dotforce
Your Source for Innovative Cybertech

Portfolio tecnologico
Ottobre 2020

Web Application Security
Web Vulnerability Management

Acunetix Web Vulnerability Scanner effettua scansioni automatiche su siti web standard e personalizzati, identificando le vulnerabilità delle applicazioni verso attacchi di tipo SQL Injection, XSS (Cross-Site Scripting), XXE, SSRF, Host Header e scoprendo altri 500 tipi diversi di vulnerabilità. Il prodotto è disponibile sia in modalità On Premise (Acunetix Standard e Premium) sia in versione On Premise / Cloud (Acunetix360).

- **Acunetix Standard** è uno scanner di vulnerabilità del web, che testa automaticamente il tuo sito Web per vedere se può essere hackerato. Lo scanner esegue in modo sicuro attacchi simulati, mostra come un hacker malintenzionato potrebbe potenzialmente accedere ai tuoi sistemi e spiega come prevenire attacchi reali. Questo è il modo migliore per proteggerti dalle comuni minacce web.

- **Acunetix Premium** si rivolge principalmente alle organizzazioni medio-grandi che devono proteggere un gran numero di siti e applicazioni Web, o che desiderano incorporare la Web Security nelle loro DevOps.

- **Acunetix 360** è una soluzione Cloud-based di Web Vulnerability Assessment & Management, progettata per far parte di qualsiasi ambiente aziendale fornendo integrazioni multiple e opzioni per l'integrazione in contesti personalizzati. E' disponibile anche On Premise (Linux-based)

Secure Email Cloud

Agari utilizza l'AI predittiva per modellare l'identità su scala Internet e prevenire il prossimo attacco zero-day. Concentrandosi sull'identità del mittente e sul comportamento rispetto al tipo di attacco stesso, Agari modella il buono per proteggerti dal male, assicurando che nessuna minaccia, nuova o esistente, arrivi nella tua casella di posta.

- **Agari Phishing Defense™**
  Ferma minacce sofisticate di identity deception tra cui BEC (business email compromise), executive spoofing, e account takeover.

- **Agari Phishing Response™**
  Accelera il triage di episodi di phishing, e l'attività di forensics, remediation, breach containment per i Security Operations Center (SOC).

- **Agari Brand Protection™**
  Automatizza l'autenticazione e l'enforcement delle e-mail con DMARC, per prevenire gli abusi dei brand aziendali, proteggendo i clienti da costosi e insidiosi attacchi email.

Agari Identity Graph™
Agari Identity Graph è un database grafico ad alte prestazioni di relazioni e modelli comportamentali tra individui, marchi, aziende, servizi e domini che utilizza centinaia di caratteristiche per definire comunicazioni affidabili.

DDoS Mitigation

Corero Network Security si dedica al miglioramento della sicurezza e della disponibilità di Internet, attraverso lo sviluppo di soluzioni innovative di mitigazione DDoS.

E' un'azienda leader nella protezione dagli attacchi DDoS automatici in tempo reale ad alte prestazioni, con visibilità, analisi e reportistica completi degli attacchi. Le soluzioni sono di tipo On Premise, Cloud oppure ibride, e proteggono migliaia di organizzazioni che operano in diverse tipologie di settore merceologico in tutto il mondo.

La famiglia di soluzioni Corero SmartWall® Threat Defense System (TDS) utilizza la moderna architettura di mitigazione DDoS per rimuovere automaticamente e chirurgicamente il traffico di attacchi DDoS, consentendo allo stesso tempo in modo ininterrotto il flusso legittimo di traffico di rete verso gli utenti.

DOMAINTOOLS **Threat Intelligence & Hunting, WHOIS**	**DomainTools** aiuta gli analisti della sicurezza a trasformare i dati delle minacce in informazioni. La soluzione utilizza gli indicatori di rete, compresi domini e IP, collegandoli con quasi tutti i domini attivi su Internet. Queste connessioni informano le valutazioni dei rischi, aiutano a profilare gli aggressori, guidano le indagini sulle frodi online e mappano l'attività di cyber sull'infrastruttura degli attaccanti. L'obiettivo è fermare le minacce alla sicurezza delle aziende prima che si verifichino, utilizzando dati dominio/DNS, analisi predittiva e monitoraggio delle tendenze su Internet. Vengono raccolti dati OSINT (Open Source Intelligence) da molte fonti, insieme a record storici, in un database centrale. I dati sono analizzati in base a vari algoritmi di connessione per fornire informazioni utili, tra cui il punteggio del dominio e la mappatura legale. DomainTools ha oltre 10 miliardi di punti di dati DNS correlati per costruire una mappa di "chi sta facendo cosa" su Internet. Le aziende Fortune 1000, le agenzie governative globali e i principali fornitori di soluzioni per la sicurezza utilizzano DomainTools come strumento critico nel loro lavoro di indagine e mitigazione delle minacce.

edgescan™ **Full Stack Vulnerability Management (DAST)**	Edgescan è stata fondata nel 2011 per affrontare il problema della (in)sicurezza dei sistemi, rimanendo al passo con i rapidi sviluppi e cambiamenti degli stessi. Utilizzando le ultime tecnologie, Edgescan fornisce una gestione delle vulnerabilità ad alto livello abbinata a una esperta validazione manuale per ogni vulnerabilità. Grazie a una verifica e validazione manuale a cura di esperti, il contesto di ciascuna vulnerabilità viene preso in considerazione quando viene valutato in base al rischio, per garantire che il rischio potenziale per ciascuna organizzazione sia compreso completamente. Edgescan è una delle poche società di sicurezza informatica che consente alle aziende di proteggere e essere proattive nella difesa delle proprie attività digitali. Dallo sviluppo di applicazioni e host alla distribuzione in produzione, dal desktop all'API al cloud ai dispositivi mobili, proteggiamo le applicazioni e l'infrastruttura Web su cui le persone fanno affidamento nella loro vita personale e professionale. Per Edgescan, questo si chiama Vulnerability Intelligence.

Faronics™ **Multilayer Endpoint Protection**	La suite di prodotti Faronics garantisce la disponibilità al 100% di ogni workstation e libera i team IT dai problemi legati al supporto tecnico del software. Di casa negli ambienti Education con Deep Freeze, Faronics è un vendor molto apprezzato anche in ambito Enterprise. • Faronics Deep Freeze riduce i costi IT preservando le configurazioni ideali dei computer su cui viene implementato. • Faronics Anti-Executable impedisce l'utilizzo di software non autorizzato • Faronics Anti-Virus garantisce protezione dal malware. • Faronics Power Save aiuta a ridurre i costi energetici. • Faronics Insight offre il controllo totale sui computer delle aule informatiche, e • Faronics WINSelect consente agli amministratori IT di personalizzare l'accesso alle applicazioni, a siti web, programmi e opzioni di Windows.

Fidelis™ Cybersecurity **NDR, EDR, Deception**	Fidelis Cybersecurity è stata fondata da cyber warrior e continua oggi questa ricca eredità. I nostri cyber warrior sono incident responder, operatori SOC, analisti di intelligence e threat hunter, provenienti dal DoD e dalle comunità Intel statunitensi, nonché dall'industria. Il nostro team ha creato alcuni degli ambienti più sicuri ed è stato chiamato nel post-violazione per guidare i programmi di risposta agli incidenti per alcune delle più grandi violazioni di dati mai registrate. La nostra piattaforma fornisce ai cyber warrior la capacità di operare all'interno del ciclo decisionale dell'avversario e rilevare e rispondere alle minacce avanzate alla velocità della linea. Fidelis ti aiuta a superare, superare in astuzia e sconfiggere gli attacchi informatici in ogni fase per mantenere al sicuro le tue operazioni aziendali ei tuoi dati. Le imprese sono svantaggiate rispetto ai loro avversari informatici. Le minacce provengono da ogni angolazione e molte organizzazioni non hanno una visibilità completa del proprio terreno informatico, consentendo agli aggressori informatici di nascondersi inosservati mentre prendono di mira dati sensibili o cercano di interrompere le operazioni aziendali. Per ottenere il vantaggio decisivo, i team di sicurezza devono pensare come il loro avversario. Ciò significa avere una maggiore visibilità tra i diversi livelli all'interno del loro ambiente, nonché l'automazione per scalare le capacità di rilevamento e risposta.

FUDO SECURITY Privileged Account Management	La nostra competenza nella sicurezza è confermata da anni di esperienza, centinaia di clienti soddisfatti e un canale di distribuzione globale. La nostra missione è progettare le soluzioni più amichevoli e affidabili per armare le organizzazioni contro l'abuso dei privilegi. I nostri prodotti ti consentono di monitorare l'attività degli utenti con accesso ad asset critici, ti aiutano a gestire la policy sulle password e ti avvisano in caso di comportamenti sospetti. Ogni azienda dovrebbe permettersi di essere sicura. Ecco perché la nostra offerta è su misura per le tue esigenze. Per i giocatori in crescita offriamo una versione gratuita della nostra soluzione: questo è il nostro impegno per rendere ogni azienda più sicura. Le più avanzate soluzioni di accesso privilegiato. Distribuito in 1 giorno. Con il miglior supporto disponibile. Punto.
iStorage® Flash/SSD/HD Encrypted Drive	I dispositivi con encryption hardware di Istorage assicurano grande portatilità dei dati più preziosi, uniti all'estrema sicurezza offerta dai sistemi di autenticazione e cifratura in essi integrati. Utilizzano encryption AES a 256 bit per garantire l'assoluta riservatezza dei dati. I Drive della serie PRO sono certificati FIPS 140-2 livello2. Le loro notevoli capacità li rendono un complemento ideale per garantire il trasporto di notevoli quantità di dati, con la velocità offerta da USB3 e SSD.
netsparker Web Application Security	Netsparker, la soluzione per la sicurezza delle applicazioni web che verifica automaticamente le vulnerabilità identificate, è stata rilasciata per la prima volta sul mercato nel 2009. Il segreto della straordinaria precisione di Netsparker è la sua tecnologia proprietaria di scansione Proof-Based. Quando Netsparker è stato rilasciato per la prima volta, i veterani del settore e i fornitori erano scettici sull'affermazione estremamente accurata; sostenendo che non è possibile costruire uno scanner con la massima precisione. Netsparker ha dimostrato che il settore si sbagliava con una soluzione che è in grado di verificare i risultati senza sacrificare la copertura e continua a ottenere il più alto tasso di rilevamento delle vulnerabilità e accuratezza nei confronti di terze parti. Oggi, Netsparker è cresciuto fino a diventare una soluzione di sicurezza delle applicazioni web leader del settore. Consentire ai team di integrarsi con CI / CD e altri sistemi nell'ambiente SDLC e DevOps. Inoltre, consente flussi di lavoro completamente personalizzabili in cui le valutazioni delle vulnerabilità, i processi di triage e verifica sono tutti automatizzati.
netwrix Auditing, Governance, GDPR	Netwrix Auditor è una piattaforma di visibilità e di governance che permette il controllo su modifiche, configurazioni e l'accesso in ambienti IT di cloud ibrido, per proteggere i dati indipendentemente dalla loro posizione. A differenza di software di controllo IT tradizionale, la piattaforma fornisce analisi di sicurezza per rilevare anomalie nel comportamento degli utenti e indagare i modelli di minaccia prima che si verifichi una violazione dei dati. Netwrix Auditor è in grado di rilevare minacce alla sicurezza dei dati fornendo analisi di sicurezza sui cambiamenti critici, le configurazioni e l'accesso ai dati stessi.
onelogin Identity & Access Management	Il passaggio al cloud offre risparmi, infrastrutture ridotte e migliore usabilità. Ma anche un'azienda ibrida presenta delle sfide: la frammentazione dell'IT mentre le organizzazioni cercano di gestire le app in ambienti cloud locali e multipli. L'approccio più diffuso richiede più sistemi **IAM (Identity Access Management)** per diversi ambienti, reti e dispositivi, portando con sé ancora più problemi: maggiore complessità e costi più elevati per l'IT, un'esperienza utente insoddisfacente e un maggiore rischio per la sicurezza. Adesso c'è un modo migliore. La piattaforma **OneLogin UAM (Unified Access Management)** centralizza l'accesso all'interno della tua organizzazione e soddisfa le esigenze in rapida evoluzione della tua azienda ibrida. Ti offre sicurezza, affidabilità e controllo per tutti i tuoi dati, dispositivi e utenti.

perimeter 81 Software Defined Perimeter VPN Alternative	**Perimeter 81** è la seconda iniziativa lanciata nel 2018 da due esperti di sicurezza informatica come Amit Bareket e Sagi Gidali. Incontratisi all'Università di Tel Aviv nel 2012, hanno unito le loro forze per fondare SaferVPN, che ora è uno dei marchi VPN più conosciuti al mondo e recentemente è stato acquisito da un conglomerato leader di Internet e dei media. Fin dalla sua fondazione, Perimeter 81 ha rapidamente guadagnato terreno nel mercato del perimetro della rete come servizio definito dal software (Software-Defined Perimeter) e come **alternativa sicura alle tradizionali VPN**, e sta trasformando il modo in cui le aziende consumano la sicurezza della rete. Perimeter 81 è stato nominato Gartner Cool Vendor, ha vinto numerosi premi per la sicurezza informatica e detiene un brevetto per la sicurezza Wi-Fi automatica. La società sta trasformando il mondo dell'accesso sicuro alla rete e aiutando le aziende di tutti i settori e dimensioni a spostarsi in modo sicuro nel cloud e potenziare la loro forza lavoro moderna e mobile. Il team di esperti Perimeter 81 si riunisce ogni giorno per offrire un servizio SaaS veramente innovativo e creare uno sportello unico per le offerte di sicurezza informatica.
Plixer Network Traffic Analysis	Plixer fornisce un sistema di analisi del traffico di rete che supporta la risposta agli incidenti rapida ed efficiente. La soluzione consente di ottenere visibilità sulle applicazioni cloud, sugli eventi di sicurezza e sul traffico di rete. Fornisce dati utilizzabili per guidare l'utente dal rilevamento di eventi di rete e di sicurezza fino all'analisi e alla mitigazione delle cause principali. Gli incidenti di rete e di sicurezza sono inevitabili. Quando si verificano, Plixer è lì per aiutarti a tornare rapidamente alla normalità e ridurre al minimo l'interruzione dell'attività. Migliaia di organizzazioni si affidano alle soluzioni Plixer per mantenere efficiente l'infrastruttura IT. **Scrutinizer** Scrutinizer, il sistema di analisi del traffico di rete di Plixer, raccoglie, analizza, visualizza e genera report sui dati di ogni conversazione di rete e transazione digitale per fornire sicurezza e informazioni di rete. Fornisce le informazioni dettagliate e storiche necessarie per gestire e ottimizzare le operazioni aziendali, riducendo al contempo i rischi rilevando e correggendo gli incidenti. **FlowPro** Le sonde FlowPro supportano la gestione delle prestazioni delle applicazioni e le funzionalità di difesa per il monitoraggio del traffico DNS. Da una singola sonda, le operazioni di rete possono gestire e ottimizzare la rete in modo efficiente, mentre le operazioni di sicurezza sono in grado di ridurre contemporaneamente i rischi, acquisire il contesto dei dati e rispondere rapidamente agli incidenti di sicurezza. **Replicator** Replicator aggrega, replica e distribuisce i metadati di flusso e log esportati dalla rete esistente su più strumenti di monitoraggio come SIEM, syslog e flow collector. Ciò migliora il valore dei dati semplificando notevolmente aggiunte, spostamenti e modifiche e proteggendo la CPU dall'esportazione di switch, router, firewall, ecc.
RAPID7 Vulnerability Management, AppSec, SIEM, SOAR	Rapid7 è un fornitore leader di soluzioni di dati e analisi di sicurezza che consentono alle organizzazioni di implementare un approccio attivo e orientato all'analisi alla sicurezza informatica. La piattaforma di dati e analisi di sicurezza è stata creata appositamente per affrontare e gestire al meglio un ambiente IT sempre più complesso e caotico. Rapid7 combina una vasta esperienza in dati e analisi di sicurezza con una profonda conoscenza dei comportamenti e delle tecniche degli aggressori, per dare un senso alla ricchezza di dati a disposizione delle organizzazioni sui loro ambienti IT e utenti. Le analisi potenti e proprietarie consentono alle organizzazioni di contestualizzare e stabilire la priorità delle minacce che si trovano ad affrontare le loro risorse fisiche, virtuali e cloud, comprese quelle poste dai comportamenti dei loro utenti. Sfruttando la piattaforma di dati e analisi di sicurezza, le soluzioni Rapid7 consentono alle organizzazioni di gestire in modo strategico e dinamico la loro esposizione alla sicurezza informatica. Le nostre soluzioni consentono alle organizzazioni di prevenire gli attacchi fornendo visibilità sulle vulnerabilità e per rilevare rapidamente i compromessi, rispondere alle violazioni e correggere le cause di fondo degli attacchi.

REAQTA NGAV+, Managed Detection & Response	ReaQta è stata fondata da un team d'élite composto da esperti di sicurezza informatica offensiva e difensiva, e da ricercatori di machine learning. Combinando queste diverse competenze, il team Reaqta ha creato una potente piattaforma di intelligence di difesa attiva. La soluzione offre funzionalità avanzate di rilevamento e risposta, senza richiedere personale aggiuntivo o altamente qualificato. Questo approccio innovativo applica gli ultimi algoritmi di Intelligenza Artificiale per automatizzare e semplificare il processo di rilevamento e gestione di nuove minacce. Su questa singola piattaforma di intelligence attiva altamente integrata, i clienti ottengono flessibilità e velocità nell'esecuzione di analisi complesse che erano possibili solo con team di grandi dimensioni e altamente specializzati. È un approccio dinamico che non protegge solo le organizzazioni nel qui e ora, ma anche nel futuro. Con ReaQta, le aziende hanno il potere di perseguire la crescita del loro business senza timore delle minacce informatiche.

Siemplify Next-Gen SOAR Platform	Siemplify nasce dall'esigenza di un modo migliore, più semplice ed efficace per gestire le operazioni di sicurezza. La soluzione è stata costruita daesperti delle operazioni di sicurezza che hanno trascorso anni ad affinare le loro capacità in prima linea nelle agenzie israeliane di cibernetica. I fondatori di Siemplify – Amos Stern, Alon Cohen e Garry Fatakhov – hanno aggiunto a questa esperienza una costante attività di formazione e di miglioramento dei team SOC in tutto il mondo. Il loro background approfondito nella gestione SOC, analisi della sicurezza e scienza dei dati, unito alla conoscenza diretta delle sfide quotidiane dei team di operazioni di sicurezza, ha portato alla creazione della Siemplify Security Operations Platform, la piattaforma indipendente leader del settore SOAR.

SpyCloud Employee Account Takeover	SpyCloud è focalizzato sulla prevenzione delle frodi online con le nostre soluzioni proattive, che proteggono miliardi di account di dipendenti e consumatori in tutto il mondo dall'acquisizione di account. Siamo il partner di fiducia per la prevenzione delle frodi in caso di acquisizione di account per organizzazioni B2B e marchi di consumatori, tra cui 4 di Fortune 10, e indagini sulle frodi per le forze dell'ordine di tutto il mondo. Le nostre soluzioni sono supportate dal repository più completo e utilizzabile di credenziali compromesse e PII recuperati da violazioni di terze parti, con oltre 100 miliardi di risorse e conteggio, comprese oltre 21 miliardi di password.

stealthbits Data Access & AD Governance	STEALTHbits è un'azienda produttrice di software per la sicurezza dei dati. Si focalizza sulla sicurezza delle informazioni aziendali, difendendole dagli abusi delle credenziali e controllando l'accesso ai dati. L'azienda propone tre soluzioni principali: StealthAUDIT – Auditing, compliance, e framework di governance per dati non strutturati e applicazioni critiche; StealthINTERCEPT – Identificazione delle minacce in tempo reale, change monitoring e alerting per infrastrutture Microsoft; StealthDEFEND – Soluzione di analisi del comportamento degli utenti e di identificazione delle minacce.

TitanHQ SpamTitan **AntiSpam Gateway** **Cloud & VA**	Con Clienti in oltre 100 paesi nel mondo, SpamTitan è una delle soluzioni antispam più complete sul mercato per proteggere gli utenti dallo spam e dalle minacce che si trasmettono e propagano via email. SpamTitan utilizza tecnologia allo stato dell'arte per offrire una soluzione facile da implementare e da gestire, ma dalle elevate caratteristiche e funzionalità di sicurezza. La versione On Premise (SpamTitan Gateway) permette di creare una propria email gateway appliance, fisica (ISO) o virtuale (Virtual Machine), offrendo protezione da Virus, Spam, Malware, Phishing e altro contenuto indesiderato. La versione Cloud non necessita di infrastruttura locale, e unisce la sicurezza di SpamTitan alla flessibilità del Cloud. SpamTitan nasce per domini illimitati, ed è quindi ideale per Internet Service Provider che desiderino offrire un servizio AntiSpam affidabile ai loro Clienti.
TitanHQ WebTitan **Web Filtering** **Gateway, Cloud & WiFi**	WebTitan è una soluzione di **web content filtering** avanzata, in grado di offrire protezione da minacce alla sicurezza che si diffondono via HTTP e HTTPS, e controllo evoluto sul **protocollo DNS** per la sicurezza di aziende, organizzazioni educational e Managed Service Provider. Premiata con cinque stelle da SC Magazine, permette alle aziende di proteggere i propri dati ed i propri utenti da malware e altre minacce Internet come virus, spyware, e phishing, e allo stesso tempo, offre strumenti di limitazione e controllo per rendere efficace l'attuazione delle politiche aziendali che riguardano la navigazione Internet. La soluzione è disponibile in modalità On Premise e Cloud. La versione Cloud non necessita di infrastruttura locale, e unisce la sicurezza di WebTitan alla flessibilità del Cloud. **WebTitan for WiFi** permette di implementare il web content filtering sugli Access Point predisposti dai WiFi Service Provider.
yubico **Multifactor Authentication** **FIDO2, WebAuthn**	Yubico cambia le regole del gioco per la strong authentication, offrendo sicurezza di livello superiore insieme a una facilità di utilizzo ineguagliata. Il prodotto principale, la YubiKey, è un piccolo dispositivo USB e NFC che supporta numerosi protocolli crittografici e di autenticazione e che garantisce l'accesso a qualsiasi numero di sistemi IT e servizi online. Con un semplice tocco, la YubiKey protegge l'accesso a computer, reti e servizi online per le più grandi organizzazioni del mondo. Yubico crea standard universali come principale contributore al protocollo aperto di autenticazione a due fattori FIDO Universal. La tecnologia Yubico è apprezzata da milioni di utenti in oltre 160 nazioni. Per proteggere i segreti sui server, Yubico ha creato anche YubiHSM, il modulo di sicurezza hardware più piccolo al mondo. L'azienda offre agli sviluppatori server open source, supporto e servizi di validazione in hosting per una facile integrazione con qualsiasi sistema IT.

dotforce
Your Source for Innovative Cybertech

Via S. Anna 41 | 20090 Vimodrone (MI) | Tel. 02/36735520 | Fax 02/36215698 | www.dotforce.it | info@dotforce.it