DIIES Dipartimento di
INGEGNERIA
dell'INFORMAZIONE, delle INFRASTRUTTURE e dell'ENERGIA SOSTENIBILE

Corso di Tecnologie per la sicurezza informatica

Security Monitoring

Metodologie di Difesa

Vincenzo Calabrò

Agenda

- La Sicurezza Difensiva
  - Definizioni
  - Analisi e ricognizione
  - Meccanismi di Autenticazione
  - Metodi per proteggere la Rete Informatica
  - Metodi per proteggere le Applicazioni e i Servizi
  - Metodi per proteggere i Dati e le Postazioni
- Security Monitoring
- Incident Response
- Digital Forensics

Introduzione

Definizioni

Metodologie

Security Analyst

Ruolo: Assicura l'implementazione della politica di sicurezza aziendale.

Contesto operativo: Propone ed implementa i necessari aggiornamenti della sicurezza. Consiglia, supporta, informa e fornisce addestramento e consapevolezza sulla sicurezza. Conduce azioni dirette su tutta o parte di una rete o di un sistema.

Attività svolta:

- Monitoraggio della sicurezza agli accessi
- Esecuzione di security assessments tramite vulnerability testing e risk analysis
- Esecuzione dei controlli di sicurezza sia interni che esterni
- Analisi delle violazioni della sicurezza per identificare la causa principale
- Aggiornamento continuo della risposta agli incidenti e dei piani di ripristino
- Verifica della sicurezza dei fornitori di terze parti e collaborazione con loro per soddisfare i requisiti di sicurezza

Framework di sicurezza, politiche, controlli e procedure

NIST Special Publication 800-53, Revision 5

L'Istituto Nazionale degli Standard e della Tecnologia (NIST) ha emesso la Pubblicazione Speciale 800-53 come catalogo di 20 gruppi di controllo di sicurezza e privacy. Il Framework Core è diviso in Funzioni (Identify, Protect, Detect, Respond e Recover)

CIS Critical Security Controls

Sviluppato dal SANS Institute, sono una serie raccomandata di azioni per la difesa informatica che forniscono modi specifici e attuabili per fermare gli attacchi più pervasivi e pericolosi. Il framework consta di 20 controlli, che indagano aree prioritarie come la sicurezza delle configurazioni hardware e software, la difesa da malware, il recupero dei dati, il monitoraggio e controllo degli account, la gestione e risposta agli incidenti, test di penetrazione ed esercizi di Red Team.

Standard ISO/IEC 27001

Sviluppato dall'International Standards Organization (ISO), fornisce alle organizzazioni i requisiti su come gestire e proteggere le loro informazioni aziendali sensibili con un cosiddetto Information Security Management System (ISMS). L'ISMS è un framework di gestione del rischio che aiuta a identificare, analizzare e affrontare i rischi di informazioni di un'organizzazione per proteggersi da minacce informatiche e violazioni dei dati

Documentazione e modulistica

La maggior parte dei i Framework di Sicurezza prevede una documentazione e una modulistica definita e formale perché spesso è necessaria per ottenere le relative certificazioni.

La formalizzazione degli atti relativi all'organizzazione, alle procedure e alle informazioni che interessano la gestione della sicurezza delle informazioni ha un duplice obiettivo:

- Normalizzare le procedure e le informazioni
- Ridurre i tempi di ricerca e di risoluzione in caso di emergenza

Approccio white/black box per l'indagine all'infrastruttura ITC

Nell'ambito della sicurezza informatica e dei relativi test di controllo ritroviamo metodologie **WHITE BOX** e **BLACK BOX**.

WHITE BOX: questa modalità prevede che il tester sia informato dal Committente riguardo all'infrastruttura ed ai servizi esistenti. In questo caso l'azienda indicherà quali servizi sono attivi e in uso, riducendo di molto i tempi di esecuzione del test. Il Tester non eseguirà la prima fase di Information Gathering, perché conosce già il sistema, i software e i servizi in essere.

BLACK BOX: questa modalità è molto più verosimile a un attacco vero e proprio apportato da un attaccante esterno. In questo caso, infatti, il tester non avrà informazioni né dell'infrastruttura né del target da analizzare. In pratica è l'esatta simulazione di un hacker malintenzionato che, da zero, dovrà impegnarsi a conoscere l'infrastruttura (servizi, software, firewall ecc…).

La scelta della modalità di indagine dipende dall'organizzazione. Se dotata di un Team ben dimensionato, si realizzano entrambe le procedure con gruppi di lavoro separati e al termine si confrontano i risultati ottenuti.

Report finale

Il risultato dell'attività del Security Analyst si concretizza con una serie di output:

- Esecuzione dell'analisi e delle valutazioni di sicurezza
- Stesura di un nuovo piano procedurale per utenti e manutentori
- Redazione di un piano di mitigazione delle vulnerabilità e contromisure
- Implementazione dei meccanismi di autenticazione
- Implementazione delle misure di protezione per la Rete Informatica
- Implementazione delle misure di protezione per le Applicazioni e i Servizi
- Implementazione delle misure di protezione per i Dati e le Postazioni
- Implementazione delle misure di protezione
- Redazione dei Piani di Continuità del Servizio e Disaster Recovery
- Redazione dei Piani di Risposta all'incidente
- ….

Analisi e Ricognizione

La prima attività da svolgere è sicuramente l'analisi e la ricognizione:

- Valutare le norme precauzionali per intervenire nell'infrastruttura
- Realizzare una mappatura della rete, dei servizi e delle utenze
- Esaminare le postazioni utente e le configurazioni software
- Predisporre i tools per esaminare file di log e le anomalie riscontrate
- Effettuare scansioni e ricerche rapide di file e informazioni pericolose
- Esaminare i servizi interni e i sistemi di autenticazione
- Realizzare una scansione rapida delle vulnerabilità e penetration testing
- Analizzare le procedure utente e i flussi di informazione
- Formalizzare una valutazione del livello di rischio e delle minacce

Risk Management

Il processo di identificazione, controllo, e gestione dell'impatto di alcuni eventi in rapporto con il valore dei beni protetti.

Il primo step è la Vulnerability Assessment:

il processo rivolto a identificare le criticità dal punto di vista dell'information security e valutare qual è il grado di protezione al momento della valutazione rispetto alle vulnerabilità intrinseche di tutte le componenti interessate nel contesto di riferimento.

Con il secondo step si effettua il Risk Assessment:

il processo che consente di determinare il Rischio associato a situazioni ben definite e a minacce conosciute.

Successivamente si esegue la Mitigazione del Rischio Informatico:

si mettono in pratica una serie di azioni e strategie per minimizzare i rischi rilevati nella fase della valutazione. Queste dipendono dai risultati delle analisi effettuate.

I rischi che rimangono dopo la Mitigazione diventano il Rischio Residuale.

Esercitazione

NESSUS VULNERABILITY ASSESSMENT

Su Kali Linux:

1. Download del Framework da:
   https://www.tenable.com/products/nessus/select-your-operating-system
2. Aprire Terminal: **cd Downloads**
3. Installare il framework: **dpkg - i Nessus-x.y.z-debian6_amd64.deb**
4. lanciare Nessus: **/bin/systemctl start nessusd.service**
5. Aprire Browser **https://127.0.0.1:8834**
6. Registrare "**Nessus Essential**" come "**Educators, students**"
7. Attivare la licenza con il codice che arriva per email e Creare un utente
8. Eseguire la scansione su tutte le macchine virtuali
9. Analizzare i risultati per intraprendere le contromisure

Meccanismi di Autenticazione

Alcuni metodi per implementare dei meccanismi di autenticazione robusti:

- Generazione e archiviazione di password sicure
- Configurazioni di dominio e group policy
- Rafforzare i servizi di autenticazione (es: RADIUS)
- Implementazioni di autenticazione biometrica e multifattore
- Cifratura delle credenziali e sistemi TPM
- Chiavi USB, firme e token digitali
- Generazione di password OTP e sistemi SSO
- Servizi trusted e gestione dei certificati digitali
- Tecniche di autenticazione per reti locali e geografiche
- Tecniche di autenticazione per servizi amministrativi e server

Proteggere la Rete Informatica

Le principali strategie per difendere una Rete Informatica:

- Configurare correttamente i sistemi di sicurezza IDS e IPS
- Applicare diverse tipologie di analisi in-band e out-of-band
- Configurare i firewall di rete e tecniche mirate e avanzate
- Installare Antivirus di rete per il rilevamento di signature malevole
- Realizzare la segregazione delle reti e la ridondanza dei collegamenti
- Implementare l'hardening dei dispositivi e dei servizi di rete
- Mettere in atto il mascheramento dei servizi e della topologia della rete
- Configurare correttamente i protocolli e le connessioni sicure
- Impostare la protezione delle reti WiFi WEP e WPA2
- Attuare le misure per proteggersi da un attacco DDoS
- Zero Trusted Configuration

Proteggere le Applicazioni e i Servizi

Le principali strategie per rendere più sicure le applicazioni e i servizi:

- Implementare sistemi per il controllo degli aggiornamenti e patch di sicurezza
- Configurare Firewall applicativi avanzati
- Attivare protezioni per attacchi specifici orientati al web
- Effettuare la chiusura e la mitigazione manuale delle falle di sicurezza
- Realizzare l'Hardening del sistema operativo e delle applicazioni di sistema
- Impostare sistemi di sandboxing e di controllo di macchine virtuali
- Configurare software antivirus e controlli di integrità periodici
- Utilizzare sistemi euristici per il rilevamento di backdoor e di attività sospette
- Avviare l'auditing degli eventi e sistemi per il logging centralizzato
- Abbonarsi alle newsletter di sicurezza e di prevenzione di attacchi zero day

Proteggere i Dati e le Postazioni

Alcuni passi per proteggere i dati e le postazioni utente:

- Verificare la sicurezza fisica essenziale e dell'ambiente operativo
- Utilizzare tecniche e strumenti di crittografia per file e dischi di archiviazione
- Proteggere efficacemente il case o l'armadio rack
- Realizzare l'Hardening del sistema BIOS/UEFI
- Impostare le Policy di dominio per la protezione della postazione
- Configurare sistemi di ripristino periodico e di controllo della sicurezza remoto
- Prevedere la tecnica corretta per la distruzione dei dati sensibili e dei dispositivi dismessi
- Redigere le norme per la protezione di dispositivi mobile e gestione remota
- Formulare le procedure utente per l'utilizzo della postazione

Continuità del Servizio e Disaster Recovery

Alcuni soluzioni per assicurare la Continuità del Servizio e il Disaster Recovery:

- Sistemi avanzati per il backup locale e geografico
- Sistemi di distribuzione dei dati e mirroring via rete
- Ridondanza dell'insfrastruttura di rete e degli apparati
- Ridondanza dei dischi e sistemi RAID
- Bilanciamento di carico e clustering dei servizi
- Tecniche e meccanismi di Switchover e Failover
- Dispositivi di generazione e continuità elettrica
- Formulazione delle procedure di gestione del disastro

Metodologia strutturata

La metodologia strutturata proposta per mitigare i rischi prevede l'adozione di un modello organizzativo secondo un approccio per casi.

Per ogni caso viene effettuata un'analisi di rischio collegata all'evento, viene proposto un metodo per permettere di documentare l'evento stesso ed infine vengono descritte le modalità di trattamento del reperto informatico, utili anche al fine di tracciare il fenomeno.

I casi che vengono presi in esame sono:

- accesso abusivo ad un sistema informatico
- violazione della casella di posta elettronica
- sottrazione di dati relativi a proprietà industriale
  - operata da dipendenti o collaboratori interni
- furto di sistemi informatici

Metodologia strutturata

Di seguito il dettaglio delle attività proposte:

(a) evento - descrizione e riferimento normativo;
(b) identificazione delle possibili cause dell'evento;
(c) identificazione delle possibili conseguenze dell'evento;
(d) classificazione di rischio associato all'evento, secondo una scala di tipo qualitativo.

Verranno utilizzati i valori L (basso), M (medio), H(alto);

(e) azioni atte a mitigare il livello di rischio rilevato.
(f) livello di rischio calcolato al termine del punto e).
(g) modalità di trattamento del reperto informatico, utili a documentare il fenomeno.

Accesso abusivo:
Analisi del rischio

L'Accesso abusivo ad un sistema informatico o telematico è un reato e come tale è sanzionato ai sensi dell'Art. 615-ter c.p. secondo cui *"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni[..]"*

Cause

1. SQL/Code injection
2. sistemi non protetti mediante tecnologie di protezione/controllo di accesso
3. insufficienza dei sistemi di protezione/controllo di accesso (es. nessuna limitazione minima sulla lunghezza e/o complessità della password, configurazione errata dei sistemi);
4. mancati aggiornamenti dei sistemi di protezione/controllo di accesso, utili alla risoluzione di vulnerabilità note (come sql injection), spesso sfruttate dagli attaccanti;
5. utilizzo di keylogger (si presuppone in questo caso la disponibilità di accesso fisico alla macchina).

Accesso abusivo:
Analisi del rischio

Conseguenze

Le principali conseguenze di tale evento riguardano la perdita di tutti i principali elementi portanti del concetto stesso di sicurezza informatica:

1. indisponibilità dei servizi
2. violazione dell'integrità dei dati (come la loro alterazione o cancellazione)
3. furto di dati
4. violazione della privatezza degli utilizzatori dei sistemi, che potrebbe sfociare in casi di furto di identità nel caso in cui le informazioni personali degli utenti a cui si riesce ad accedere siano molto dettagliate.

Livello di rischio calcolato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	H	1÷4:H	H
2	L	1÷2:M 3÷4:L	L
3	H	1÷3:H 4:M	H
4	H	1÷3:H 4:M	H
5	M-L	1÷3:H 4:M	M

Accesso abusivo:
Azioni per mitigare il livello di rischio

Per poter mitigare i livelli di rischio individuati occorre sostanzialmente ridurre la probabilità di occorrenza delle cause degli attacchi. In particolare è necessario:

- aggiornare costantemente i sistemi di controllo di accesso, così da ridurre la vulnerabilità agli attacchi noti;
- monitorare il funzionamento di tutti i sistemi, così da poter verificare preventivamente la presenza di errate configurazioni e apportare le dovute correzioni prima che si verifichi un attacco;
- imporre vincoli rigidi di protezione logica e fisica sui sistemi, come ad esempio password lunghe almeno 8 caratteri, da aggiornare periodicamente, sistemi antivirus abilitati e funzionanti, controllo di accesso fisico ai locali.

Livello di rischio mitigato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	L	1÷4:H	M
2	L	1÷2:M 3÷4:L	L
3	L	1÷3:H 4:M	M
4	L	1÷3:H 4:M	M
5	L	1÷3:H 4:M	L

Accesso abusivo:
Trattamento del reperto

In questo caso possiamo distinguere tre reperti informatici, presupponendo di aver già implementato le misure di mitigazione descritte:

1. copia forense del disco del personal computer del dipendente
2. file di log contenenti attività degli utenti sul server
3. filmato di videosorveglianza della stanza in cui risiede il sistema.

Nel primo caso, la costruzione di una timeline delle attività all'interno del personal computer, con particolare focus sul periodo di tempo indicato in fase di segnalazione, unito all'analisi del filmato di videosorveglianza può portare all'individuazione del soggetto che ha compiuto tali azioni e dei dati che sono stati visionati/prelevati abusivamente dal sistema. Tale timeline risulta utile anche nel caso di accesso da remoto.

Nel secondo caso, l'analisi dei file di log risulta molto utile per capire chi si è introdotto e a quali file ha avuto accesso.

Il terzo reperto normalmente serve ad identificare persone fisiche che hanno avuto accesso ai sistemi nella finestra temporale individuata, per cui risulterebbe ad esempio inutile nel caso di un accesso abusivo da remoto.

Violazione della casella di posta elettronica: Analisi del rischio

Violazione della casella di posta elettronica, tale reato è sanzionato ai sensi dell'Art.616 c.p., secondo cui *"Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516.[..]*

Cause

1. utilizzo di account/pc condiviso
2. memorizzazione automatica delle credenziali di accesso alla casella di posta
3. mancata esecuzione del logout
4. password banale (es. parole prese da dizionario, nomi di persone/città)
5. utilizzo della postazione di lavoro del dipendente in sua assenza (es. malattia)
6. accesso abusivo

Violazione della casella di posta elettronica: Analisi del rischio

Conseguenze

Le principali conseguenze della violazione di una casella di posta elettronica si possono riassumere in:

1. violazione privacy dell'utilizzatore di tale casella;
2. possibile esposizione di informazioni riservate/critiche per il business aziendale o confidenziali.

Livello di rischio calcolato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	H	1:M 2:H	H
2	H	1:M 2:H	H
3	H	1:M 2:H	H
4	H	1:M 2:H	H
5	H	1:M 2:H	H

Violazione della casella di posta elettronica:
Azioni per mitigare il livello di rischio

Per poter mitigare i livelli di rischio occorre sostanzialmente ridurre la probabilità di occorrenza degli errori umani individuati. In particolare è necessario:

- inibire l'accesso alla casella di posta aziendale dall'esterno dell'azienda.
- nel caso in cui il punto precedente non fosse realizzabile, produrre e far rispettare un regolamento stretto per la consultazione della casella di posta all'esterno dell'ambiente lavorativo;
- non autorizzare la consultazione della casella email attraverso un pc utilizzato da più utenti
- divieto di memorizzare automaticamente le credenziali di accesso alla casella di posta
- imporre limitazioni sulla complessità minima per la password
- utilizzo di inoltro e/o riposta automatici
- utilizzo di meccanismo di logout automatico dall'account di posta se si riscontra inattività dell'utente
- utilizzo di meccanismo di autenticazione con verifica delle credenziali a doppia componente

Livello di rischio mitigato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	L	1:M 2:H	L
2	L	1:M 2:H	L
3	L	1:M 2:H	L
4	M	1:M 2:H	M
5	L	1:M 2:H	L

Violazione della casella di posta elettronica: Trattamento del reperto

In questo caso possiamo distinguere due reperti informatici, presupponendo di aver già implementato le misure di mitigazione descritte:

1. copia forense del disco del personal computer del dipendente
2. file di log contenenti attività dell'utente sul server di posta

Nel primo caso, la costruzione di una timeline delle attività all'interno del personal computer, con particolare focus sulle attività compiute dall'utente sul client di posta o sul browser possono essere utili per risalire alla causa che ha permesso l'accesso abusivo alla casella di posta ed eventualmente (nel caso di utilizzo del client) comprendere le azioni dell'utente al fine di individuare, ad esempio, l'inoltro di informazioni riservate a persone esterne all'azienda.

Nel secondo caso, l'analisi dei file di log risulta molto utile per comprendere le attività effettuate dall'utente sul server di posta quando ad esempio non è stato possibile risalire alla postazione da cui si è collegato.

Sottrazione di proprietà industriale: Analisi del rischio

Si applica il reato di furto perchè si considera che i dati prelevati siano contenuti all'interno di un supporto e quindi l'oggetto del furto è il supporto e non il dato.

Cause

1. mancanza di supervisione dei collaboratori interni
2. mancanza di sistemi di controllo di accesso (fisico e logico) ai sistemi e/o ai locali contenenti dati classificati come proprietari
3. possibilità di accesso alla rete aziendale e ai sistemi senza specifici livelli di autorizzazione definiti
4. mancato controllo in ingresso e in uscita dei sistemi in possesso dei dipendenti
5. mancato monitoraggio dell'utilizzo di supporti rimovibili per il trasferimento di informazioni
6. mancato divieto di accesso a piattaforme di file hosting/sharing (come ad esempio Drobpox, Google Drive)
7. recupero di dispositivi o informazioni impropriamente smaltiti
8. intercettazione delle comunicazioni all'interno della rete aziendale
9. errata configurazione dei livelli di autorizzazione (ad es. impiegato che accede ad informazioni confidenziali su accordi finanziari)
10. mansioni e/o aree di responsabilità non correttamente definite, che potrebbero indurre all'errata autorizzazione all'accesso ai dati
11. mancanza o insufficienza di procedure per mantenere in ordine la postazione di lavoro (scrivania e computer).

Sottrazione di proprietà industriale:
Analisi del rischio

Conseguenze

Le conseguenze di tali vulnerabilità riguardano principalmente l'accesso di tali dati da parte di persone non autorizzate che potrebbero utilizzarli per diversi scopi.

Di seguito le conseguenze di maggior rilievo:

1. furto di progetti in via di sviluppo, che potrebbero venir copiati e completati da una azienda concorrente, che otterrebbe quindi un vantaggio competitivo
2. esposizione dell'azienda a ricatti da parte del dipendente/collaboratore interno, che potrebbe esigere dei benefici personali o economici per la restituzione/distruzione dei dati di cui è in possesso
3. danno di immagine per l'azienda.

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	H	1÷3:H	H
2	L	1÷3:H	L
3	L	1÷3:H	L
4	M	1÷3:H	M
5	H	1÷3:H	H
6	H	1÷3:H	H
7	H	1÷3:H	H
8	L	1÷3:H	L
9	M	1÷3:H	M
10	M	1÷3:H	M
11	H	1÷3:H	H

Livello di rischio calcolato

H: alto M: medio L: basso

Sottrazione di proprietà industriale:
Azioni per mitigare il livello di rischio

Per poter mitigare i livelli di rischio individuati occorre ridurre la probabilità di occorrenza delle cause individuate. In particolare è necessario:

- definire la supervisione dei collaboratori interni
- tutti i locali e i sistemi devono essere dotati di un sistema di controllo di accesso
- l'accesso alla rete aziendale va vietato ai collaboratori interni, o può essere permesso mediante specifico sistema di livelli di autorizzazione. Per quanto concerne i dipendenti invece, l'accesso alle informazioni va regolato in modo tale che ogni dipendente sia autorizzato esclusivamente all'accesso a dati inerenti la sua mansione lavorativa
- controllo in ingresso ed in uscita, mediante addetti alla sicurezza, di eventuali dispositivi non autorizzati in possesso del dipendente (Es. Hard disk esterno, pen drive)
- monitoraggio continuo dell'avvenuta copia di informazioni su dispositivi rimovibili.
- utilizzo di sistema proxy aziendale per negare l'accesso a siti web che consentono la memorizzazione, anche temporanea, di file
- definire accuratamente lo smaltimento di dispositivi o informazioni non più utili (es. effettuare formattazione a più passate dei supporti rimovibili non più utili)
- definire correttamente ruoli e responsabilità per ogni dipendente/collaboratore, così da consentire l'accesso a quest'ultimo solo alle informazioni realmente necessarie per la sua mansione lavorativa
- istruire i dipendenti al mantenimento in ordine e in sicurezza della scrivania e della postazione pc (Es. Utilizzo della metodologia 6S, logout quando ci si allontana dalla postazione di lavoro, tenere il desktop in ordine)

Sottrazione di proprietà industriale:
Azioni per mitigare il livello di rischio

Livello di rischio mitigato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	L	1÷3:H	L
2	L	1÷3:H	L
3	L	1÷3:H	L
4	M	1÷3:H	M
5	L	1÷3:H	L
6	L	1÷3:H	L
7	L	1÷3:H	L
8	L	1÷3:H	L
9	L	1÷3:H	L
10	L	1÷3:H	L
11	M	1÷3:H	M

Sottrazione di proprietà industriale: Trattamento del reperto

In questo caso possiamo distinguere quattro reperti informatici, presupponendo di aver già implementato le misure di mitigazione descritte:

1. copia forense del dispositivo (Es disco del dipendente o dispositivo smaltito)
2. file di log contenenti attività sul server (Es. accesso a cartelle condivise, copia dei file)
3. file di log degli accessi ottenuto dal sistema di lettore badge
4. filmato di videosorveglianza della stanza in cui risiede il sistema.

Nel primo caso, la costruzione di una timeline delle operazioni effettuate sul dispositivo, con particolare focus sul periodo di tempo indicato in fase di segnalazione, unito all'analisi del filmato di videosorveglianza può portare all'individuazione del soggetto che ha compiuto tali azioni e dei dati che sono stati visionati/prelevati dal sistema.

Nel secondo caso, l'analisi dei file di log risulta molto utile per capire chi ha visionato specifici insiemi di dati e se ne ha effettuato una copia, così da risalire all'utente ed operare in seguito sul suo personal computer alla ricerca di eventuali tracce.

Nel terzo caso, tale reperto è utile, insieme al quarto, per capire chi ha avuto accesso a quale stanza (Es. ufficio, stanza smaltimento) e in quale esatto momento.

Il quarto reperto servirà anche a dare un volto alla persona (poichè il badge potrebbe essere stato sottratto al proprietario, quindi da solo non fornisce prova certa)

Furto di sistemi informatici: Analisi del rischio

In questo caso vengono considerati i dispositivi forniti dall'azienda al proprio dipendente al fine di permetterne l'esecuzione dell'attività lavorativa, come ad esempio notebook aziendale ed eventualmente anche il cellulare.
Tale reato rientra all'interno della definizione di furto, che è sanzionato ai sensi dell'Art.624 c.p., secondo cui *"Chiunque s'impossessa della cosa mobile altrui, sottraendola a chi la detiene, al fine di trarne profitto per sè o per altri, è punito con la reclusione[..].*

Cause

1. incuria del dipendente;
2. furto domestico o durante viaggio/trasferta del dipendente;
3. mancanza o insufficienza di adeguate procedure per il mantenimento in condizione sicura dei dispositivi assegnati.

Furto di sistemi informatici:
Analisi del rischio

Conseguenze

Le principali conseguenze del furto di dispositivi aziendali si possono riassumere in:

1. esposizione di segreti aziendali/industriali: si pensi a documentazione contenuta all'interno del dispositivo e classificata come Business only o Confidential
2. impossibilità o difficoltà nell'esecuzione delle attività lavorative da parte del dipendente
3. possibile danno economico per l'azienda, che deve fornire al dipendente un dispositivo in sostituzione di quello sottratto.

Livello di rischio calcolato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	H	1:H 2÷3:M	H
2	H	1:H 2÷3:M	H
3	M	1:H 2÷3:M	M

Furto di sistemi informatici:
Azioni per mitigare il livello di rischio

Per poter mitigare i livelli di rischio individuati occorre sostanzialmente incrementare il livello di attenzione del dipendente nei confronti dei dispositivi ad esso affidati, mediante l'utilizzo di adeguate procedure e misure di sicurezza. In particolare è necessario:

- protezione fisica dei dispositivi (es. messa in sicurezza all'interno di cassaforte del dispositivo quando ci si allontana dalla stanza d'albergo, utilizzo del cavo antifurto di tipo Kensington)
- utilizzo di sistema di controllo di accesso, che nel caso di controllo di accesso alla rete aziendale deve essere notevolmente complesso, come ad esempio autenticazione alla VPN con utilizzo di certificato al posto della (meno sicura) password
- utilizzo di tecniche di cifratura (come ad esempio BitLocker)
- utilizzo di sistema di backup centralizzato, così da permettere la disponibilità dei documenti utili al lavoro del dipendente anche in seguito al furto
- predisposizione di meccanismo di blocco/disabilitazione del dispositivo con relativa eliminazione dei dati contenuti all'interno utilizzabile da remoto.

Livello di rischio mitigato

H: alto

M: medio

L: basso

Causa	Probabilitá di occorrenza	Conseguenze	Livello di rischio
1	L	1:H 2÷3:M	L
2	L	1:H 2÷3:M	L
3	M	1:H 2÷3:M	M

Furto di sistemi informatici:
Trattamento del reperto

In questo caso possiamo distinguere tre reperti informatici:

1. analisi di eventuali file di log contenenti attività degli utenti sul server, nel caso in cui ci si renda conto che siano riusciti ad accedere alla rete aziendale utilizzando i dispositivi oggetto di furto
2. tracciato degli spostamenti del cellulare ed elenco delle chiamate effettuate/ricevute successivamente al furto (mediante collaborazione con il provider telefonico). Nel caso in cui anche il notebook fosse dotato di connessione GSM le considerazioni fatte valgono anche per il notebook
3. copia forense del dispositivo recuperato (sia esso il personal computer o il cellulare) ed ulteriori investigazioni secondo necessità.

Nel primo caso, l'analisi dei file di log risulta molto utile per capire chi si è introdotto (tracciare la connessione) e a quali file ha avuto accesso.

Nel secondo caso, l'analisi di tali tracciati può essere utile a rintracciare chi ha perpetrato il furto e recuperare il dispositivo.

Nel terzo caso, la costruzione di una timeline delle operazioni effettuate con il personal computer o il cellulare può essere utile per capire se sono stati letti/copiati file critici per il business aziendale, o ricostruire le operazioni effettuate da chi deteneva i dispositivi.

Security Monitoring

Definizioni

Strumenti

Security Monitoring

Il monitoraggio della sicurezza (Security Monitoring), talvolta denominato "Security Information Monitoring (SIM)" o "Security Event Monitoring (SEM)", implica la raccolta e l'analisi di informazioni per rilevare comportamenti sospetti o modifiche di sistema non autorizzate sulla tua rete, definendo quali tipi di comportamento dovrebbero generare avvisi e quindi adottare contromisure basate sugli avvisi, secondo necessità.

L'aumento della complessità che le aziende si trovano ad affrontare per proteggere le proprie informazioni e quindi il proprio business obbliga di fatto le aziende ad attivare un monitoraggio continuo della sicurezza, per mettere al sicuro le proprie informazioni e quindi il proprio business.

Data la natura onnipresente e inevitabile dei rischi alla sicurezza, per mantenere protetto il sistema sono indispensabili tempi di risposta rapidi ed è quindi **fondamentale un monitoraggio della sicurezza continuo e automatizzato per un rapido rilevamento delle minacce e l'adozione di contromisure.**

I principi secondo il NIST

Il NIST, all'interno del documento di linee guida "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" (SP 800-137), dà la seguente definizione di Information Security Continuous Monitoring:

"Information Security Continuous Monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions".

I componenti chiave di un ISCM sono:

- definizione di una strategia di monitoring
- definizione di un programma di monitoring
- implementazione del programma di monitoring
- analisi e report delle evidenze
- risposta alle evidenze
- revisione e modifica della strategia e del programma dell'ISCM

Secondo il NIST, l'ISCM deve essere allineato con il programma di risk management che coinvolge tutta l'organizzazione. Le misure di sicurezza individuate per la riduzione del rischio devono essere monitorate a più livelli.

I principali benefici

Tra i principali benefici derivanti dall'adozione del S.M. si possono citare:

- consolidamento delle informazioni rilevanti ai fini della Cybersecurity
- miglioramento dei livelli generali di sicurezza
- maggiore efficienza nella rilevazione e risposta alle anomalie/incidenti
- monitoraggio continuo del rispetto delle policy, procedure, configurazioni e standard aziendali
- automazione dei controlli sulle componenti tecnologiche critiche e relativa notifica dei malfunzionamenti
- miglioramento continuo della cyber security
- misurabilità del servizio
- riduzione del rischio
- attribuzione puntuale delle responsabilità
- veloce individuazione delle inefficienze e loro risoluzione

I prerequisiti

Affinché un'organizzazione possa adottare efficacemente un processo di monitoring, sono necessari alcuni requisiti di tipo organizzativo e tecnologico:

- Politica di log management
- Sinergia tra diverse funzioni interne
- Maturità della cyber security
- Risk assessment
- Gestione degli asset
- Gestione delle vulnerabiltà
- Approccio orientato alla difesa
- Team dedicato alla gestione operativa della sicurezza
- Committment aziendale

Cosa monitorare

Gli strumenti di monitoraggio della sicurezza posti all'interno dell'azienda possono essere divisi in due categorie:

1. sonde dedicate al monitoraggio

   Particolarmente utile per intercettare il traffico anomalo o malevolo o per monitorare i dispositivi che non gestisco i log (p.e. i dispositivi IoT e i sensori)

2. log di sistemi e applicazioni
   - **sistemi di sicurezza** (firewall, IPS, sistemi antimalware di qualsiasi tipo, VPN, web proxy, sistemi di autenticazione)
   - **sistemi operativi e DBMS**
   - **applicazioni e web service**

AlienVault OSSIM di AT&T

AlienVault Open Source Security Information and Event Management

1. **Asset Discover & Inventory**
   - Identificazione e Prioritizzazione degli asset
   - Rilevamento di asset non autorizzati
2. **Vulnerability Assessment**
   - Identificazione delle vulnerabilità degli asset, tramite utilizzo di database sulle vulnerabilità note
   - Valutazione più efficace delle risorse sfruttando una modalità di autenticazione dell'asset (ad esempio tramite SSH)
3. **Intrusion Detection**
   - Monitoraggio del traffico, dei messaggi di registro di sistema e delle attività dell'utente
   - Un host-based intrusion detection (HIDS) con funzioni aggiuntive di monitoraggio dell'integrità di file e controllo dei file di sistema
   - Un network-based intrusion detection (NIDS) che tramite un monitoraggio passivo della rete in cerca di potenziali attività dannose
4. **Behavioral Monitoring**
   - Un monitoraggio comportamentale fornisce dei modelli di traffico e dei flussi di dati NetFlow, utilizzati per rilevare anomalie che le semplici statistiche di rete non evidenziano
   - Monitoraggio continuo delle funzionalità e delle attività degli asset
5. **SIEM Event Correlation**
   - Aggregazione e analisi di log raccolti dalla rete e dagli asset

AlienVault OSSIM di AT&T

AlienVault Open Source Security Information and Event Management

I componenti dell'Architettura di suddividono in :

1. **SERVER: analizza e correla le informazioni ricevute dai sensori, agent e logger, e fornisce un'interfaccia web per la gestione della piattaforma**
2. **SENSORE (1..n): svolge, principalmente, due funzioni:**
   - Raccolta e normalizzazione delle informazioni grezze dalla rete
   - Invio dei dati al server

   La raccolta delle informazioni avviene in due modi:
   - Monitoraggio passivo del traffico di rete, attraverso l'uso di un NIDS
   - Monitoraggio delle attività di un host della rete attraverso un agent HIDS
3. **AGENT (1..n): la comunicazione tra un sensore e un host della rete avviene tramite un meccanismo client-server, ed in particolare fa uso di un agent installato sugli host.**
   Il software integrato con la piattaforma è OSSEC HIDS che esegue:
   - analisi dei log
   - intrusion detection (HIDS)
   - controllo di integrità dei file
   - monitoraggio dei file di sistema
   - rilevamento di rootkit
4. **LOGGER (1..n): archivia in modo sicuro i dati di ogni singolo evento, sia per conformità normative sia per successive analisi forensi (è presente nella versione a pagamento)**

AlienVault OSSIM di AT&T

Passi per installazione:

1. Scaricare l'immagine ISO dal sito https://cybersecurity.att.com/
2. Creare una Macchina Virtuale dall'immagine ISO (16 Gb RAM e 3 LAN)
3. Impostare l'Indirizzo IP dell'interfaccia
4. Aprire da un altro browser l'url: https://indirizzo_ip

Welcome to AlienVault OSSIM

Let's Get Started

1. NETWORK INTERFACES
2. ASSET DISCOVERY
3. DEPLOY HIDS
4. LOG MANAGEMENT
5. JOIN OTX

Configure Network Interfaces

The network interfaces in AlienVault OSSIM can be configured to run Network Monitoring or as Log Collection & Scanning. Once you've configured the interfaces you'll need to ensure that the networking is configured appropriately for each interface so that AlienVault OSSIM is either receiving data passively or has the ability to reach out to the desired network.

NIC	PURPOSE	IP ADDRESS	STATUS
eth0	Management	192.168.79.100	-
eth1	Network Monitoring	N/A	
eth2	Log Collection & Scanning	192.168.79.102	-

Information

- **Management:** The Management interface was configured on the OSSIM Console and allows you to connect to the web UI. This interface cannot be changed from the web UI.
- **Network Monitoring:** Passively listen for network traffic. Interface will be set to promiscuous mode. Requires a network tap or span. See Instructions on how to setup a network tap or span.
- **Log Collection & Scanning:** Collect or receive logs from your assets, run an asset scan, or deploy the HIDS agent. Requires routable access to your networks.
- **Not in Use:** Use this option if you do not want to use one of the network interfaces.

SKIP ALIENVAULT WIZARD

NEXT

Welcome to AlienVault OSSIM

Let's Get Started

1. NETWORK INTERFACES
2. ASSET DISCOVERY
3. DEPLOY HIDS
4. LOG MANAGEMENT
5. JOIN OTX

Scan & Add Assets

In order to begin monitoring your environment we must first find the assets in your network. There are three (3) ways you can add assets to monitor: you can scan your network using network ranges, import a CSV of assets in your network, or you can add assets manually.

Add Asset Manually

Hostname | IP | Select an Asset Type | + ADD

SCAN NETWORKS | IMPORT FROM CSV

Search

HOSTNAME	IP	TYPE
alienvault	192.168.79.100	Linux
Host-192-168-79-1	192.168.79.1	Select an Asset Type
Host-192-168-79-128	192.168.79.128	Select an Asset Type
Host-192-168-79-129	192.168.79.129	Select an Asset Type
Host-192-168-79-130	192.168.79.130	Windows
Host-192-168-79-131	192.168.79.131	Select an Asset Type
Host-192-168-79-2	192.168.79.2	Select an Asset Type
Host-192-168-79-200	192.168.79.200	Linux
Host-192-168-79-254	192.168.79.254	Select an Asset Type

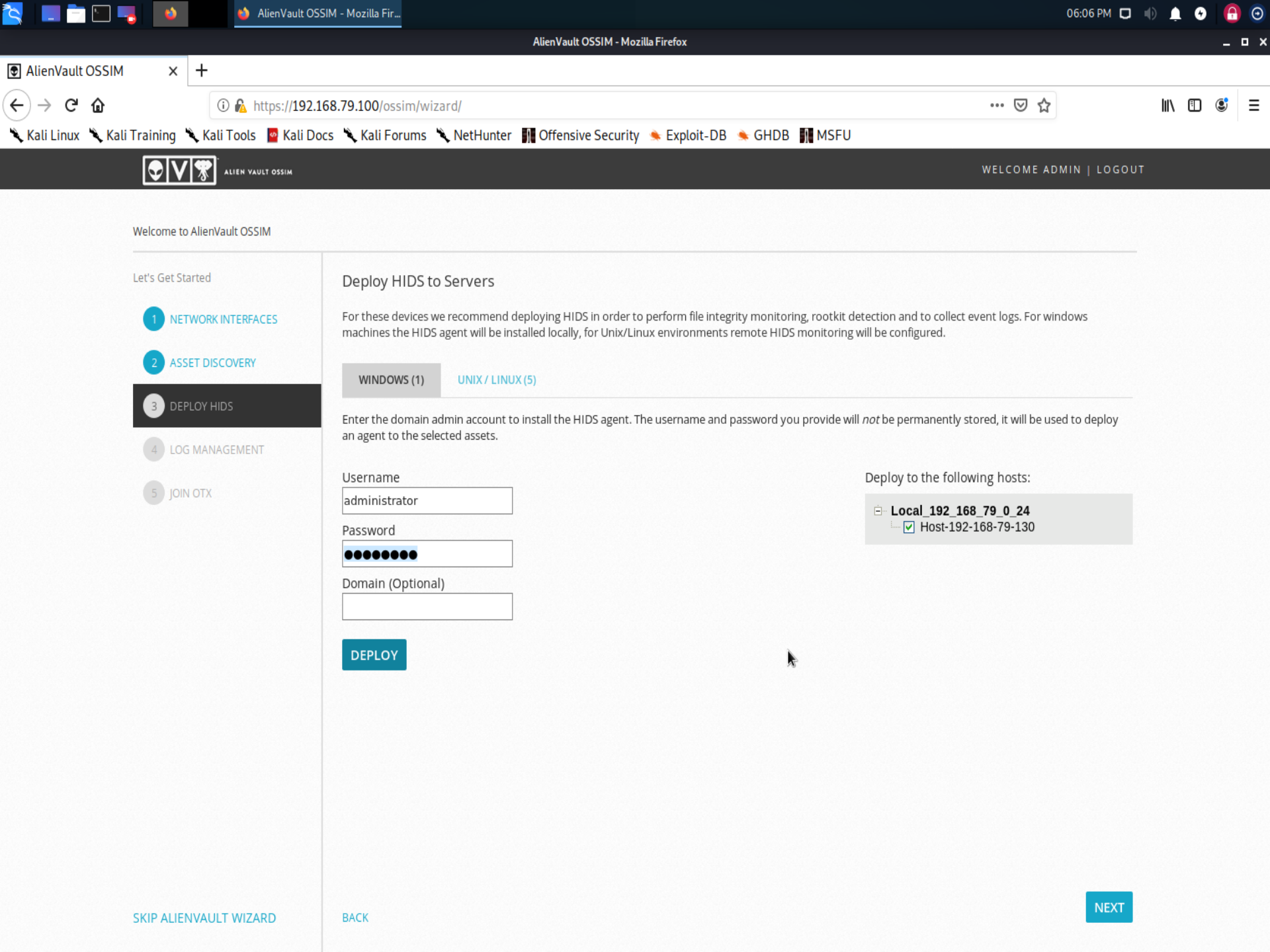
SHOWING 1 TO 9 OF 9 ASSETS

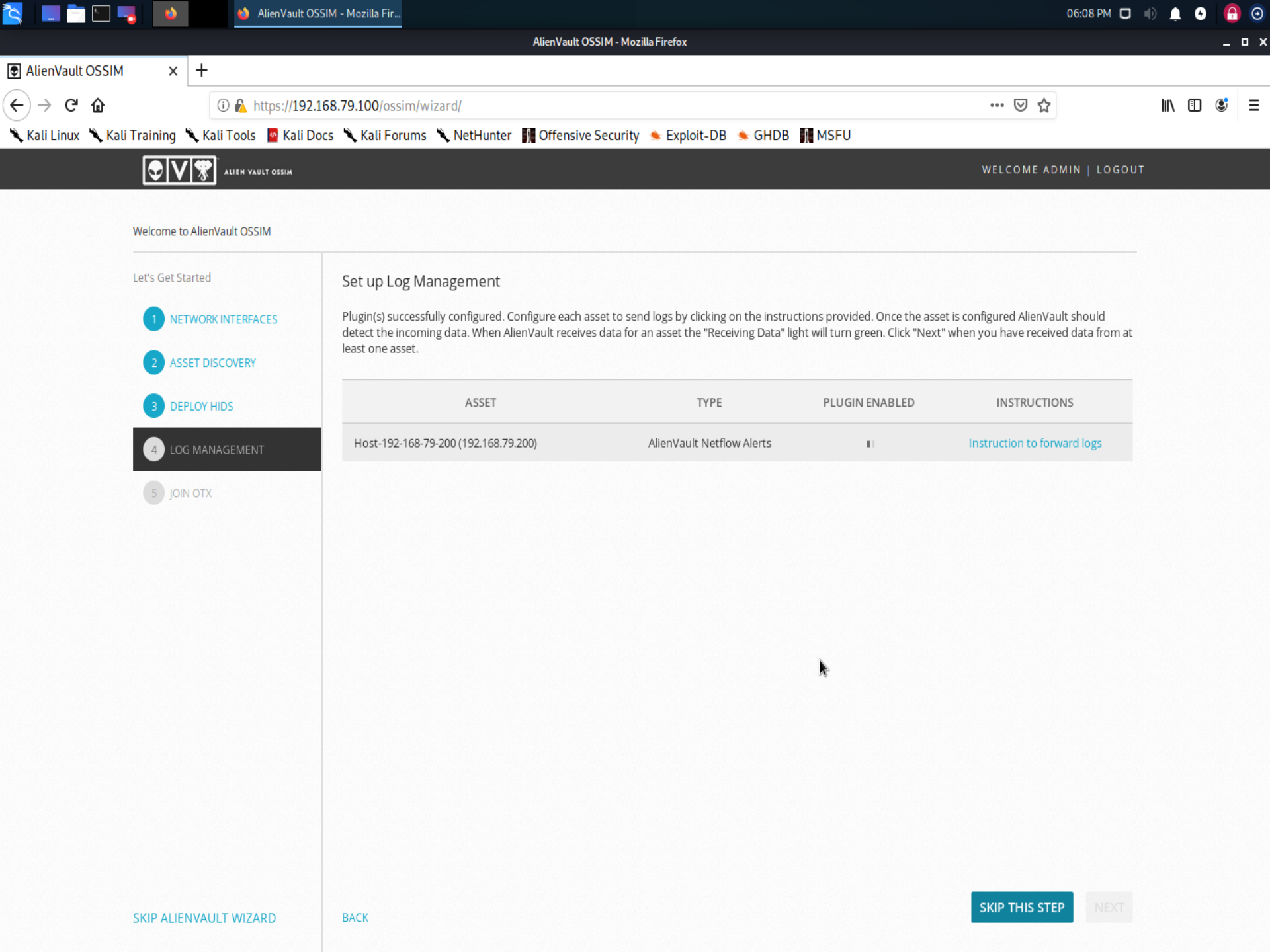
FIRST PREVIOUS 1 NEXT LAST

SKIP ALIENVAULT WIZARD

BACK

NEXT


AlienVault OSSIM - Mozilla Fir...
06:06 PM
AlienVault OSSIM - Mozilla Firefox
AlienVault OSSIM
https://192.168.79.100/ossim/wizard/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
ALIEN VAULT OSSIM
WELCOME ADMIN | LOGOUT
Welcome to AlienVault OSSIM
Let's Get Started
1 NETWORK INTERFACES
2 ASSET DISCOVERY
3 DEPLOY HIDS
4 LOG MANAGEMENT
5 JOIN OTX
Deploy HIDS to Servers
For these devices we recommend deploying HIDS in order to perform file integrity monitoring, rootkit detection and to collect event logs. For windows machines the HIDS agent will be installed locally, for Unix/Linux environments remote HIDS monitoring will be configured.
WINDOWS (1)
UNIX / LINUX (5)
Enter the domain admin account to install the HIDS agent. The username and password you provide will not be permanently stored, it will be used to deploy an agent to the selected assets.
Username
administrator
Password
Domain (Optional)
DEPLOY
Deploy to the following hosts:
Local_192_168_79_0_24
Host-192-168-79-130
SKIP ALIENVAULT WIZARD
BACK
NEXT


AlienVault OSSIM - Mozilla Fir...
06:08 PM
AlienVault OSSIM - Mozilla Firefox
AlienVault OSSIM
https://192.168.79.100/ossim/wizard/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
ALIEN VAULT OSSIM
WELCOME ADMIN | LOGOUT
Welcome to AlienVault OSSIM
Let's Get Started
1 NETWORK INTERFACES
2 ASSET DISCOVERY
3 DEPLOY HIDS
4 LOG MANAGEMENT
5 JOIN OTX
Set up Log Management
Plugin(s) successfully configured. Configure each asset to send logs by clicking on the instructions provided. Once the asset is configured AlienVault should detect the incoming data. When AlienVault receives data for an asset the "Receiving Data" light will turn green. Click "Next" when you have received data from at least one asset.
ASSET
TYPE
PLUGIN ENABLED
INSTRUCTIONS
Host-192-168-79-200 (192.168.79.200)
AlienVault Netflow Alerts
Instruction to forward logs
SKIP ALIENVAULT WIZARD
BACK
SKIP THIS STEP
NEXT

Welcome to AlienVault OSSIM

Let's Get Started

1. NETWORK INTERFACES
2. ASSET DISCOVERY
3. DEPLOY HIDS
4. LOG MANAGEMENT
5. JOIN OTX

Join the Open Threat Exchange - Threat Intelligence for You, Powered by the Community

What is OTX?

AlienVault Open Threat Exchange (OTX™) is the world's first truly open threat intelligence community. OTX enables you to strengthen your network security defenses with community-powered, accurate, and relevant threat intelligence. With AlienVault OTX, you can respond faster to changes in the threat landscape by receiving real-time, detailed threat intelligence from the community.

Why should I join?

OTX automatically instruments your USM and OSSIM deployments with actionable threat intelligence from community-generated "Pulses". Pulses are a group of indicators of compromise (IoCs) that have been identified as an active threat. These pulses provide specific, actionable information that help you to detect the latest threats in your environment.

How does it work?

Enabling OTX in your OSSIM installation will enable you integrate OTX Pulses containing the latest threat intelligence, including Indicators of Compromise (IoC) into your installation. When IOCs from a pulse interact with assets in your environment, a security event will be generated. These events will be used in correlation to provide you with deeper insight into the activities happening on your network. Additionally, you can contribute to the community by sending anonymous threat data to OTX. See what data is being sent to OTX.

To get the community-powered threat intelligence from OTX into your installation, sign up for an OTX Account. Once your email address has been verified, you will receive an OTX key to connect.

SIGN UP NOW

Enter your OTX key below to connect your account.

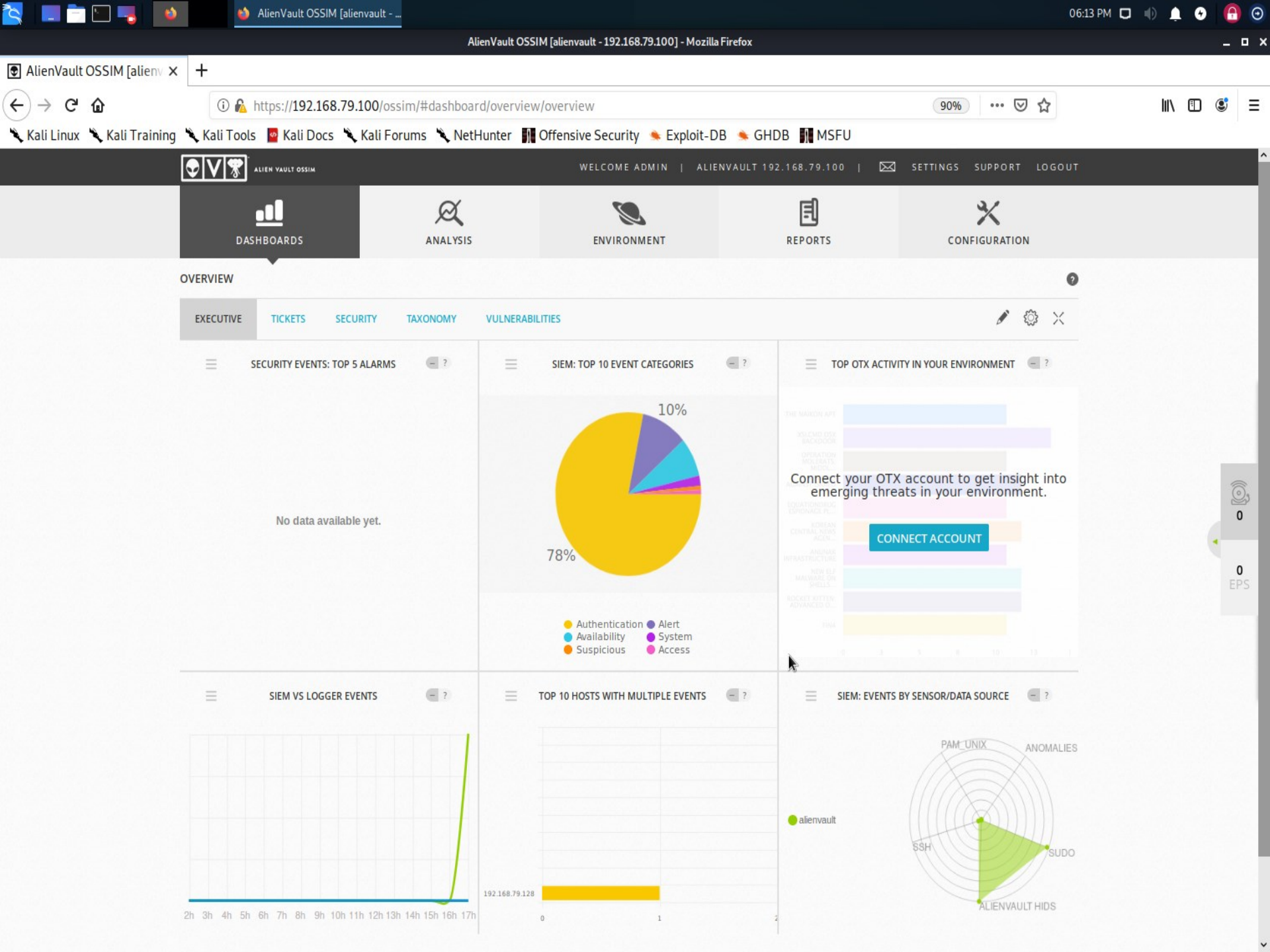
d1d062c77ad90c420ecd532264654ec637037af74446f7e543b2169ae0b8f886

SKIP ALIENVAULT WIZARD

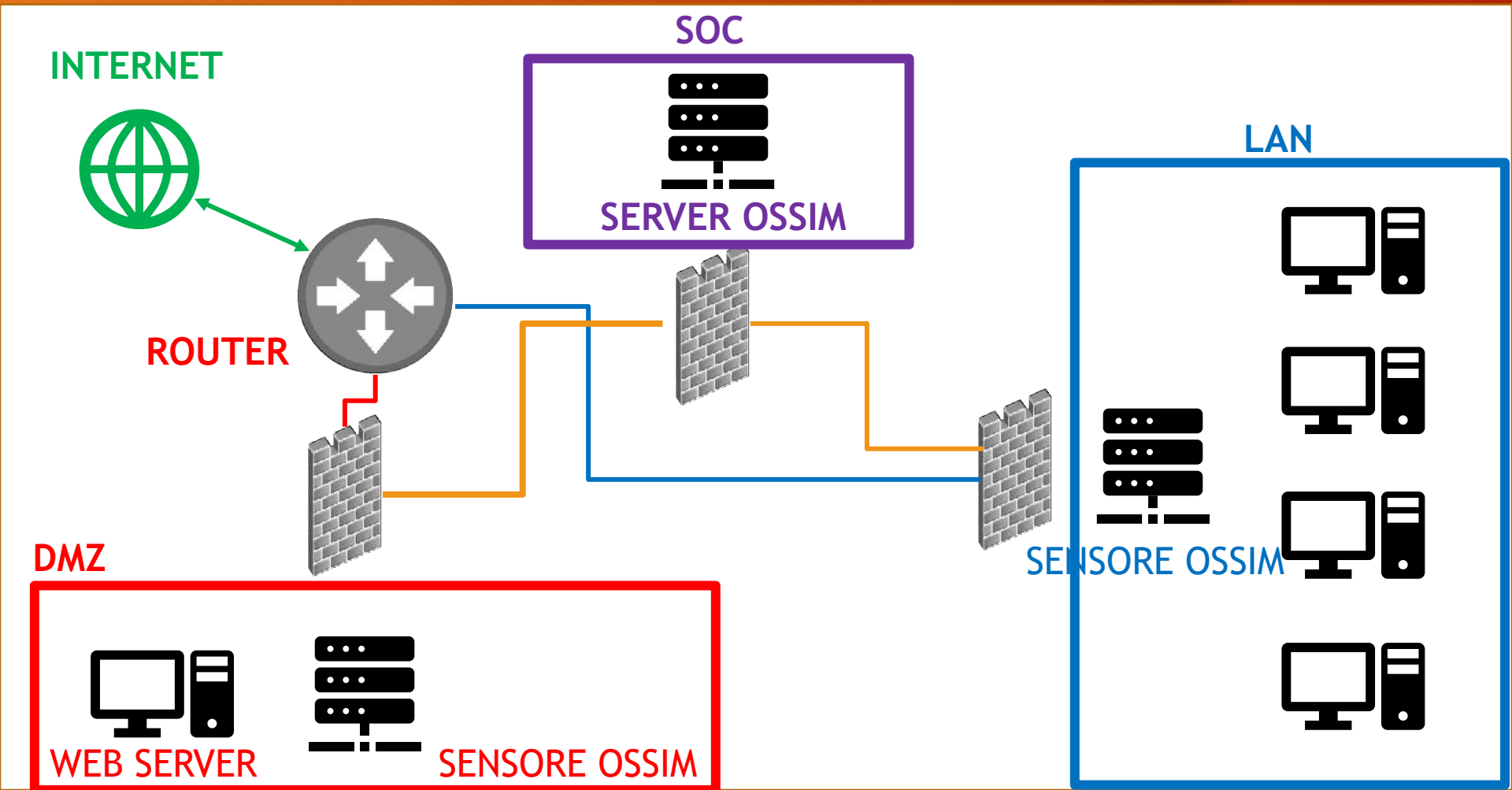
BACK

SKIP THIS STEP

NEXT


AlienVault OSSIM [alienvault - 192.168.79.100] - Mozilla Firefox
AlienVault OSSIM [alienv
https://192.168.79.100/ossim/#dashboard/overview/overview
90%
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
ALIEN VAULT OSSIM
WELCOME ADMIN | ALIENVAULT 192.168.79.100 | SETTINGS SUPPORT LOGOUT
DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
OVERVIEW
EXECUTIVE
TICKETS
SECURITY
TAXONOMY
VULNERABILITIES
SECURITY EVENTS: TOP 5 ALARMS
No data available yet.
SIEM: TOP 10 EVENT CATEGORIES
10%
78%
Authentication
Alert
Availability
System
Suspicious
Access
TOP OTX ACTIVITY IN YOUR ENVIRONMENT
Connect your OTX account to get insight into emerging threats in your environment.
CONNECT ACCOUNT
SIEM VS LOGGER EVENTS
2h 3h 4h 5h 6h 7h 8h 9h 10h 11h 12h 13h 14h 15h 16h 17h
TOP 10 HOSTS WITH MULTIPLE EVENTS
192.168.79.128
SIEM: EVENTS BY SENSOR/DATA SOURCE
PAM_UNIX
ANOMALIES
alienvault
SSH
SUDO
ALIENVAULT HIDS
0
0
EPS

Esempio


SOC
INTERNET
SERVER OSSIM
LAN
ROUTER
SENSORE OSSIM
DMZ
WEB SERVER
SENSORE OSSIM

Esercitazione

- Installare OSSIM e gli Agent HDIS su Windows e Linux
- Provare gli attacchi di Penetration Testing sulle macchine Windows e Linux
- Analizzare su OSSIM i risultati ottenuti
- Implementare regole di alert

Fine

vincenzo.calabro@unirc.it

linkedin.com/in/vincenzocalabro