Emergency Response Plan
- Cercherai di attivare tutte le azioni di rimedio per riportare i nostri clienti up & running
- Lavorerai al continuous improvement dei processi di risposta agli incidenti tramite l'applicazione di lesson learned definite nell'ambito delle attività di post-mortem analysis.

Cyber Threat Intelligence

Il vero valore ai nostri tempi sono le informazioni: in un mondo sempre più iper-connesso e dove ogni evento lascia una traccia, le strategie militari ci insegnano quanto importante e di valore possano essere le informazioni di intelligence, in quanto avere le giuste informazioni risulta fondamentale per prevenire ed evitare un attacco.

Molti tipi di intelligence hanno preso forma negli ultimi anni, soprattutto a causa dei nuovi mezzi di comunicazione, tra di essi spicca la Cyber Threat Intelligence (CTI), ovvero la raccolta, analisi e condivisione di informazioni riguardanti minacce informatiche con l'obiettivo di migliorare la sicurezza e la capacità di risposta di un'organizzazione. Le informazioni raccolte riguardano gli attacchi informatici, i loro metodi, le tecniche, le tattiche utilizzate dagli aggressori, nonché gli indicatori di compromissione (IoC).

Avere a disposizione le informazioni giuste derivanti da sorgenti accreditate e affidabili, sia di tipo aperto (OSINT) che privato (CLOSINT) fa la differenza tra analizzare gli impatti di un attacco ed evitarlo completamente.

Se entrerai a far parte del nostro team di Cyber Threat Intelligence:

- Approfondirai, contestualizzerai e lavorerai alerts di Cyber Threat Intelligence riguardanti i nostri clienti attraverso l'utilizzo di MIIST, la piattaforma di Cyber Threat Intelligence di RAD.
- Riprodurrai le vulnerabilità critiche che vengono scoperte per fornire le azioni di remediation e detection ai nostri clienti.
- Utilizzerai strumenti open source e proprietari per trasformare i dati grezzi trovati nel deep & dark web in informazioni utili fruibili dal SOC e dal team di Detection Engineering.
- Produrrai report su Threat Actors e minacce emergenti che potrebbero avere un impatto sui clienti attraverso l'utilizzo di framework specifici come il MITRE ATT&CK ed il Diamond Model.
- Sfrutterai linguaggi di scripting come Python per automatizzare i processi e migliorare l'efficienza.

Cyber Threat Identification & Simulation

La pluriennale, e riconosciuta, esperienza del personale RAD in ambito Blue Team si fonde con le conoscenze di personale altamente specializzato in ambito Red Team per fornire ai propri clienti un approccio integrato, multidisciplinare e multi-tecnologico per gli assessment e la messa in sicurezza della propria infrastruttura. Le metodologie e gli approcci seguiti

RAD S.r.l. via Achille Papa, 30, 20149 MI
info@radsec.it \ radsrl.pec@legalmail.it
P.IVA 10282620961 \ www.radsec.it

consentono di massimizzare i benefici per il cliente a fronte di una ottimizzazione dei costi e dell'impegno necessario nel traguardare gli obiettivi di sicurezza prefissati.

RAD, infatti, non si limita ad effettuare un'assessment di sicurezza, ma offre una strategia completa che parte dall'identificazione dei possibili attaccanti, dei loro possibili obiettivi e delle strategie, o attack path tenendo in forte considerazione le peculiarità, i perimetri e i punti di forza di ciascun cliente.

Il valore di questo approccio sta nel poter prioritizzare le attività di remediation e hardening sui punti infrastrutturali più esposti o deboli ed è reso possibile dalle competenze che permettono al personale RAD di immedesimarsi sia negli attaccanti che nei difensori e di sfruttarne entrambi i punti di vista per massimizzare il risultato ottenuto.

Se entri a far parte dei "nostri hacker":

- Lavorerai attivamente per scoprire le vulnerabilità note e non note sul perimetro dei nostri clienti
- Supporterai gli sviluppatori nell'implementazione di codice sicuro
- Supporterai i nostri clienti nell'implementare le opportune misure di sicurezza, contestualizzandola con gli occhi dell'attaccante

Cloud & Container Security

Negli ultimi anni, l'adozione del cloud e delle tecnologie container è cresciuta esponenzialmente, spingendo le aziende a ridefinire le loro strategie di sicurezza per proteggere questi nuovi ambienti dinamici e scalabili. La sicurezza dei workload distribuiti su piattaforme cloud, insieme alla protezione dei container, richiede un approccio diverso rispetto alle tradizionali soluzioni di sicurezza on-premise, in quanto la natura effimera e altamente orchestrata di questi ambienti introduce nuove sfide.

Il Competence Center "Cloud & Container Security" in RAD si concentra sulla progettazione, implementazione e ottimizzazione di soluzioni di sicurezza cloud-native, capaci di proteggere ambienti multi-cloud e infrastrutture basate su container. Il nostro team si specializza nell'integrazione di soluzioni di Cloud Native Application Protection, Cloud Identity Security e Cloud Secure Access, fornendo visibilità, controllo e compliance su tutte le tipologie di servizi.

Le nostre attività comprendono la gestione dei rischi legati alla configurazione del cloud, la protezione dei dati e delle identità, il monitoraggio dei servizi per l'identificazione e la risposta a minacce, l'implementazione di soluzioni di runtime security per garantire la sicurezza delle applicazioni anche durante l'esecuzione.

Se entrerai a far parte di questo team:

- Lavorerai su tecnologie di sicurezza cloud-native per proteggere le infrastrutture, le identità e i dati di cloud pubblici, privati e ibridi
- Implementerai soluzioni di sicurezza per container e orchestratori come Kubernetes, con focus sulla gestione delle vulnerabilità e la protezione a runtime

RAD S.r.l. via Achille Papa, 30, 20149 MI
info@radsec.it \ radsrl.pec@legalmail.it
P.IVA 10282620961 \ www.radsec.it

- Collaborerai con i team di sviluppo e DevOps per assicurare che le best practice di DevSecOps siano integrate nei processi di sviluppo del software
- Sarai coinvolto nella configurazione e nel monitoraggio delle policy di sicurezza per garantire la compliance con i principali standard di sicurezza del cloud e normativi

Digital Identity

Il processo di trasformazione digitale insiste in primis sulle identità digitali e la tematica Identity & Access Management non è più esclusivamente una preoccupazione dei CISO ma, al contrario, impatta l'intera azienda sia da un punto di vista normativo (GDPR, PCI, ecc.), che a livello di opportunità e necessità di business. Sempre di più le aziende sfruttano risorse esterne, applicazioni SaaS e piattaforme IaaS per eseguire il proprio lavoro. Tutte queste nuove risorse cloud richiedono alle aziende una gestione, un controllo ed un governo adeguato dei privilegi e degli accessi che la propria forza lavoro dispone in relazione alle risorse aziendali. Considerando inoltre la maggiore esposizione alle minacce che le applicazioni e i servizi cloud hanno rispetto alle risorse on-premise, per le aziende è ancora più importante garantire l'applicazione di pratiche di sicurezza – in termini di visibilità, gestione, protezione e governo – necessarie a mitigare i rischi.

Inoltre, le esigenze di sicurezza descritte, i continui attacchi informatici ai quali le aziende sono esposte – che hanno l'obiettivo di entrare in possesso di dati ed informazioni critiche per il business – nonché gli episodi di esfiltrazione di dati messi in atto anche dal personale interno delle aziende, hanno portato alla definizione di leggi e normative sempre più stringenti in termini di sicurezza. Tali regolamentazioni impongono alle aziende di mettere in atto tutte le contromisure di sicurezza necessarie alla mitigazione dei rischi derivanti dall'accesso incontrollato e non autorizzato a dati e risorse sensibili.

Tutto questo rende necessario un drastico cambio di approccio spostando il focus delle strategie di sicurezza. Se prima infatti molti elementi delle strategie di sicurezza si fondavano in qualche modo sul concetto di perimetro aziendale, oggi questo approccio non può più essere valido. Il nuovo punto centrale dei programmi di sicurezza che le aziende devono mettere in atto è l'identità.

Se entrerai a far parte dei nostri "lammer":

- Lavorerai sulla definizione dei processi riguardanti l'identità digitale e la loro digitalizzazione
- Implementerai i processi e le logiche di gestione delle identità e degli account digitali
- Proteggerai le identità privilegiate dei nostri clienti utilizzando tecnologie ad-hoc
- Lavorerai nella definizione delle strategie di autenticazione ai sistemi

Data Protection

RAD offre una varietà completa di servizi e soluzioni con lo scopo di proteggere i dati ed al contempo assicurare un adeguato livello di accesso. Crediamo che una strategia di sicurezza dei dati efficace ed efficiente necessiti lo sviluppo di un approccio data-centrico: ovunque si trovano i dati, a prescindere da chi li utilizza e indipendentemente dalla modalità con cui questi vengono condivisi.

RAD S.r.l. via Achille Papa, 30, 20149 MI
info@radsec.it \ radsrl.pec@legalmail.it
P.IVA 10282620961 \ www.radsec.it

Le iniziative progettuali a cui abbiamo preso parte, nonché il costante studio delle evoluzioni di questo settore, ci hanno consentito di constatare che la protezione del dato è una tematica fortemente collegata a quella delle identità. Per poter applicare delle politiche di sicurezza che siano efficaci ma che al contempo non ostacolino l'operatività dell'azienda, è fondamentale – come nella gestione delle identità – tenere in considerazione il contesto aziendale di ciò che deve essere in qualche misura protetto.

A questo proposito, per entrambe le tematiche abbiamo adottato un approccio comune incentrato sui processi di business inerenti ai dati stessi; un certo dato infatti, è rilevante per un determinato soggetto (identità) o per uno specifico processo di business.

Ciò è ancora più vero oggigiorno, in virtù del fatto che le aziende si trovano a dover fronteggiare esigenze di sicurezza in un contesto senza perimetri, derivante sia dalla maggiore adozione di soluzioni cloud che dall'impiego diffuso di forza lavoro remota. Da un lato, infatti, le aziende stanno sempre più spingendo per l'impiego di applicazioni SaaS o, più in generale, di servizi cloud, dall'altro devono consentire alla propria forza lavoro (dipendenti, consulenti esterni e partner), di lavorare da qualsiasi parte del mondo senza compromettere la produttività.

Se entrerai a far parte del team di Data Protection:

- Aiuterai i nostri clienti nel definire strategie di protezione dei dati
- Definirai le strategie in ambito classificazione, discovery e governo dei dati
- Supporterai i clienti all'aderenza normativa in ambito gestione del dato

Fraud Detection, Prevention & Response

La continua evoluzione di scenari di attacco complessi in ambito antifrode, è una delle minacce più serie che le aziende devono fronteggiare oggi.

Inizialmente, le frodi online si sono concentrate sulle transazioni finanziarie e sulle operazioni di login, e coinvolgevano principalmente le banche ed il commercio digitale.

Oggi, queste industrie necessitano di strategie antifrode innovative, per aumentare la loro capacità di identificazione delle frodi, ottimizzare gli strumenti e la forza lavoro a disposizione, e per migliorare l'esperienza utente.

Tuttavia, le tipologie di attacchi fraudolenti si sono moltiplicate ed evolute, ed ora comprendono una gamma molto più ampia di casi d'uso che impattano diverse tipologie di business, sia in ambito finanziario che non, come le frodi legate alla creazione di identità sintetiche o all'erogazione di bonus e promozioni da parte delle aziende (bonus/promotion abuse, proprie del mondo e-commerce).

Migliorare i tassi di frode, ridurre al minimo i falsi positivi, migliorare l'esperienza utente, rispettare la compliance e minimizzare i costi sono tutti fattori da bilanciare quando si sviluppa una strategia antifrode.

RAD, attraverso il suo competence center di Fraud Prevention, Detection & Response, supporta i suoi clienti nella definizione, valutazione, sviluppo e manutenzione delle strategie

RAD S.r.l. via Achille Papa, 30, 20149 MI
info@radsec.it \ radsrl.pec@legalmail.it
P.IVA 10282620961 \ www.radsec.it

e delle soluzioni antifrode, adottando un approcciando omnicomprensivo, che tiene conto delle tendenze e degli scenari attuali, con focus su tecnologie e processi.

Se entrerai a far parte del team:

- Supporterai i nostri clienti nella definizione e della gestione delle strategie antifrode
- Aiuterai i nostri clienti a minimizzare l'esposizione alle frodi
- Lavorerai con tecnologie innovative in ambito Transaction Monitoring, Behavioural Analysis, Fraud and Mule Intelligence, Brand Abuse e Digital Trust
- Aiuterai i nostri clienti a rispettare i requisiti di sicurezza imposti da normative e direttive di settore