dotforce
Your Source for Innovative Cybertech

Portfolio tecnologico

Luglio 2019

acunetix **Web Application Vulnerability**	La sicurezza dei siti web è oggi una priorità in ogni azienda, considerato che gli hacker stanno concentrando i loro sforzi proprio sulle applicazioni web-based (carrelli di e-shopping, moduli web, pagine di login, contenuti dinamici, etc.). Qualsiasi strumento di difesa a livello di sicurezza di rete non potrà offrire protezione alcuna dagli attacchi alle applicazioni web, visto che questi vengono sferrati sulla porta 80 – che deve restare aperta. Oltre a ciò, le applicazioni web sono spesso fatte su misura, e per questo meno testate del software standard, il che le rende maggiormente vulnerabili. **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.
AGARI **Secure Email Cloud**	Ci sono più di quattro miliardi di caselle di posta elettronica nel mondo. Milioni di utenti inviano e ricevono centinaia di miliardi di messaggi ogni giorno. E i cybercriminali ne approfittano, trasformando quelle che dovrebbero essere comunicazioni affidabili in un luogo in cui possono rubare dati sensibili e generare profitti. **Agari** prende posizione contro questi criminali informatici con una missione audace: proteggere le comunicazioni digitali per garantire che l'umanità prevalga sul male. 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.
Centrify **Privileged Access Management**	Da più di dieci anni **Centrify** è riconosciuta come società leader nel mercato dei PAM (Privileged Access Management). Basandosi su queste solide e comprovate fondamenta, Centrify eleva la tecnologia PAM a livelli ancora più alti grazie ai servizi Zero Privilege, pronti per il cloud, riducendo e rendendo più sicura la superficie di attacco in continua espansione delle aziende moderne. **Zero Trust Privilege** ridefinisce il concetto di Privileged Access Management (PAM) adattandolo alle superfici a rischio delle imprese moderne. Le organizzazioni devono scartare il vecchio modello di "fiducia ma verifica", che si basava su confini ben definiti. Zero Trust impone un approccio "non fidarti mai, verifica sempre, garantisci i privilegi minimi necessari" all'accesso privilegiato, dall'interno o dall'esterno della rete. L'approccio Zero Trust Privilege è basato sulla verifica di chi richiede l'accesso, sul contesto della richiesta e sul rischio dell'ambiente di accesso. Implementando l'accesso con privilegi minimi, le organizzazioni riducono la superficie di attacco, migliorano la visibilità di audit e conformità e riducono rischi, complessità e costi per l'azienda ibrida moderna. Oggi, oltre 5.000 imprese in tutto il mondo, tra cui metà delle Fortune 50 e oltre 80 agenzie federali, si affidano a Centrify
CODE42 **Data Leakage Protection**	È tempo di ripensare alla prevenzione della perdita di dati. Le organizzazioni odierne progressiste, incentrate sui dipendenti e ricche di idee sono alla ricerca di nuovi modi meno restrittivi per proteggere i propri dati. Code42 Next-Gen Data Loss Protection è un modo più semplice e veloce per proteggere i dati di endpoint e cloud di un'azienda da perdita, perdita, uso improprio e furto. Nonostante gli sforzi di prevenzione meglio intenzionati, la realtà è che la perdita di dati ad alto valore avviene ogni giorno. Code42 ritiene che ogni file abbia un valore e Code42 Next-Gen Data Loss Protection è progettato per proteggere ogni file. Code42 Next-Gen DLP raccoglie, indicizza e analizza tutti i file e l'attività dei file, offrendo ai nostri clienti piena visibilità ovunque i loro dati vivano e si muovano, dagli endpoint al cloud. Con questo tipo di supervisione, i team di sicurezza possono monitorare, investigare, conservare e ripristinare i dati in modo facile e veloce senza le complesse regole di classificazione e le policy che bloccano la collaborazione e la produttività dei dipendenti. Nativo per il cloud, Code42 Next-Gen DLP funziona senza costosi requisiti hardware e distribuisce in pochi giorni. Oggi oltre 50.000 organizzazioni in tutto il mondo si affidano a Code42 per proteggere i propri dati dalla perdita.

 **Threat Intelligence & Hunting, Domains & 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 la piattaforma DomainTools come ingrediente critico nel loro lavoro di indagine e mitigazione delle minacce.
 **Enterprise Cyber Analytics Real Time Detection**	La rete è l'unica cosa che collega tutte le interazioni digitali. **ExtraHop** ha inventato un modo radicalmente nuovo per osservare e analizzare queste interazioni: l'elaborazione del traffico di rete in tempo reale, che è una fonte di informazioni completa, unica e affidabile per il business, la sicurezza e l'IT. ExtraHop offre visibilità in tempo reale su tutta l'azienda ibrida, traffico cloud e crittografato compreso. ExtraHop trasforma i raw wire data in informazioni strutturate, mentre l'apprendimento automatico consente di scoprire e rispondere a minacce nascoste, con impatto zero sulle prestazioni. ExtraHop è progettato per soddisfare le esigenze di scalabilità dell'impresa ibrida moderna, dal Core al Cloud. La piattaforma Reveal(x) trasforma la rete in una fonte di sicurezza e visibilità IT più completa e oggettiva, fornendo al tempo stesso un ricco set di dati – wire data – che permette un apprendimento automatico focalizzato, preciso e affidabile come nessun altro. Visibilità senza precedenti: l'analisi in tempo reale consente di rilevare e classificare tutte le risorse aziendali, mappare tutte le connessioni e le dipendenze e monitorare il flusso di traffico fino a 100 Gbps (incluse le sessioni crittografate SSL o PFS). Approfondimenti precisi: l'apprendimento automatico avanzato utilizza rivelatori potenti basati sulla riduzione della dimensionalità e sul rilevamento di valori anomali per identificare le anomalie, correlando tali dati con le risorse critiche per far emergere le minacce incombenti. Risposte immediate: Un semplice flusso di lavoro di tipo investigativo stabilisce una causa inequivocabile in pochi secondi (e non giorni), mentre le integrazioni aziendali accelerano e automatizzano la risposta prima che le minacce incidano sulla tua attività.
	Faronics produce software che consente di gestire, semplificare e proteggere gli ambienti di elaborazione multiutente. Garantisce al 100% la disponibilità delle workstation, e libera i team IT da problemi di assistenza 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 la configurazione originaria di PC e Mac. Faronics Anti-Executable impedisce l'utilizzo di software non autorizzato. Faronics Anti-Virus garantisce protezione dal malware. Faronics Insight offre il controllo totale sui computer delle aule informatiche.
	Flexera sta reinventando il modo in cui il software viene acquistato, venduto, gestito e protetto. Le nostre soluzioni di monetizzazione e sicurezza aiutano i venditori di software a trasformare i loro modelli di business, a generare ricavi ricorrenti ea minimizzare il rischio open source. Le soluzioni Vulnerability e Software Asset Management (SAM) eliminano sprechi e imprevedibilità dal software di procurement, aiutando le aziende ad acquistare solo il software e i servizi cloud di cui hanno bisogno, a gestire ciò che hanno e a ridurre i rischi di conformità e sicurezza.

gemalto a Thales company	Gemalto è leader a livello globale nel settore della sicurezza informatica. L'azienda fornisce una sicurezza completa utilizzando proprie tecnologie di crittografia e di strong authentication per proteggere le comunicazioni, la proprietà intellettuale e le identità digitali. L'offerta comprende dispositivi HSM (Hardware Security Module) per la protezione delle chiavi di firma digitale e delle transazioni bancaria, appliance per la cifratura di Database (DB Encryptor) e Reti (Network Encryptor). Gli HSM di Gemalto offrono una protezione affidabile per applicazioni, transazioni, e asset informatici salvaguardando le chiavi crittografiche che risiedono al centro di ogni soluzione basata su encryption.
ImmuniWeb® AI for Application Security	ImmuniWeb è un fornitore globale di test di sicurezza e valutazioni di sicurezza per applicazioni Web e mobili. La piattaforma ImmuniWeb® AI combina il genio dell'intelligenza umana con il potere dell'intelligenza artificiale e dell'apprendimento automatico. La piattaforma AI ImmuniWeb® sfrutta l'apprendimento automatico e l'intelligenza artificiale per l'automazione e l'accelerazione intelligenti di test di penetrazione sensibili alla minaccia. Spinto dall'intelligenza umana, rileva rapidamente anche le vulnerabilità più sofisticate e viene fornito con uno SLA a garanzia di zero falsi positivi.
idaptive	Viviamo in una nuova era. Ci aspettiamo che tutto sia ovunque, all'istante. Il volume di API, servizi cloud, dispositivi e dati che guidano questa trasformazione è estremamente complesso. Allo stesso tempo, la sofisticazione e la portata delle violazioni che minacciano questo nuovo mondo non hanno precedenti. Siamo letteralmente sotto assedio. Nessuna compagnia è immune e quasi tutti restano indietro. Questa nuova realtà richiede un nuovo tipo di piattaforma di accesso. Nata da Centrify e basata su Zero Trust, **Idaptive** sta creando una nuova era – accesso sicuro ovunque – che combina in modo unico funzionalità leader per integrare senza soluzione di continuità Single Sign-on, autenticazione a più fattori, gestione della mobilità aziendale e analisi del comportamento degli utenti.
iStorage®	I flash drive, hard drive e SSD drive cifrati con encryption hardware di **Istorage** assicurano grande portabilità 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 livello 2. Le loro grandi capacità li rendono ideali per garantire il trasporto di notevoli quantità di dati, con tutta la velocità offerta da USB3 e SSD.
Malwarebytes	**Malwarebytes** è la società di sicurezza informatica di ultima generazione, che ha la fiducia di milioni di utenti in tutto il mondo. Malwarebytes protegge in modo proattivo le persone e le aziende contro le minacce pericolose come malware, ransomware, ed exploit che sfuggono al rilevamento dalle soluzioni antivirus tradizionali. **Malwarebytes Endpoint Protection**, prodotto business di punta dell'azienda, combina tecnologie euristiche avanzate di rilevamento delle minacce con tecnologie signature-less, per rilevare e bloccare gli attacchi informatici prima che si verifichi un danno. Più di 10.000 aziende utilizzano in tutto il mondo le soluzioni Malwarebytes con fiducia. **Malwarebytes Endpoint Protection & Response** integra la protezione multivettore con capacità di rilevamento e risposta tramite un unico agente. Garantisce visibilità, riduce il tempo di permanenza delle minacce 0-day e, oltre alle notifiche, offre opzioni di correzione. Endpoint Protection & Response elimina la complessità EDR grazie a monitoraggio, rilevamento e correzione degli endpoint intuitivi.

netwrix	**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 del software tradizionale di controllo IT, 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. 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. Permette inoltre di svolgere analisi del comportamento degli utenti, rilevando attività insolite e sospette. Con Auditor è possibile superare gli Audit di Compliance con minore sforzo e investimento, dimostrando la conformità agli standard PCI DSS, HIPAA, HITECH, SOX, FISMA, GLBA, FERPA, NERC CIP, ISO / IEC 27001 e **soprattutto è di estremo aiuto e utilità per il GDPR**. Grazie alla possibilità di automatizzare operazioni quali change management e reporting, permette una maggiore produttività e precisione all'intero reparto IT aziendale.

NeuraLegion	NexPloit di **Neuralegion** è una soluzione AST potente e flessibile, può essere facilmente utilizzata in un modo che si adatta alle tue esigenze di sicurezza. NexPloit può essere attivato tramite un'interfaccia Web intuitiva o tramite i ganci API, fornendo un'integrazione perfetta nei flussi di lavoro SDLC (CI / CD) che consentono di eseguire rapidamente test di sicurezza DAST / IAST alla velocità di DevOps. NexPloit può essere utilizzato come soluzione di test per la sicurezza delle applicazioni dinamiche direttamente dal cloud, una nuova scansione può essere avviata in pochi minuti, senza integrazione richiesta! NexPloit agirà sulla tua applicazione utilizzando strategie evolutive per generare scenari di attacco dannoso, individuando e riportando immediatamente a quale di questi scenari sei esposto, senza falsi positivi. NexPloit è una pura soluzione di Application Security Testing interattiva, il che significa che è stata progettata e costruita come soluzione IAST fin dall'inizio. Quando si esegue una scansione dinamica, NexPloit comunica in perfetta armonia con l'agente locale sul sistema di destinazione, utilizzando Machine Learning per scoprire vulnerabilità che possono essere scoperte dall'interno solo da hacker o esperti di sicurezza. Inoltre, l'utilizzo di un agente ti consentirà di accedere alle funzionalità SAST come la strumentazione, individuando la posizione nel codice in cui è possibile risalire alle vulnerabilità scoperte. In poche parole, NexPloit utilizza un'interazione registrata come base da cui apprendere i punti di ingresso dell'applicazione e il tipo di dati che si aspettano. Dopo la fase di scoperta iniziale, l'agente NexPloit Cloud e NexPloit interagiscono per generare continuamente nuovi scenari dannosi, utilizzando algoritmi ML evolutivi e apprendimento di rinforzo. Questi scenari sono testati sulla destinazione fino a quando non viene scoperta una vulnerabilità.

onelogin	**OneLogin** semplifica la gestione delle identità con accesso sicuro, con un solo clic, per dipendenti, clienti e partner, attraverso tutti i tipi di dispositivi, a tutte le applicazioni aziendali cloud e on-premise Il passaggio al cloud offre un risparmio sui costi, un'infrastruttura ridotta e un'usabilità moderna. Ma anche un'azienda ibrida ha delle sfide: la frammentazione dell'IT man mano che le organizzazioni cercano di gestire le app in ambienti cloud on-prem e multipli. L'approccio più diffuso richiede più sistemi IAM per diversi ambienti, reti e dispositivi, portando ancora più problemi: maggiore complessità e costi più elevati per l'IT, un'esperienza utente compromessa e maggiori rischi per la sicurezza. Ora c'è un modo migliore. La piattaforma OneLogin UAM centralizza l'accesso attraverso l'organizzazione e soddisfa le esigenze in rapida evoluzione dell'azienda ibrida. Ti offre sicurezza, affidabilità e controllo per tutti i tuoi dati, dispositivi e utenti.

Plixer	**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.
RAPID7	**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.
Siemplify	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.
STEALTHbits TECHNOLOGIES	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.
STRONGKEY	StrongKey, Inc. è una società privata con sede a Silicon Valley, in California. È leader nell'infrastruttura di gestione delle chiavi di livello enterprise, portando nuovi livelli di capacità e sicurezza dei dati a un prezzo decisamente inferiore rispetto alle altre soluzioni presenti sul mercato. Fornendo prodotti e servizi nella gestione delle chiavi simmetriche, crittografia, tokenizzazione e PKI, StrongKey si concentra sulla protezione dei dati nel cloud computing, nell'e-commerce, nella sanità, nella finanza e in altri settori che richiedono la protezione dei dati sensibili. StrongKey ha definito un'architettura per applicazioni Web unica, conforme al Regulatory Cloud Computing (RC3), che consente il cloud computing sicuro. L'architettura RC3 è stata convalidata dai clienti per la protezione dei dati finanziari e sanitari utilizzando le soluzioni di StrongKey.

TitanHQ SpamTitan	SpamTitan è una delle soluzioni antispam più complete sul mercato per proteggere le email dallo spam e dalle minacce che si trasmettono e propagano via email. 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. SpamTitan nasce per domini illimitati, ed è quindi ideale per Internet Service Provider che desiderino offrire un servizio AntiSpam affidabile. La versione Cloud non necessita di infrastruttura locale, e unisce la sicurezza di SpamTitan alla flessibilità del Cloud.
TitanHQ WebTitan	WebTitan è una soluzione di web content filtering premiata con cinque stelle da SC Magazine, che permette alle aziende di proteggere i propri dati ed i propri utenti da malware e altre minacce Internet come virus, spyware, e phishing. Allo stesso tempo, offre strumenti di limitazione e controllo per rendere efficace l'attuazione delle politiche aziendali che riguardano la navigazione Internet. Il prodotto 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.
yubico	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. Con un semplice tocco, 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.
ZEROFOX	ZeroFOX, leader nel mercato della protezione digitale e sui social media, protegge le aziende di oggi dai rischi fisici, oltre che inerenti il marchio e la sicurezza dinamica, su piattaforme social, mobile, web e di collaborazione. Mediante l'utilizzo di varie origini dati e dell'analisi basata sull'intelligenza artificiale, la piattaforma ZeroFOX Platform identifica e risolve gli attacchi di phishing mirati, la compromissione delle credenziali, la fuga di dati, l'utilizzo non autorizzato del marchio, le minacce agli executive e relative alla posizione, e molto altro ancora. La tecnologia SaaS brevettata ZeroFOX elabora e protegge giornalmente milioni di post, messaggi e account nel panorama digitale e dei social media, compresi LinkedIn, Facebook, Slack, Twitter, HipChat, Instagram, Pastebin, YouTube, App Store mobili, deep e dark web, domini …

dotforce
Your Source for Innovative Cybertech

Via S. Anna 41 | 20090 Vimodrone (MI), Italy

Tel. 02/36735520 | Fax 02/36215698

www.dotforce.it | info@dotforce.it