...fallo con Jarvis

#VulnerabilityManagement oltre il #Vuappìttì

SECURITY SUMMIT, 7 Giugno 2017, ROMA

Francesco MORINI
@franarchic

GREEN

BL4CKSWAN SRL

info@bl4ckswan.com

Bl4ckSwan dal 2012 soddisfa le necessità di mercato di alcune tra le realtà significative del panorama nazionale.

Un'azienda giovane e tutta (per ora) italiana

Milano

Roma

Socio Clusit – Associazione Italiana per la Sicurezza Informatica

Oracle Community For Security

Socio UNINFO

PCI Security Standards Council – QUALIFIED SECURITY ASSESSOR

ETSI

PECB – Professional Evaluation and Certification Board – AUTHORIZED TRAINING PARTNER

BL4CKSWAN SRL

info@bl4ckswan.com

Bl4ckSwan Srl - 4 #BusinessLine e qualche servizio

Certificazione

#PCIDSS

#ISO 27001

Governance

#RiskManagement

#Privacy and #GDPR

Operations

#SecDevOps and #Appsec

#VulnerabilityManagement

Formazione

#ISO-Implementer

#Professional-Certific

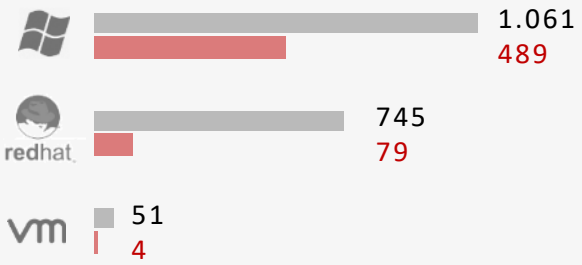
BL4CKSWAN SRL

info@bl4ckswan.com

Se parliamo di vulnerabilità, conti alla mano... «*s'hadda lavurà*»

Trend in aumento (da sempre)

Lo si dice dalla notte dei tempi – i trend sono in forte crescita:



Vulnerabilità by vendor 2015-2016

Vuol dire che...

Un'infrastruttura che opera 2 virtual center, con 20 server Ms e CentOs...:

VC = (1*2)+(195*20)+(31*20) =

4.522

vulnerabilità CRITICHE

Solo la punta dell'iceberg

Con i conti fatti copriamo, salvo eccezioni, quasi esclusivamente sistemi operativi...

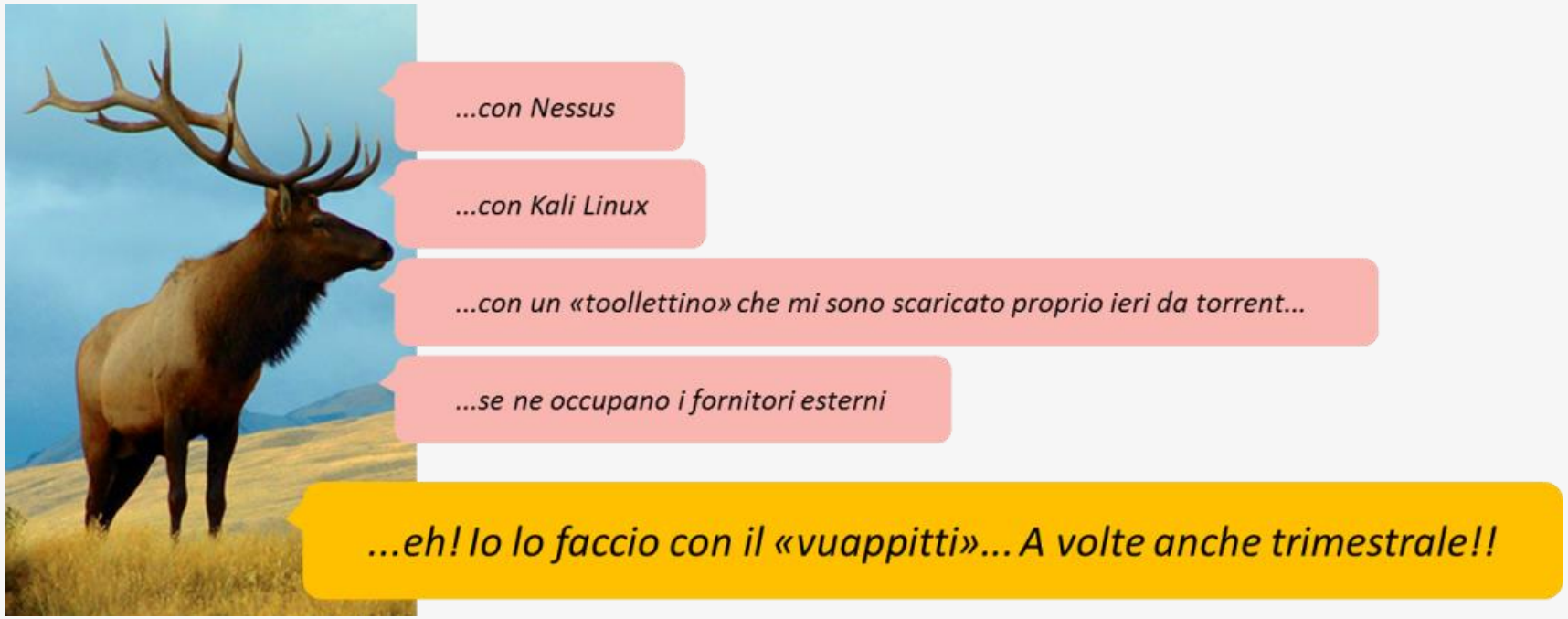
Servizi | Middleware | Database

App. Custom | Siti Web | App. OTF

BL4CKSWAN SRL

info@bl4ckswan.com

L'ultima volta avevamo stabilito che il #VulnerabilityManagement NON si fa...



BL4CKSWAN SRL

info@bl4ckswan.com

Ci eravamo anche lasciati con qualche best practice…

Programmazione

- Identificare perimetri
- Selezionare audit applicabili
- Selezionare fornitori

Rilevamento

- Confermare copertura perimetro
- Convergenza in un solo punto di analisi

Analisi

- Valutare il vero rischio delle vulnerabilità:

Business impact

Il contesto esterno

Risoluzione

- Identificare lotti di intervento secondo il costo-opportunità
- Definire piani di intervento con gradi di dettaglio

Monitoraggio

- Severity changes
- Controlli compen
- Stato avanzamento remediation
- Risk in general

BL4CKSWAN SRL

info@bl4ckswan.com

...e qualche problematica frequente...

Programmazione

- Non so quali applicazioni esposte su rete pubblica sono state testate l'anno passato.

Rilevamento

- Uno in html, l'altro in pdf, poi l'Excel...

Analisi

- Non so come muovermi attraverso tutte le segnalazioni.
- Troppe ridondanze!

Risoluzione

- Le vulnerabilità sono tante e diverse – ok – ma ci sarà un punto da cui converrà partire?

Monitoraggio

- Nessuno sa dirmi se questa vulnerabilità è presente su qualche sistema business-critical?

BL4CKSWAN SRL

info@bl4ckswan.com

...ma non con la soluzione al problem...

Jarvis è una vulnerability management suite ideata non solo per le **IT-Ops** e **SecOps**, ma anche per **IT Compliance** e **Risk Management** .

jarvis
at your service

Jarvis è una fattore abilitante per:

Pianificare attività

Identificare priorità

Ottimizzare l'operatività

Supportare decisioni

Monitorare avanzamenti

BL4CKSWAN SRL

info@bl4ckswan.com

Jarvis in qualche pillola

Una cybersecurity "business app

Colma il vuoto che viene a formarsi subito dopo la consegna del malefico «vuappitti».

Facile, intuitiva e orientata alla produttività e collaborazione inter-dipartimentale.

Risultati evidenti

Introduce molti principi dettati da standard e best practice anche in ambienti «strutturati».

Risparmi significativi a partire dalla prima settimana di operatività (a volte).

Solida realtà (?)

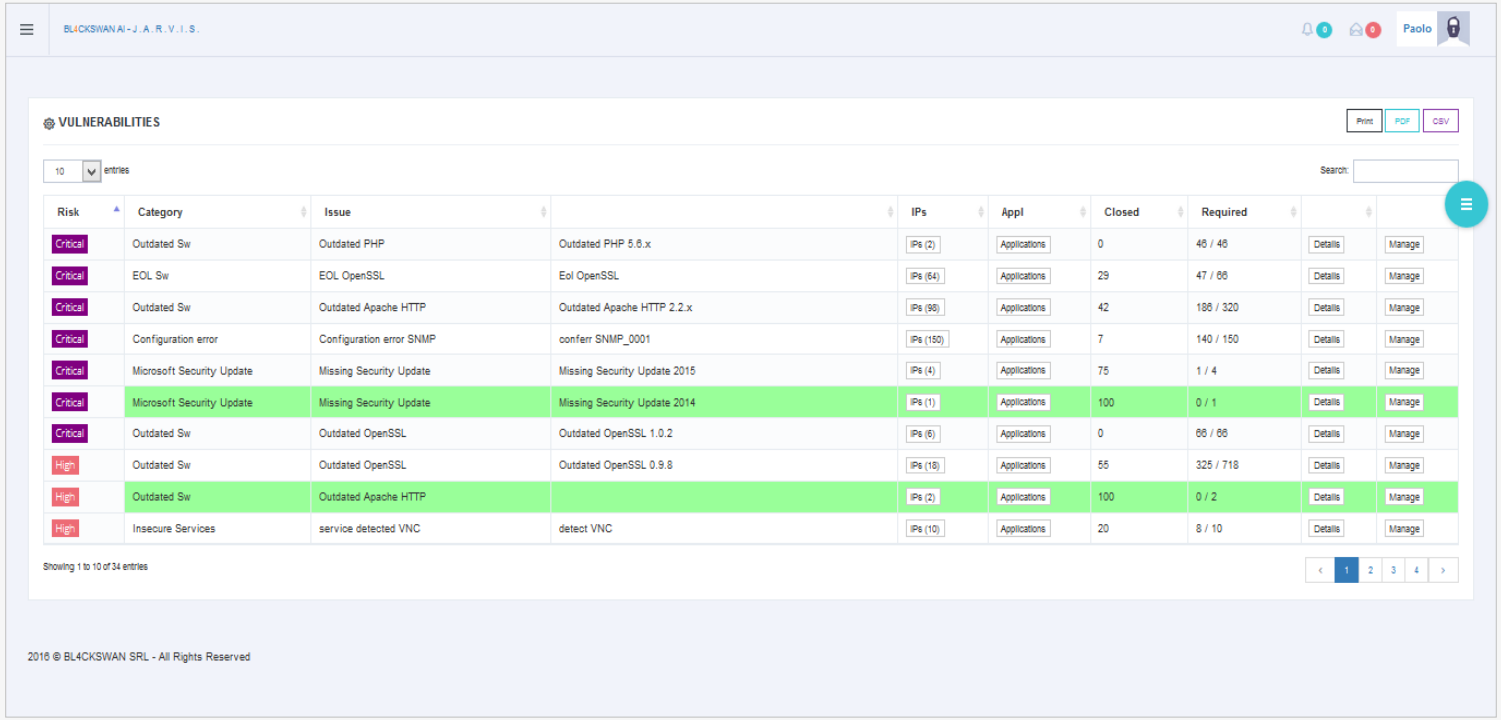
Due installazioni operative in ambienti di dimensioni medio/grandi (+200 nodi).

Aggiornamento settimanale su vulnerability bi-settimanale tramite push/pull update.

BL4CKSWAN SRL

info@bl4ckswan.com

Jarvis aggrega vulnerability data proveniente da più fonti in una schermata condivisibile.



BL4CKSWAN SRL

info@bl4ckswan.com

Una rete ospita nodi infrastrutturali...

- Subnets
- Networks
- Entities

Che possono presentare vulnerabilità...

- Business Software
- Service Software
- Operating System
- Host

Che comportano un rischio per varie dimensioni aziendali o organizzative.

- Dipartimento
- Outsourcer
- Risorsa Umana
- Processo

Una base dati che mette in relazione perimetri fisici, reti, infrastrutture fisiche e virtuali, applicazioni e processi consentono di esercitare un controllo totale su qualsiasi ambito – non solo il Vulnerability Management.

Nonostante la generazione di un asset inventory maturo richieda tempo e risorse, possiamo ottenere già oggi qualcosa di valido e utilizzabili sfruttando qualche procedura automatizzata e (sigh)... un vuappitti:

I raw degli scanner consentono di censire gli host, servizi o applicativi e quanti più informazioni su una base dati condivisibile.

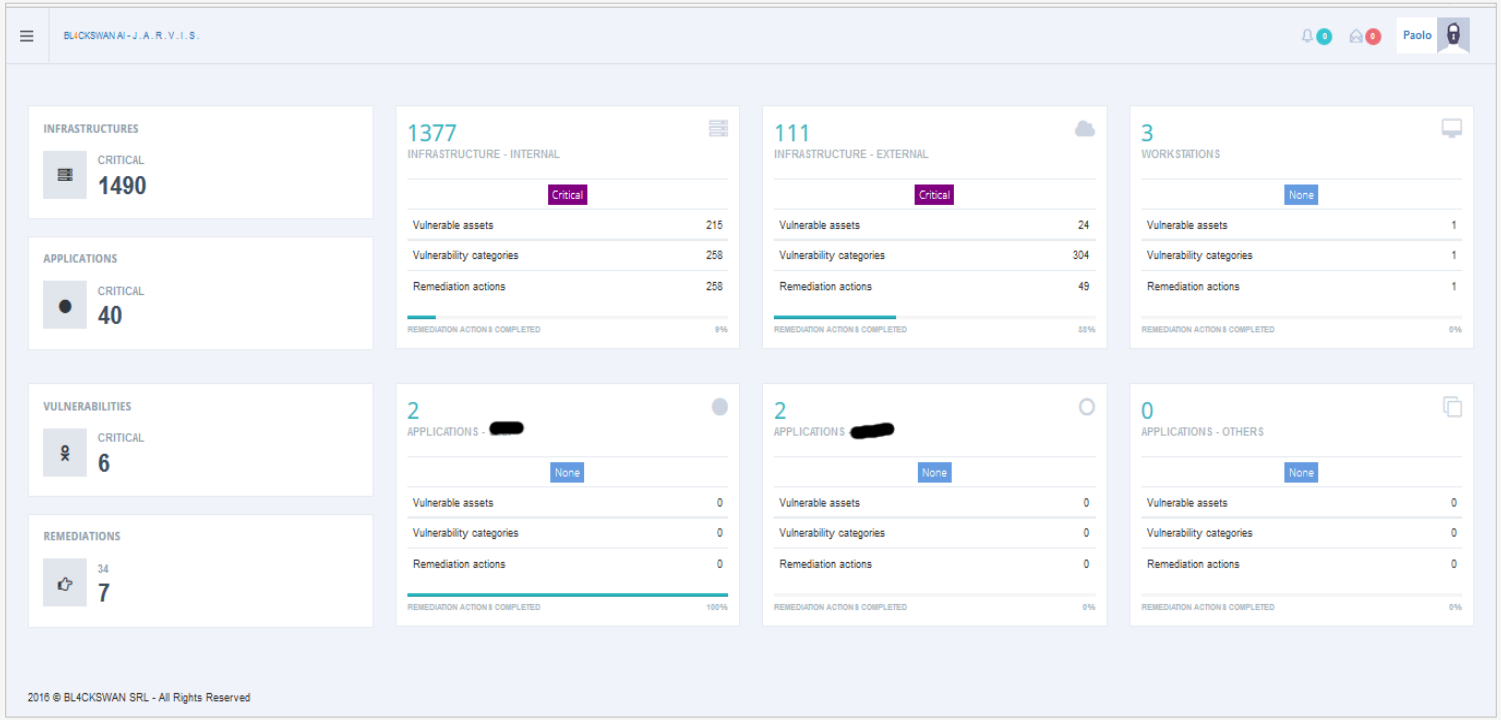
Analisi semantica ed espressioni regolari, suggeriscono al proprio utente opzioni per il popolare automaticamente più livelli di descrizione per diversi insiemi di asset.

Funzioni di filtro, ricerca avanzata e multiselezione aiutano a identificare le informazioni mancanti, indirizzando il loro reperimento con efficacia.

BL4CKSWAN SRL

info@bl4ckswan.com

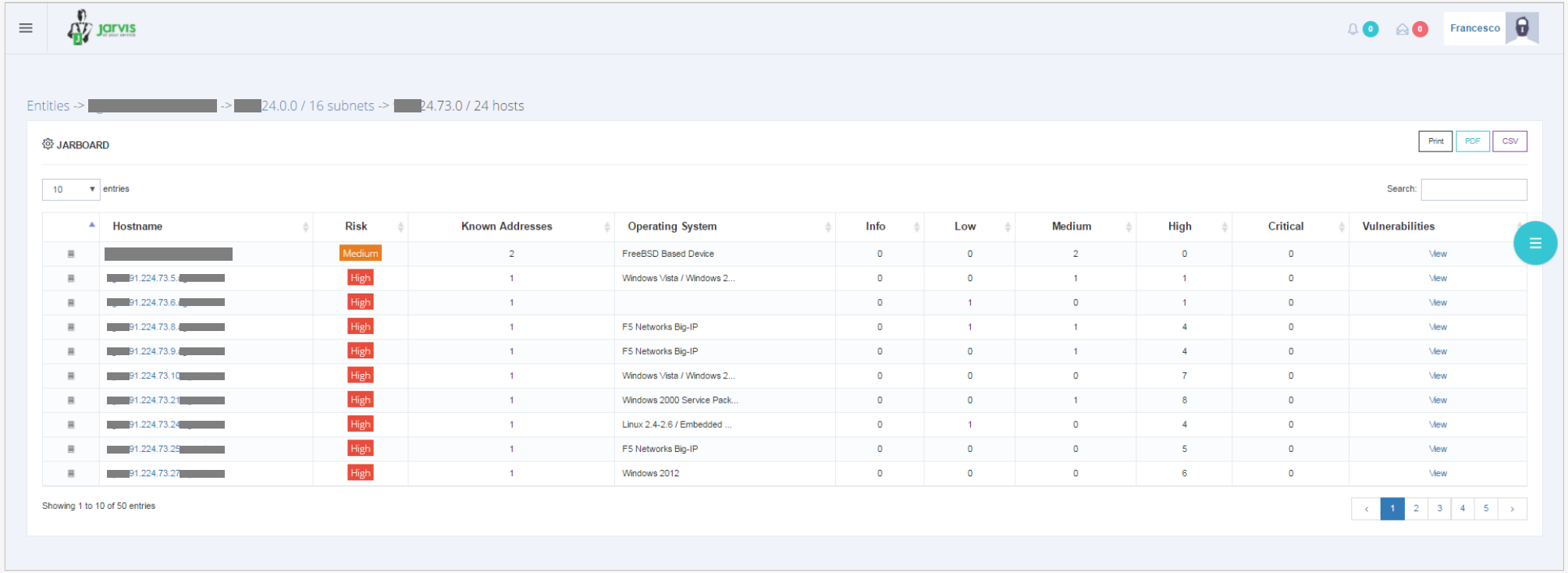
Può essere rappresentato anche cosi:



BL4CKSWAN SRL

info@bl4ckswan.com

Anche se il metodo più utile alla lunga diventa questo....



BL4CKSWAN SRL

info@bl4ckswan.com

Jarvis introduce il #VulnerabilityManagement come processo organizzato e facilmente assimilabile attraverso il paradigma dell'action based automation.

Programmazione

- Identificare perimetri
- Selezionare audit applicabili.
- Selezionare fornitori

Rilevamento

- Confermare copertura perimetro.
- Convergenza in un solo punto di analisi.

Analisi

- Valutare il vero rischio delle vulnerabilità:

Business impact

Il contesto esterno

Risoluzione

- Identificare lotti di intervento secondo il costo-opportunità.
- Definire i piani di intervento con gradi di dettaglio.

Monitoraggio

- Severity changes
- Controlli compensativi
- Avanzamento remediation
- Tracciare tutto!

BL4CKSWAN SRL
info@bl4ckswan.com

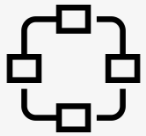
Programmazione

Identificare perimetri di interesse.

Selezionare audit applicabili.

Selezionare fornitori

Avviare il processo.



Definizione obiettivi

- Suggerisce lotti di asset – omogenei e/o accomunati da carattersitiche quali, cluster applicativo di appartenenza, infrastructure service, ecc.

Perimetri “custom”

- Arricchisce l’opzione di raggruppamento, usando criteri user driven.

Collaborazione

- Una piattaforma che unisce sicurezza, operations, acquisiti e terze parti.

Protocolli

- Introduce modalità di gestione delle attività di security audit, introducendo un standard di delivery consistente tra più parti.

BL4CKSWAN SRL

info@bl4ckswan.com

Rilevamento

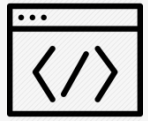
Confermare copertura del perimetro.

Confermare verbosità profondità dello scan.

Convergenza in un solo punto di analisi.

Network Scanner

- Compatibile con i principali network e security scanner open-source e proprietari.



Application Scanner

- Compatibile con i principali web application e security scanner open-source e proprietari.
- Anche prodotti di code review (beta).

Configuration Dumps

- Interpreta la semantica di configuration file (OS, servizi) paragonandoli a baseline CIS Security.

Manual Findings

- È possibile creare vulnerabilità «custom», con proppria cateogie e assegnarle a qualsiasi perimetro o asset, con criticità e quant'altro.

BL4CKSWAN SRL
info@bl4ckswan.com

Analisi

Valutare il vero rischio di una data vulnerabilità in base a:

- Sensibilità degli asset
- Sensibilità dei processi
- Il contesto esterno.

Scanner Data

- Aggrega in un punto solo i dati di tutti gli scanner.
- Elimina ridondanze.
- Sfrutta le informazioni delle bistrattate «info».

Business Knowledge

- Integrano logiche di analisi e valutazioni derivanti da asset inventory e knowledge aziendale interno.

Open Sources

- Integrano logiche di analisi derivanti da standard aperti.
- Integra tanti acronimi - CVE, CWE, CVSS, CWSS, OVAL, CPE, SCAP, OWASP, CAPEC.

Human Perspective

- Integrano logiche di analisi personalizzabili.
- Da possiblità di incorporare punti di vista, attraverso workflow guidati.

BL4CKSWAN SRL

info@bl4ckswan.com

Remediation

Identificare lotti di intervento secondo il costo-opportunità.

Definire i piani di intervento con vari gradi di dettaglio.

Basic Remediation

- Presenta remediation tactics suggerite dagli scanner.

Kb Support

- Punta le remediation tactics ed eventuali hotfix, patch, update disponibili dai siti vendor.

Internal Knowledge

- Presenta remediation tactics «custom» precedentemente definite.

Follow-up

- Segnala le modalità per confermare la risoluzione di una vulnerabilità – per andare «oltre il vuappitti».

Meet Jarvis: Supporto al monitoraggio

una business application per il #vulnerabilitymanagement

BL4CKSWAN SRL
info@bl4ckswan.com

Monitor and Govern

Severity changes

Controlli compensativi

Stato avanzamento remediation.

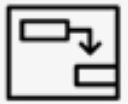
Risk in general

Analisi incoerenze

- Nuovi asset deployati e mai segnalati.
- Vulnerabilità riemerse su un server già bonificati.
- Hostname-IP conflicts

Activity backlog

- Possibilità di bypassare alcuni step del workflow, pur mantenendo chiaro controllo sul «backoffice».



Task scadenziate

- Calendarizzazione collaborazione Creazione task Email reminder
- Workflow autorizzativi.

Tracciabilità

- Ricostruire passo passo tutte le attività e ragionamenti effettuati in ambito del processo di vulnerablity management.

GREEN

BL4CKSWAN SRL

info@bl4ckswan.com

Espandi le capability di Jarvis con moduli addon

Asset Inventory

Fw Ruleset Reviewer

Wireless Rogue Detection

...falla una demo con Jarvis

;)

info@bl4ckswan.com

GREEN