dotforce
Your Source for Innovative Cybertech

Portfolio tecnologico

Ottobre 2019

Web Application Security **Web Vulnerability Management**	La sicurezza dei siti web è un aspetto trascurato di tutta l'attività di IT security, mentre dovrebbe essere una priorità, visto 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.). **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. Acunetix è un leader globale per la web security. Prima società a realizzare uno scanner di vulnerabilità web totalmente dedicato e automatizzato, Acunetix porta sul campo un'esperienza senza rivali. Acunetix web vulnerability scanner è utilizzato con fiducia da clienti che operano in ambienti con elevate necessità di sicurezza, tra cui numerose aziende Fortune 500.
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.
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.
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 la piattaforma DomainTools come ingrediente critico nel loro lavoro di indagine e mitigazione delle minacce.

ExtraHop **Real Time IT analytics**	ExtraHop è progettato per soddisfare le mutevoli esigenze e la solida 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 DEFINITIVI – 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 – non giorni – , mentre le integrazioni aziendali accelerano e automatizzano la risposta prima che le minacce incidano sulla tua attività.
Faronics **Multilayer Endpoint Protection**	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 **Software Vulnerability & Management**	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.
idaptive **Identity & Access Management**	Viviamo in una nuova era. Ci aspettiamo che tutto sia disponibile in ogni momento e in ogni luogo. L'ambiente composto da API, servizi cloud, dispositivi e dati che guidano questa trasformazione è estremamente complesso. Le aziende espandono le risorse e i team IT aldilà delle loro location fisiche, e le identità diventano il nuovo perimetro di sicurezza. Allo stesso tempo, la sofisticazione e la portata delle violazioni che minacciano questo nuovo mondo non hanno precedenti. Siamo letteralmente sotto assedio. Nessuna azienda è immune e sono in poche a essere al passo con i tempi. Questo nuovo scenario richiede un nuovo tipo di piattaforma di accesso. Nato da Centrify e basato su Zero Trust, Idaptive sta creando una nuova era – accesso sicuro ovunque – che integra perfettamente SSO, MFA, EMM e UBA, e rende più forti le difese di sicurezza aziendale, gestendo e mettendo al sicuro le identità dalle minacce cyber. Il risultato è una sicurezza e una compliance più robusta, una migliore agilità nel business e una migliore produttività degli utenti attraverso il single sign-on. Oggi, oltre 5.000 imprese, tra cui metà delle Fortune 50 e oltre 80 agenzie federali, si affidano a Idaptive per mettere al sicuro le loro identità.
iStorage® **Flash/SSD/HD Encrypted Drives**	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.

Antimalware & EDR	Malwarebytes, società fondata nel 2004, è un leader mondiale nelle soluzioni software nella protezione e remediation di Advanced Malware. Malwarebytes offre una suite di prodotti per proteggere gli utenti e il business da attacchi malevoli che sfuggono alle soluzioni tradizionali di anti-virus. Il prodotto di punta, Malwarebytes Anti-Malware, protegge dagli attacchi ben prima ben prima che gli altri prodotti li abbiano identificati, grazie ad un avanzato sistema euristico di rivelazione che ad oggi ha rimosso oltre 5 miliardi di attacchi malevoli sui pc di tutto il mondo. Se l'identificazione dell'attacco fallisce, la tecnologia Malwarebytes Remediation pone rimedio ed elimina qualsiasi infezione.
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. 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.
Identity & Access Management	Entrambi i fondatori di OneLogin, Thomas e Christian Pedersen, sono stati coinvolti nel successo della migliore applicazione di help desk on-demand al mondo: Zendesk. Attraverso le loro interazioni con i clienti di Zendesk, è diventato evidente ai fondatori che le aziende si stavano muovendo nel cloud a frotte. Mentre il cloud computing offre numerosi vantaggi, la gestione di dozzine di applicazioni cloud pone sfide significative in termini di sicurezza e produttività. L'idea è nata per creare una soluzione di gestione dell'identità e degli accessi facile da usare come le applicazioni cloud da cui le aziende dipendono. OneLogin è stato lanciato nella primavera del 2010 e ha ricevuto il supporto di CRV. Da allora, OneLogin ha collaborato con i principali fornitori SaaS e ha ottenuto la fiducia delle organizzazioni attente alla sicurezza in tutto il mondo.
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.
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 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.

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.
STEALTHbits TECHNOLOGIES **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.
STRONGKEY **Encryption, Strong Authentication, Key Management**	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 **AntiSpam Gateway Cloud & VA**	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 **Web Filtering Gateway Cloud & VA**	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 **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. 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 **Digital Risk & Brand Protection**	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