SGBOX

CORRELAZIONE DEGLI EVENTI E ANALISI DEL COMPORTAMENTO NELL'INDIVIDUAZIONE DELLE MINACCE INFORMATICHE

Alberto Savoldelli
Co-founder & R&D SGBox

Cosa intendiamo per minacce informatiche

Includono, ma non sono limitate a

Virus/malware e oggetti correlati

Attacchi informatici di massa e mirati

Attacchi dall'interno del network

Comportamenti scorretti degli utenti

…

Possibili protezioni

- ✓ Perimetrali
- ✓ Su gateway
- ✓ Network
- ✓ Su device
- ✓ .....

Fonti di informazione

Questi strumenti di protezione ci forniscono informazioni

- Perimetrale

  Firewall, connessioni consentite/bloccate ma soprattutto informazioni “ad alto livello”

- Network

  IDS-IPS, potenziali attacchi (attenzione ai falsi positivi)

  Honeypot, fonte di eventi estremamente significativi

- Su gateway

  Antispam / application protection / IDS-IPS / DLP / WAF

- Su device

  Antivirus / Host IDS

  Informazioni su attività utente (policy e criteri di protezione)

Gestione delle informazioni

Troppe informazioni = nessuna informazione

- Informazioni slegate tra loro
  - Ogni strumento "vede" solo le informazioni di propria pertinenza.
  - Il firewall ci informa sulle connessioni.
  - L'antivirus segnala quanto rilevato sul endpoint.
  - l'IDS o HIDS segnala comportamenti anomali su network e host.
- Manca un filo conduttore
- Anche se le informazioni rappresentano eventi analoghi manca una normalizzazione di queste segnalazioni
  - (logon su unix ! = da logon su windows ! = da logon su switch)

Definizione di SIEM

- Il SIEM è lo strumento che centralizza le informazioni
- Le normalizza e le categorizza
- Riconosce famiglie di eventi
- Permette di definire scenari
- Valuta i comportamenti degli utenti
- Prende contromisure

Definizione di evento

- L’evento è la rappresentazione univoca di quanto comunicato da differenti tipologie di fonti dati
- Serve a riconoscere, indicando solo gli elementi significativi, una certa informazione

Logon windows? UNIX? (ev#4624 oppure ssh logon)
Privilege escalation? (ev#4672 oppure su)
…

Correlazione degli eventi

Correlare significa definire un legame tra eventi per riconoscere un determinato scenario

- Esempio (fonte dati: server di autenticazione / host)

  Rilevo un tentativo fallito di autenticazione. *È un'informazione utile?*

  Rilevo 100 tentativi falliti di autenticazione da parte dello stesso utente in 5 minuti. *Cambia qualcosa rispetto a prima? Cosa ci suggerisce?*

- Non stiamo correlando, stiamo riconoscendo. Proviamo a correlare:

  Dopo aver rilevato 100 tentativi falliti, rilevo un evento di autenticazione dello stesso utente sullo stesso (o un altro) servizio. Cosa ci suggerisce?

Correlazione degli eventi

- Esempio (Fonte dati: auth. server / host)

  Rilevo la connessione di un utente ad un servizio pubblicamente accessibile da un IP geolocalizzato in Italia.

  Entro 6 ore rilevo la connessione dello stesso utente da un IP geolocalizzato in un altra nazione.

- Esempio (Fonte dati: firewall, auth server / host)

  Rilevo la creazione/modifica di una regola sul FW relativa ad un server in orario non lavorativo.

  Rilevo una connessione al server dall'esterno.

- Esempio (Fonte dati: server VPN e policy server e auth. server)

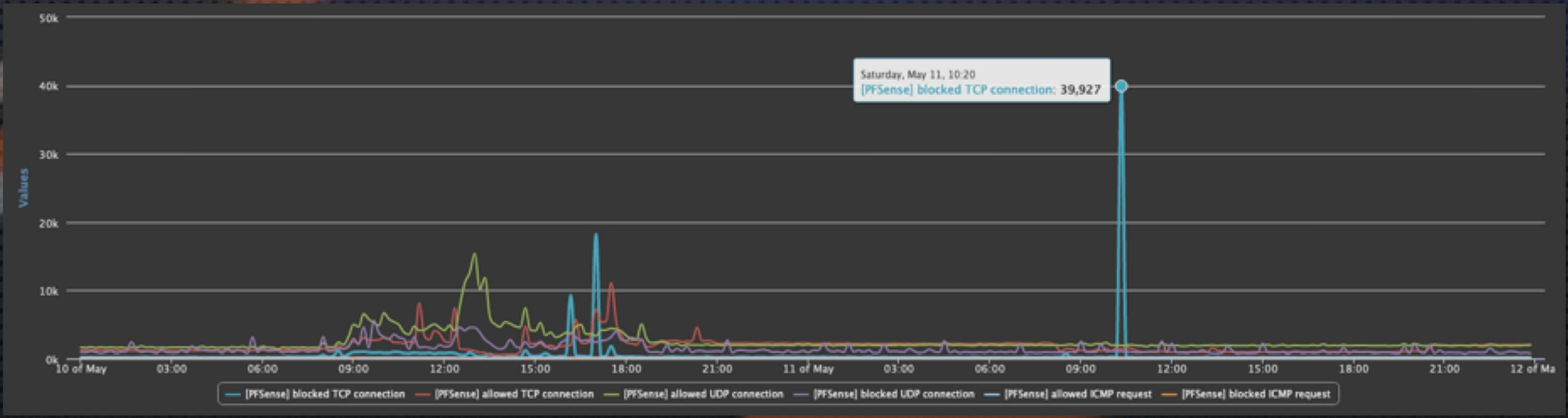
  Rilevo l'autenticazione di un amministratore via VPN.

  Rilevo la modifica di privilegi di un utente da parte di quell'amministratore.

  Rilevo la connessione di quello stesso utente su un servizio critico.

Analisi del comportamento

- Negli esempi precedenti abbiamo correlato informazioni raccolte da fonti dati presenti nella nostra rete
- Queste informazioni descrivono ciò che si sta verificando
- Anche la quantità di queste informazioni può fornirci informazioni interessanti



Esempio fonte dati: firewall

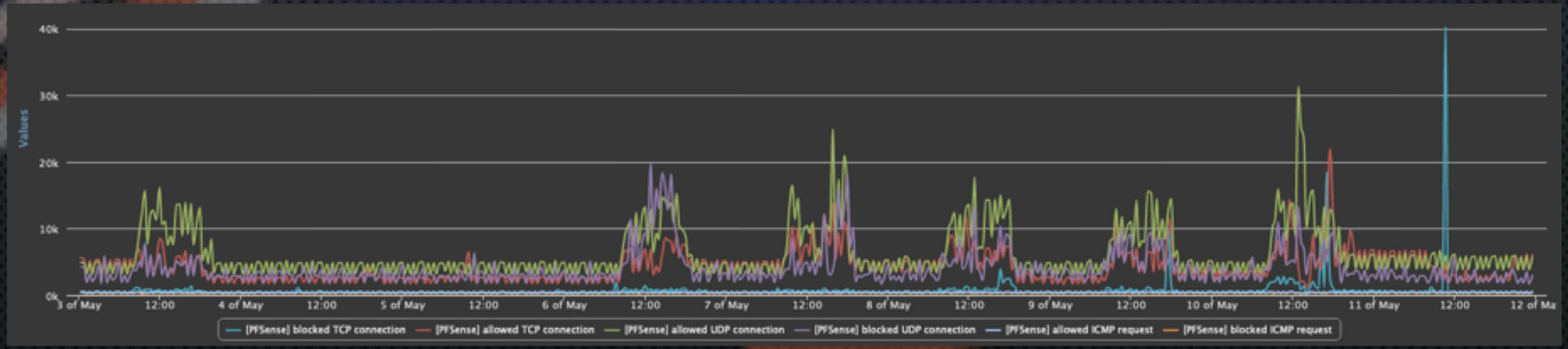
Analisi del comportamento

L'esempio precedente può essere rilevato anche con una regola, o semplicemente con un riconoscimento (valida se rilevo + di 1000 eventi in 10 min. Qui ne abbiamo 40k…)

Con la regola possiamo rilevare questo scenario, ma come possiamo capire se questo evento è normale?

Cosa significa "normale"?

- Che si è già verificato nello stesso intervallo di tempo.
- Che si ripete con analoga numerosità in un intervallo di tempo o in una posizione nel tempo.



Analisi del comportamento

- Oltre a valutazioni sui volumi, può essere utile associare ad un evento un rischio
- Può essere inoltre utile associare l'evento ad un utente (e di conseguenza un rischio ad un utente)
- Esempio (Fonte dati: server di autenticazione / host)

  Rilevo la connessione di un utente ad un server (servizio, risorsa, ecc.) in una certa fascia oraria.

  In passato quell'utente non si è mai connesso in quella fascia oraria.

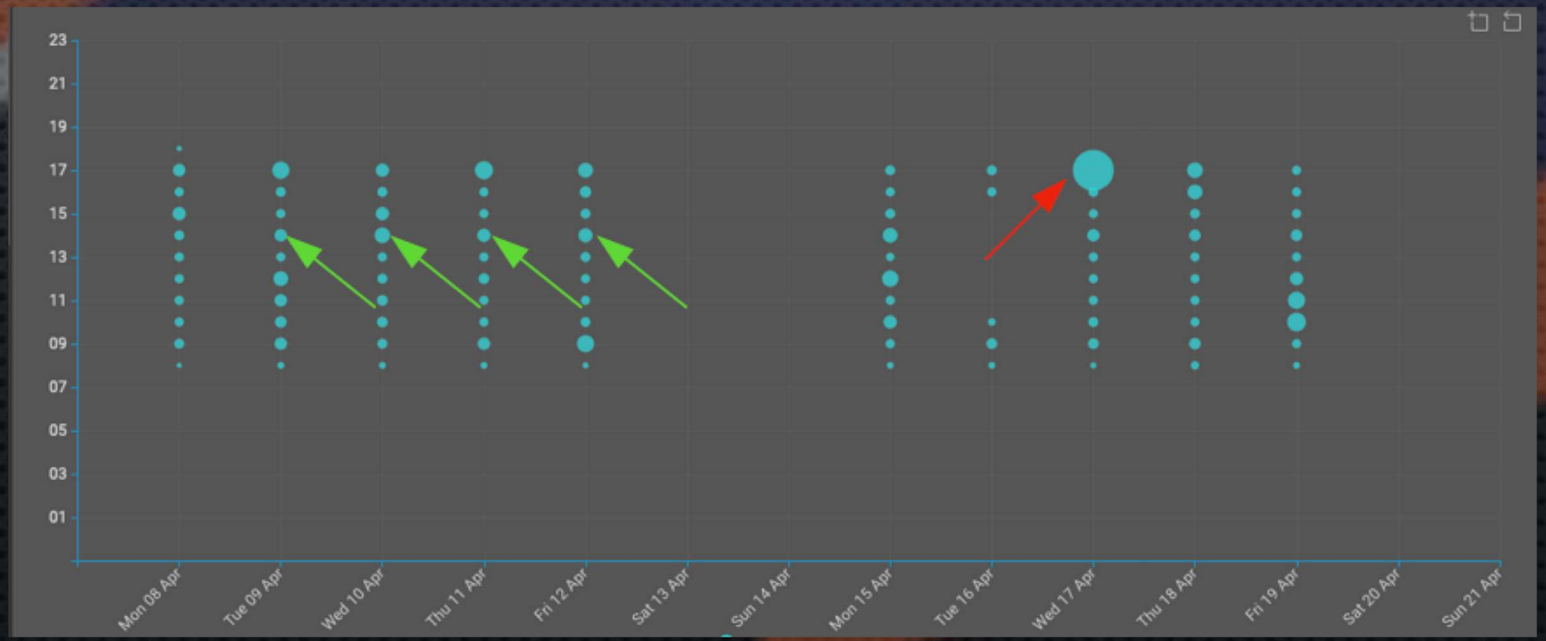
  Oppure

  In passato quell'utente non si è mai connesso a quella risorsa (eventualmente in quella fascia oraria).

In questo caso non siamo più legati alle (comunque indispensabili) regole di correlazione, ma cerchiamo di capire se quanto si sta verificandosia o meno normale

Analisi del comportamento

- In alcuni casi è facile intuire il comportamento di un utente in riferimento ad un dato evento.
- In questo grafico è rappresentata la frequenza di accesso al servizio di posta per uno specifico utente
- In alcune situazioni è possibile evidenziare una quantità anomala di eventi per utente/periodo di riferimento



Analisi del comportamento

Mediante l'associazione utente → evento → rischio, è inoltre possibile stilare una classifica degli utenti per grado di rischio

Attenzione alla numerosità (utente associato ad 1 evento ad alto rischio è più significativo di utente associato a molti eventi a basso rischio)

Conclusioni

Numerose differenti minacce da valutare con un approccio dinamico

I meccanismi di difesa non devono variare (devono evolvere)

L’analisi trasversale delle informazioni rivela comportamenti anomali

Gli scenari variano per ogni situazione e devono essere adattati

SGBOX

WWW.SGBOX.IT

sies

Partner Tecnico

Maggiori informazioni presso l'area espositiva