Studio Fiorenzi
Security & Forensics

ENTERPRISE DIGITAL FORENSICS E SICUREZZA CON STRUMENTI OPEN: AUTOMATIZZARE AUDIT, INDAGINI INFORMATICHE FORENSI E L'INCIDENT RESPONSE CON VELOCIRAPTOR E AWX ANSIBLE

Presentazioni

Dottore in Scienze dell'Informazione (informatica)
mi occupo di Sicurezza Informatica dal 1997 e Digital Forensics dal 2002

AlessandroFiorenzi.it

Albo CTU Tribunale di Firenze
Albo Periti Tribunale di Firenze
Albo Consulenti Tecnici CCIAA di Firenze
Albo Docenti Sistema Informatico dell'Ateneo Fiorentino (SIAF)
Albo Esperti in Innovazione Tecnologica (ex Innovation Manager) MISE
Elenco Consulenti Arbitratori CCIAA di Firenze

Abilitazione NATO NCAGE AT568
Certificazione ECEE: European Certificate on Cybercrime and Electronic Evidence
Auditor/Lead Auditor Sicurezza delle Informazioni - ISO 27001:2013

Co Autore per gli aspetti di computer forensics libro "Internet e il danno alla persona" edito da Giappichelli nel 2012
Membro del Pool di esperti Europena Data Protection Board

Clusit Associazione Italiana per la Sicurezza Informatica
ONIF: Osservatorio Nazionale Informatica Forense
CGT: Circolo Giuristi Telematici
ANRA: Associazione Nazionale Risk Manager

Board of Directors ONIF – Osservatorio Nazionale Informatica Forense www.onif.it
Promotore e gestore canale Telegram DataBreach https://t.me/databreach
Promotore e gestore del sito sul repertamento informatico www.repertamento.it

Di cosa parleremo

Digital Forensics Applicata al contesto Aziendale:

- Indagini Informatiche e Incident Response
- Audit

Come

- Con due strumenti «diversamente open»
- Velociraptor © Rapid7
- AWX + Ansible © RedHat

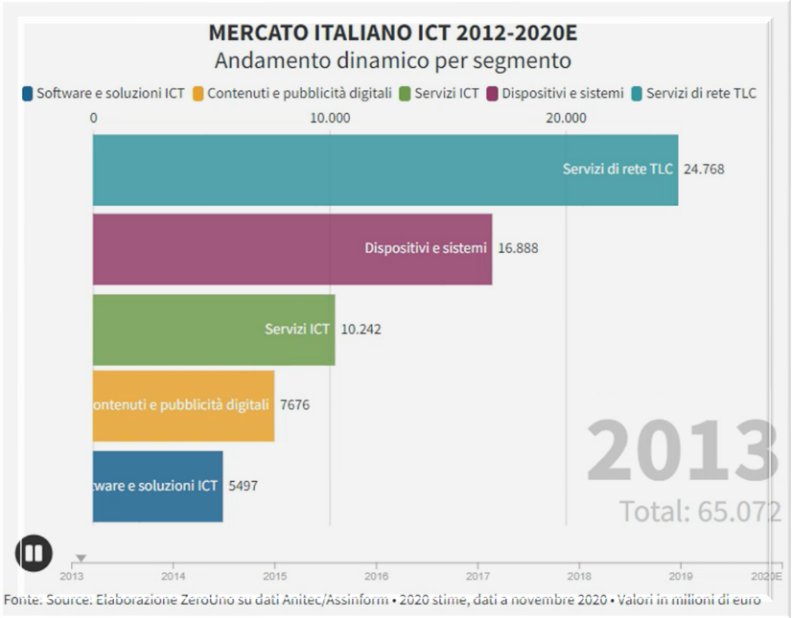
Evoluzione dei contesti aziendali

- Le aziende 10 anni fa, 2012
  - Aziende non completamente digitalizzate (molta carta)
  - Sistemi on premises, su server fisici
  - Storage di piccole dimensioni
  - Molti desktop dischi piccoli
  - Smartphone aziendali (privati) 32G era un lusso
  - Aziende poco connesse
- Le aziende nel 2023
  - Digitalizzazione delle aziende
  - Sistemi on premises e/o in cloud
  - Storage medio grandi 20TB
  - Desktop e portatile con dischi molto capacitivi
  - Smartphone aziendali minimo 128GB
  - Aziende iperconnesse
    - VPN C2S per dipendenti, consulenti
    - VPN S2S per fornitori e manutentori

Si evolvono anche i problemi

- Gestire un incidente informatico significava
  - individuare il perimetro dei sistemi coinvolti
  - Fare copia forense dei sistemi (disk imaging)
  - Avviare analisi copie forensi (time consuming)
  - Ripristinare l'ultimo backup e azioni di remediation

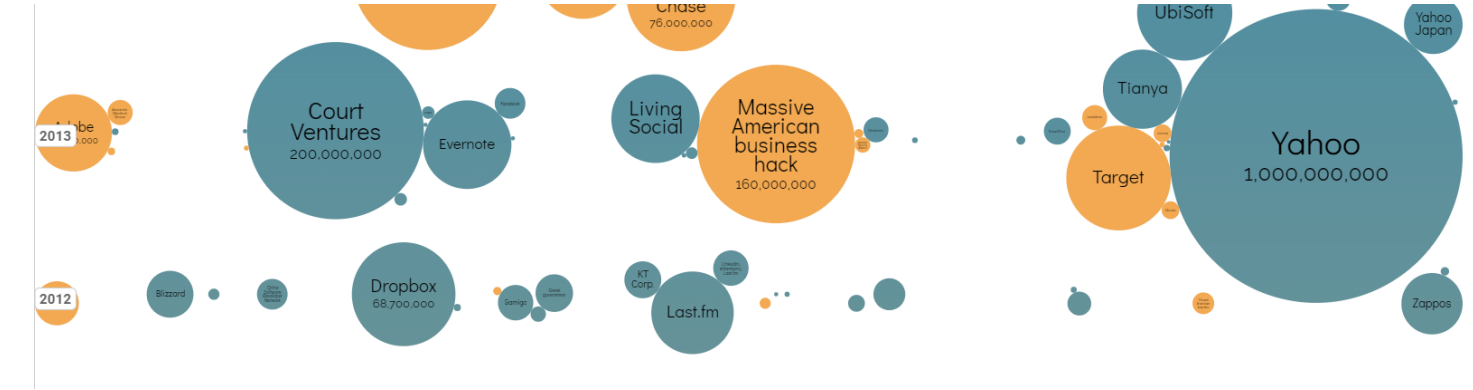
- Problemi oggi
  - Il numero di sistemi server e pdl è molto maggiore
  - La dimensione dei dischi/storage è cresciuta
  - La quantità di informazione presente su pdl e server è cresciuta
  - Tempestività nella risposta ad un attacco/data breach
  - E' sempre più difficile identificare con certezza il perimetro interessato
  - DF con Disk imaging e analisi in contesti aziendali di medie dimensione è complesso e richiede un numero considerevole di risorse

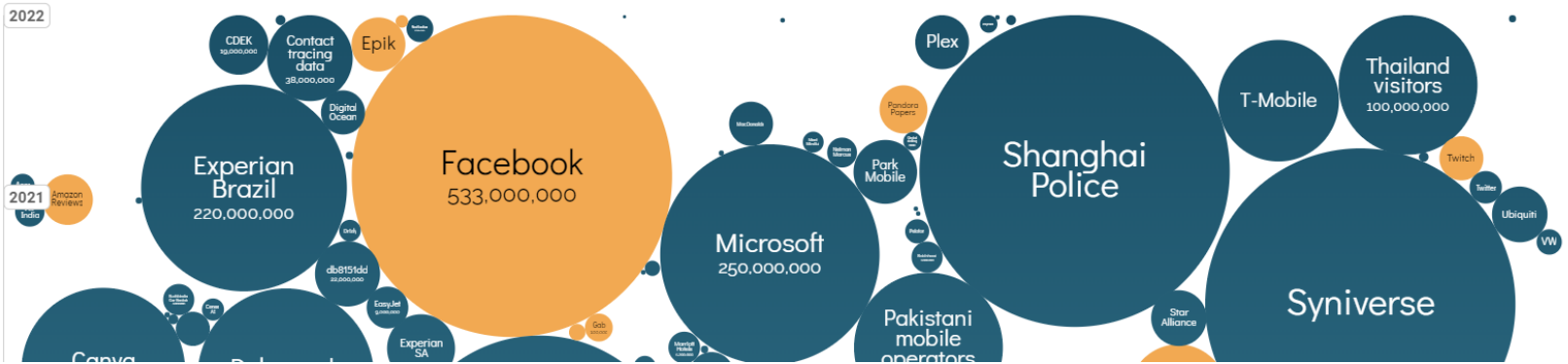


Per seguire l'evoluzione dei Data Breach
https://t.me/databreach

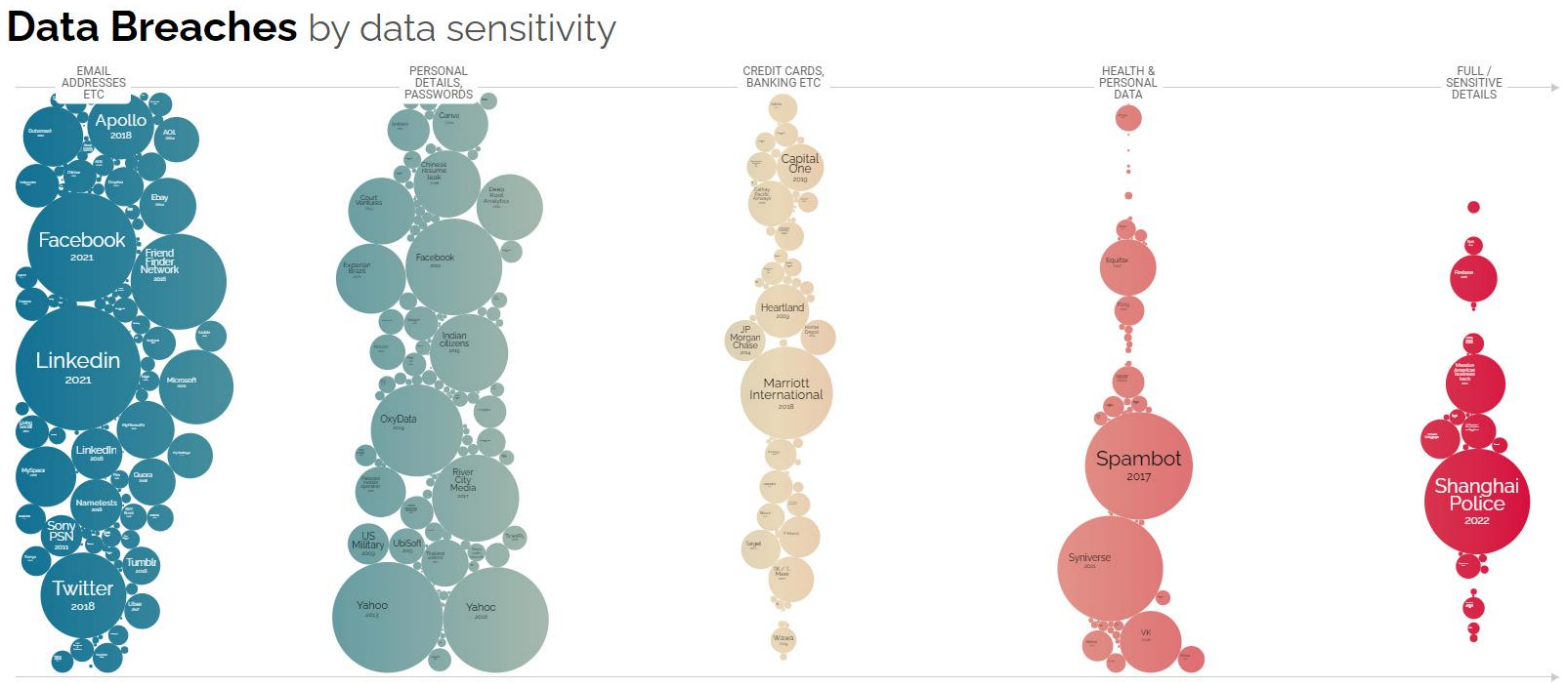
Fonte: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Data breach


2013
Court Ventures
200,000,000
Evernote
Living Social
Massive American business hack
160,000,000
Chase
76,000,000
UbiSoft
Yahoo Japan
Tianya
Target
Yahoo
1,000,000,000
2012
Blizzard
Dropbox
68,700,000
KT Corp.
Last.fm
Zappos


2022
CDEK
Contact tracing data
38,000,000
Epik
Digital Ocean
Experian Brazil
220,000,000
Facebook
533,000,000
Plex
Pandora Papers
Park Mobile
Shanghai Police
T-Mobile
Thailand visitors
100,000,000
Twitch
Twitter
Ubiquiti
VW
2021
Amazon Reviews
India
db8151dd
EasyJet
Experian SA
Microsoft
250,000,000
Pakistani mobile operators
Star Alliance
Syniverse

Target degli attacchi



Incidenti di sicurezza

Data Breach

- un incidente di sicurezza in cui dati sensibili, protetti o riservati vengono acceduti, consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato

Incidente Informatico

- qualsiasi evento che non fa parte dell'operatività standard di un servizio e che causa, o può causare, un’interruzione e una riduzione della qualità di tale servizio: un sabotaggio, una violazione dei sistemi, la sottrazione di PI sono incidenti informatici

DFIR: Digital Forensics Incident Response

- L’utilizzo di strumenti e metodi della digital forensics nella risposta agli incidenti per la raccolta e analisi delle evidence. **La gestione di un incidente è un evento critico:** può avere impatti sulla filiera produttiva, può comportare un danno finanziario, reputazione, può riguardare i dati di clienti e dipendenti e richiedere la notifica alle forze dell’ordine o al Garante Privacy

- DFIR è la risposta alla gestione degli incidenti informatici

- DFIR = Digital Forensics + Incident Response
  - La digital forensics con processi e strumenti per raccogliere, conservare e analizzare le prove forensi.
  - L’incident Response consiste nel contenere, bloccare e prevenire un attacco informatico

Aziende: soluzioni di sicurezza

- Molte aziende sono già dotate di questi strumenti di sicurezza
  - Firewall
  - Rete segmentata
  - Centrostella
  - IDS/IPS
  - Proxy Protezione Navigazione
  - Protezione DNS (umbrella)
  - XDR/EDR
  - SIEM
  - Backup
  - Personal Firewall

Aziende: sicurezza e incidenti di sicurezza

- E’ sufficiente disporre di tutte le soluzioni di sicurezza viste per gestire un incidente di sicurezza o un data breach?
  - Sono strumenti utile a ridurre il rischio di un incidente
  - Sono strumenti utili al ripristino delle funzionalità

- Le Aziende:
  - sono organizzate per la detection di molte situazioni di attacchi ma non di tutto, e non lo saranno mai al 100%
  - In caso di violazione
    - Non sono in grado di fare analisi, correlazione e ricerca di elementi di compromissione
    - Non sono in grado di effettuare acquisizione di evidence, file, chiavi di registro, cartelle, database etc….
    - Non sono in grado di fare distribuire ricerca di elementi di prova, IoC, malware etc.. Su tutti i sistemi IT dell’azienda.
    - Sono un campanello di allarme ma non sono in grado di individuare il perimetro coinvolto.

In caso di incidente & DF tradizionale

- Avrei bisogno che su ogni pc/server del perimetro (ammesso che sia stato individuato) ci fosse un analista forense a raccogliere dati su processi, file, hash, log, costruire la timeline delle ultime 76 ore o degli ultimi 10 giorni.

- Non avemmo mai abbastanza analisti forensi per gestire un incidente serio in un'azienda di medie (200 pdl 50 vm) o di grandi dimensioni: 1000-10000 pdl e 100-3000 vm

- Abbiamo però degli strumenti che ci permettono di eseguire sistematicamente le stesse operazioni su tutti i computer, su gruppi o su un singolo computer indipendentemente che siano nella stanza accanto o che siano nella sede norvegese o in cloud nella region asiatica si AWS

Soluzioni Open per DFIR

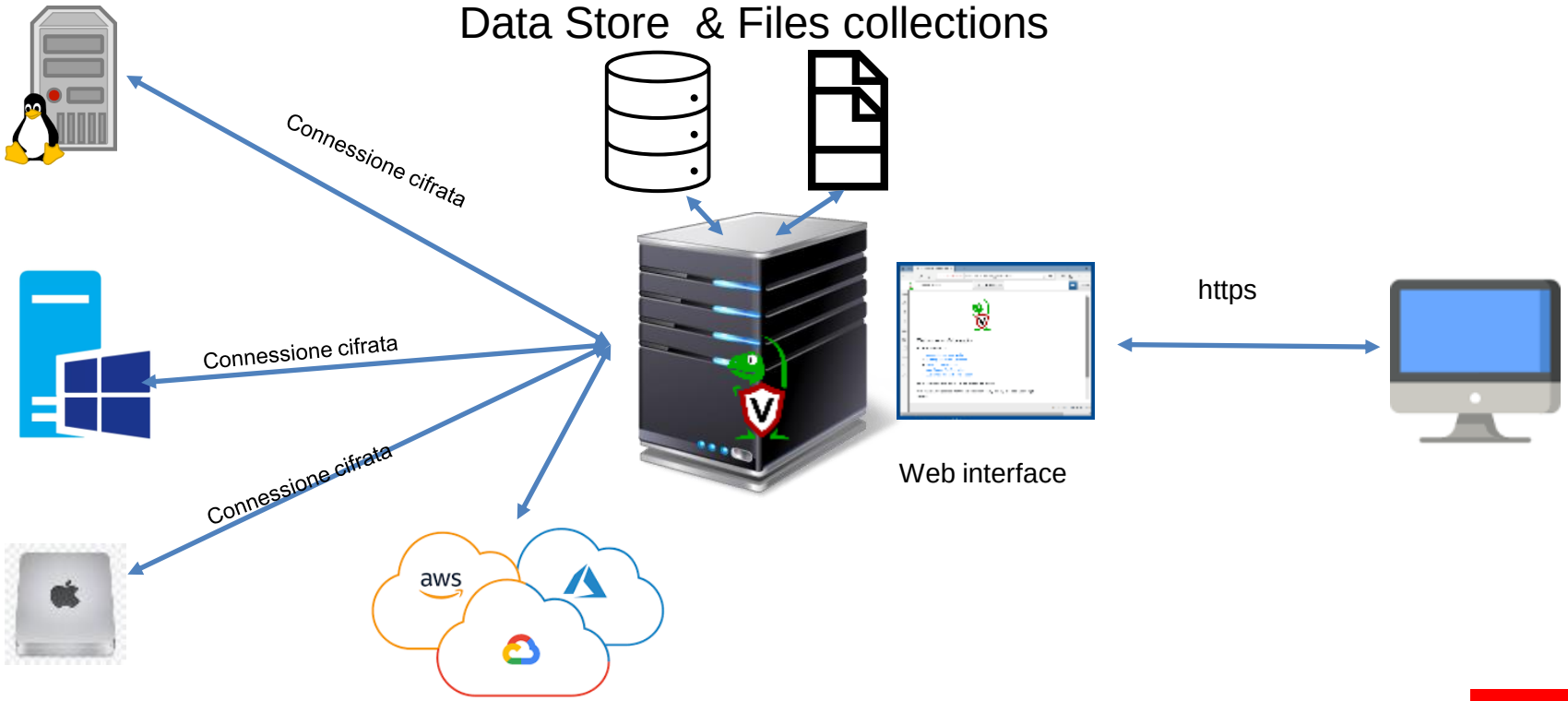
Velociraptor

- Velociraptor is an advanced digital forensic and incident response tool that enhances your visibility into your endpoints.
- È stato creato da Michael Cohen, contributor di Volatility, e progetti Google Rekall e Google Rapid Response (GRR)
- E' open ma è stato acquisito da Rapid7 nel 2021.
- **23 Settembre 2023 "Rapid7** is excited to announce the **integration** of **Velociraptor** DFIR into the Insight Platform for InsightIDR"
- **Agent based**

AWX + Ansible

- Ansible è un software che usato comunemente per automatizzare configurazione e gestione sui sistemi Unix e Windows
- AWX è il servizio web e console realizzata per consentire l'utilizzo di Ansible a team di tecnici IT.
- AWX e Ansible sono due prodotti Open di RedHat
- **Agentless**

Velociraptor: Architettura



Velociraptor

- Velociraptor è open su github https://github.com/Velocidex/velociraptor con binari per Linux, Windows, Mac e Freebsd
- Un unico eseguibile, in fase di configurazione si stabiliscono i parametri del server generando i file di configurazione da usare per i client
- Una volta configurato il server si procedere alla generazione dei pacchetti Unix e Window con la configurazione derivata dal server
- Durante l'installazione viene configurata una utenza amministrativa ma successivamente si possono configurare altre utenze con profili di accesso diversi

Velociraptor: I pilastri funzionali

- VQL Velociraptor Query Language
- VFS – Virtual File system
- Artefatti
- Hunting
- Monitoring

Velociraptor: VQL

- VQL è un linguaggio simile a SQL ma più semplice senza strutture complesse come «join» e «having»
- Gli statement sono del tipo :

- Gli statement lavorano su gli output dei VQL Plugin, un set ampio di plugin di base, che permettono di estrarre informazione dagli endpoint fornendo output in colonne
- Perché un query language ? Per ridurre il tempo necessario per scoprire un IoC sui sistemi aziendali: si progetta una regola per rilevare l'IoC, quindi si l'esecuzione di questa query su tutti i i sistemi della nostra infrastruttura ottenendo in pochi secondo o pochi minuti un output da ognuno di essi.
- Utilizzando VQL, in caso di un nuovo IoC l'analista forense può scrivere le query VQL pertinenti, inserirle in un artefatto e cercare l'artefatto nell'intero asset di hosts in pochi minuti: TEMPESTIVITA' ed identificazione del perimetro interessato.

Velociraptor: VFS

- La GUI di Velociraptor mostra l’elenco dei client. Selezionando un client, possiamo esaminare il suo filesystem, la VFS è la Virtual File System view dell’endpoint
- Il VFS è una cache lato server della struttura del file system e sui dati dei file presenti sull'endpoint. Se un ramo dell’albero della directory risulta vuoto è sufficiente richiedere la sync con l’endpoint per acquisirne i contenuti.
- Le informazioni di cache VFS dei client sono raccolte a intervalli regolari o al primo accesso.
- Possiamo operare sul file system come fossimo sull’endpoint, effettuando anche il download sul server Velociraptor dei file di interesse.
- In caso di file system NTFS è possibile effettuare ricerche e accedere ai dati ADS Alternate Data Stream
- Per gli endpoint Windows è possibile accedere ai contenuti del file di registro

Velociraptor: Artefatti

- VQL è l'elemento principale di Velociraptor, le query possono essere usate in modo interattivo su un endpoint o possono essere utilizzate per costituire un Artefatto inserendo le query in un file formato YAML con parametri da impostare in fase di esecuzione e una descrizione comprensibile che ne definisca scopo e uso.

- Velociraport è "volgarmente" un esecutore di query VQL strutturate in artefatti nei confronti di uno o n-endpoint

- Velociraptor arriva con un seti di Artefatti per Windows, Mac e Linux ma si possono costruire e definire nuovi artefatti per individuare specifiche necessità, come un nuovo IoC o si possono trovare nella community di Velociraptor

Velociraptor: Hunting

- Hunt Manager è un componente Velociraptor responsabile della pianificazione dell'esecuzione di una raccolta «di artefatti» e raccolte di client che soddisfano determinati criteri
- hunting, consiste nel recuperare informazioni previste dagli artefatti su tutti gli endpoint gestiti
- Una volta individuato un pattern di attacco si può mettere a punto una VQL ad hoc testarla in modalità interattiva, trasformarla in artefatto, utilizzare tale artefatto per operazioni di hunting

Velociraptor:Monitoring

- Il monitoraggio degli endpoint avviene attraverso gli Hunt. A tale scopo sono presenti alcuni plugin, chiamati “Event VQL Plugins”, che si mantengono costantemente in esecuzione sull'endpoint.

- A partire dalle query che utilizzano questo tipo di plugin è quindi possibile definire artefatti, e degli hunt che li contengono, che rimangano in esecuzione in attesa di eventi che si verificano sui client, inviandoli al server quando si realizzano.

- attraverso l'integrazione con sistemi di terze parti può essere impostata un'azione di follow-up

Velociraptor: indaghiamo

- Possiamo definire query in VQL per ricercare specifici elementi: IoC , hash, IP, chiavi di registro, nomi file, log etc.. da linea di comando verso un endpoint o verso tutti
- Possiamo ricercare artefatti Window Linux e Mac con parametri, ad esempio costruzione timeline
- Possiamo percorrere il file system dell'endpoint, acquisire metadati, ADS (NTFS) e altro dai file, selezionarli ed acquisirli
- Possiamo navigare e interrogare il file di registro di windows
- Possiamo Hunt, ovvero artefatti che vengono ricercati ciclicamente (l'utilizzo dell'utenza root o administrator, la creazione di una utenza locale)
- Attraverso gli Hunt possiamo monitorare condizioni degli endpoint rispetto a specifici artefatti

Velociraptor:

- Ricerca di nomi di file: Una delle operazioni più comuni in DFIR è la ricerca di file in base ai nomi dei file.
- Ricerca di contenuti : YARA è un potente scanner di parole chiave che consente di cercare dati binari non strutturati in base alle regole fornite dall'utente.
- Analisi file binari: Velociraptor utilizza VQL per creare una query VQL al fine di recuperare anche attraverso l'analisi di file binari.
- Prova dell'esecuzione: Velociraptor dispone di un ricco set di artefatti che possiamo utilizzare per dedurre l'esecuzione del programma in ambito Windows e Linux.
- Registri eventi: Velociraptor dispone di un seti artefatti per l'analisi del registro eventi di Windows come per i file di log di Unix .
- Stato del server (memoria e altro) :Tradizionalmente le prove volatili vengono acquisite utilizzando un dump completo della memoria del sistema (volatily) , e framework per la loro analisi. Velociraptor cerca di ottiene le stesse informazioni utilizzando le API del sistema operativo.

Velociraptor: riferimenti

- https://www.rapid7.com/products/velociraptor/
- https://github.com/Velocidex/velociraptor
- https://docs.velociraptor.app/
- Discord https://discord.com/invite/YAU3vRE

AWX Ansible: cosa sono?

Ansible

- Ansible è uno strumento open source per l'automazione IT che consente di automatizzare per il provvisioning,configurazione, deployment di sistemi e applicazioni.
- E' normalmente usato a livello sistemistico per installare i software, automatizzare le attività quotidiane, eseguire il provisioning dell'infrastruttura, migliorare i livelli di sicurezza e conformità, applicare patch ai sistemi.
- Ansible si connette ai sistemi target ed esegue i programmi e i comandi le istruzioni che prima si sarebbero svolte manualmente.
- Ansible è Agentless e si basa su una connessione ssh con utenza amministrativa

AWX

- fornisce un'interfaccia utente web based, API REST e l'engine per l'esecuzione dei task Ansible. È uno dei progetti RedHat Ansible Automation Platform

AWX Ansible architettura

User

- L'utente amministra la piattaforma e scrive i playbook

Playbook

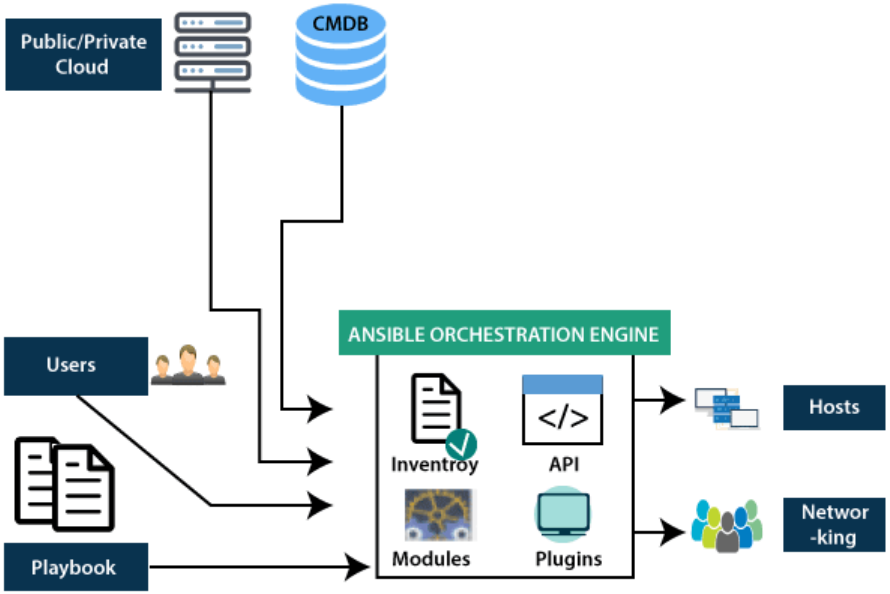
- Il playbook definisce i task che il processo di automazione dovrà eseguire, i task verranno eseguiti nell'ordine in cui sono riportati. Il playbook è scritto in YAML

Inventory

- E' l'elenco dei target system

Deploy

- Un job seleziona un playbook da applicare ad un inventory
- L'esecuzione di un job avviene attraverso connessione ssh (linux+windows) o WinRM (Windows Remoto Management) con le credenziali amministrative di ogni asset dell'inventory



AWX Ansible

- Gratuito
- Agentless
- Attraverso i playbook si può
  - Installare software, cancellare, copiare
  - Eseguire comandi bash o powershell
  - Selezionare e raccogliere gli output
- Un playbook può
  - essere eseguito interattivamente su un target system
  - diventare parte di un job applicato ad un asset inventory.
- Si può usare con sistemi on premises e in cloud a differenza di sistemi di automazione come Terraform che sono solo cloud oriented

AWX Ansible

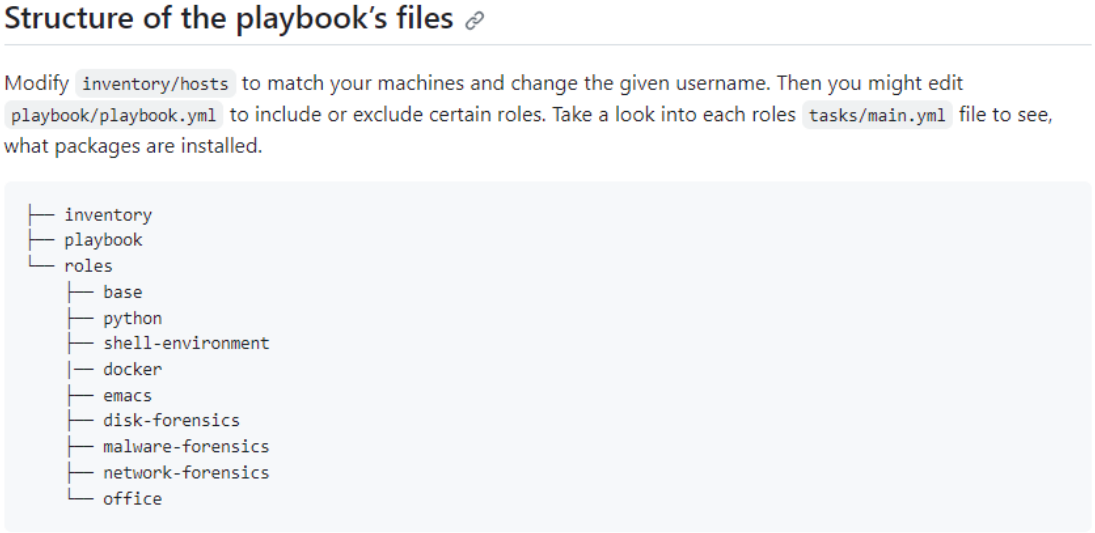
Con AWX e Ansible
Si possono definire playbook per eseguire indagini di tipo DFIR
Come le eseguirebbe un analista forense sul server
Infatti:
I comandi che un analista eseguirebbe nello svolgere un'analisi forense di un server possono diventare tanti task, di un playbook in cui alcuni task vengono eseguiti solo se si verificano certe condizioni altrimenti vengono eseguiti altri task.

Il risultato è un'analisi metodologica come fosse fatta da una persona ma distribuita istantaneamente su tutti i i sistemi dell'asset inventory

AWX Ansible

La community ha già progetti di playbook DFIR :

- https://github.com/jgru/ansible-forensic-workstation



Structure of the playbook's files

Modify `inventory/hosts` to match your machines and change the given username. Then you might edit `playbook/playbook.yml` to include or exclude certain roles. Take a look into each roles `tasks/main.yml` file to see, what packages are installed.

```
├── inventory
├── playbook
└── roles
    ├── base
    ├── python
    ├── shell-environment
    |── docker
    ├── emacs
    ├── disk-forensics
    ├── malware-forensics
    ├── network-forensics
    └── office
```

AWX Ansible

- https://github.com/brian-olson/ansible-live-response (SANS2019)

Section 2 - DFIR Triage

This playbook performs some basic information gathering and collects some artifacts of use during a webserver investigation.

- Running Processes
- Netstat
- Memory Dump*
- Apache Logs
- System Logs
- Bash History
- Web Server Files (webdir)

2.1 Run DFIR-triage playbook.

```
ansible-playbook DFIR-triage.yml
```

2.2 Review artifacts ($pwd/artifacts) retrieved and build out the response playbook.

Section 3 - DFIR Response

This playbook makes some changes to the host based on the findings of the triage phase.

Phase 1

- Patch
- Reconfigure/secure services

Phase 2

- Remove malware
- Remove unauthorized local users
- Terminate suspicious processes & network connections

3.1 Run the DFIR-response playbook to eradicate the adversary

DF & Audit

Gli Audit Si basano normalmente su

- Esame documentale
- Registrazioni
- Interviste
- Riscontri ispettivi
- Campionamenti
- ecc

E’ sufficiente oggi?

Audit Nuovi scenari

- Si ricorre all'Audit Interno ed Esterno nella certificazione secondo norme volontarie
- Si ricorre alle strutture interne di Audit per cercare evidenze di inadempienze, illeciti o reati a cui dare seguito con azioni disciplinari o l'apertura di procedimenti civili o penali

PCI-DSS, HIPAA, ISO 27001/27002, NIST 800-53, NIS II, DORA etc..

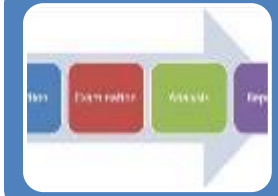
Tutto l'ambito della compliance richiede che gli elementi di audit e gli esiti dei controlli riportino elementi oggettivi acquisiti con metodi che diano certezza della fonte e dell'autenticità

Internal Audit ingaggiato da

- Governance
- HR
- ODV
- Ufficio legale

Audit Nuovi scenari

I metodi tradizionali della raccolta delle evidenze, in ambito Audit non sono sufficienti a garantire l'accettabilità della prova in giudizio.



E' necessario un nuovo approccio che per le evidenze raccolte garantisca

- Accettabilità
- Autenticità
- Completezza
- Attendibilità

La Computer Forensics è la risposta metodologica e scientifica per gestire le prove IT

Controlli di Auditing

- Se il controllo richiesto dall'azienda è verticale, come l'analisi ex-post di dipendente uscito dall'azienda, si può certamente operare con DF tradizionale :disk imaging + analisi

- Se l'audit o il controllo riguarda una OU o tutta l'organizzazione, in particolare quando le organizzazioni sono medio grandi, strumenti come Velociraptor e AWX Ansible sono strumenti maggiormente idonei ad per eseguire un controllo distribuito su tutti i sistemi in tempi nell'ordine di minuti o al più di ore.

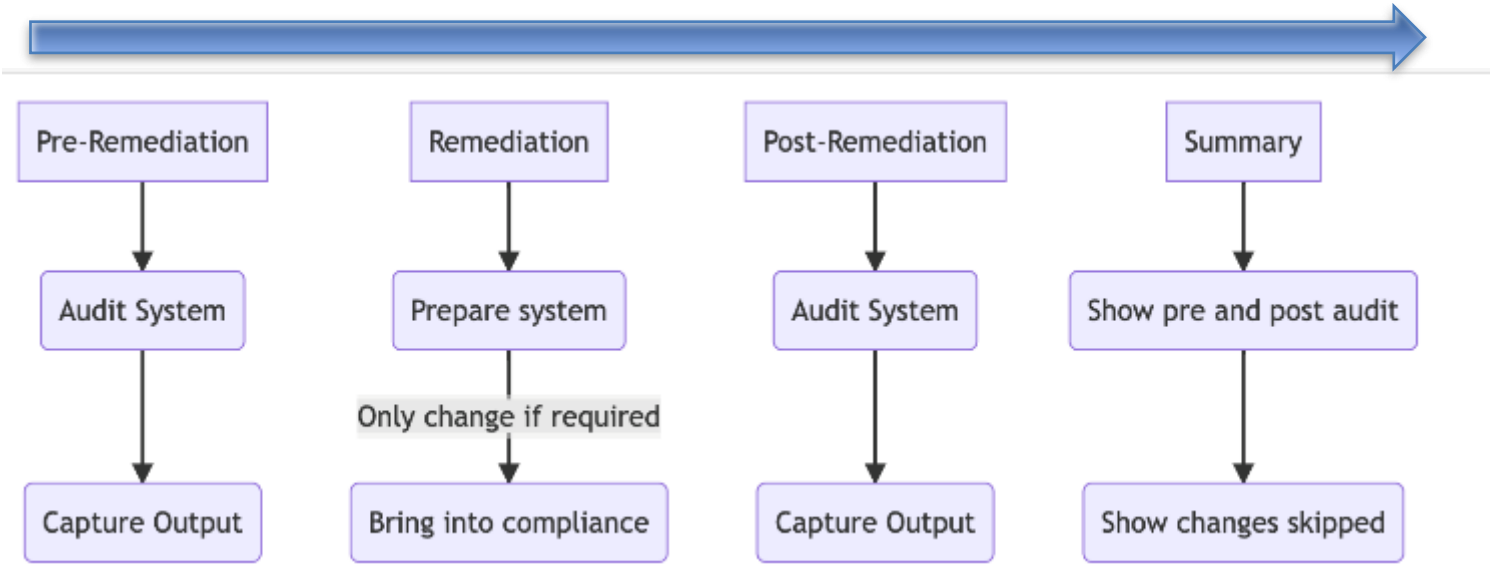
Security Standard compliance: enforcing, benchmarking & Audit

Sempre più spesso durante un Audit di norme come PCI-DSS, HIPAA, ISO 27001/27002, NIST 800-53, NIS e DORA l'Auditor ha la necessità di documentare gli esiti dei controlli anche dal punto di vista del processo seguito al fine di garantire la veridicità e autenticità dei dati di output che confluiscono nelle evidenze dell' Audit

I processi e gli strumenti della digital forensics, per loro natura, forniscono questo tipo di garanzie. Soluzioni come AWX+Ansible permettono

- Enforcing di security policy e configuration
- Benchmarking dell'infrastruttura rispetto agli standard di riferimento per le certificazioni
- Audit
  - Piano controlli secondo lo standard adottato, e gap analysis
  - Remediation
  - Audit post remediation certificazione rispetto compliance

Sviluppo di un Audit



Infine…

«Il futuro dipende da quello che facciamo nel presente»

Mahatma Gandhi

Studio Fiorenzi
Security & Forensics

Dott. Alessandro Fiorenzi
Email af@studiofiorenzi.it
Mobile: +393487920172
https://www.studiofiorenzi.it