L’evoluzione del SOC di un’infrastruttura critica

Bologna, 6 Maggio 2017

Giovanni Mellini

Funzione Security

@merlos1977

giovannimellini

https://scubarda.wordpress.com

> ENAV Mission

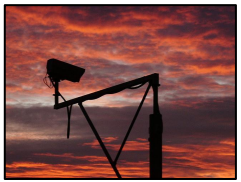
Garantire sempre la sicurezza e la puntualità ai milioni di passeggeri che volano nei cieli italiani. Contribuire alla crescita del trasporto aereo nazionale ed europeo con efficienza ed innovazione.

> Security Mission in ENAV

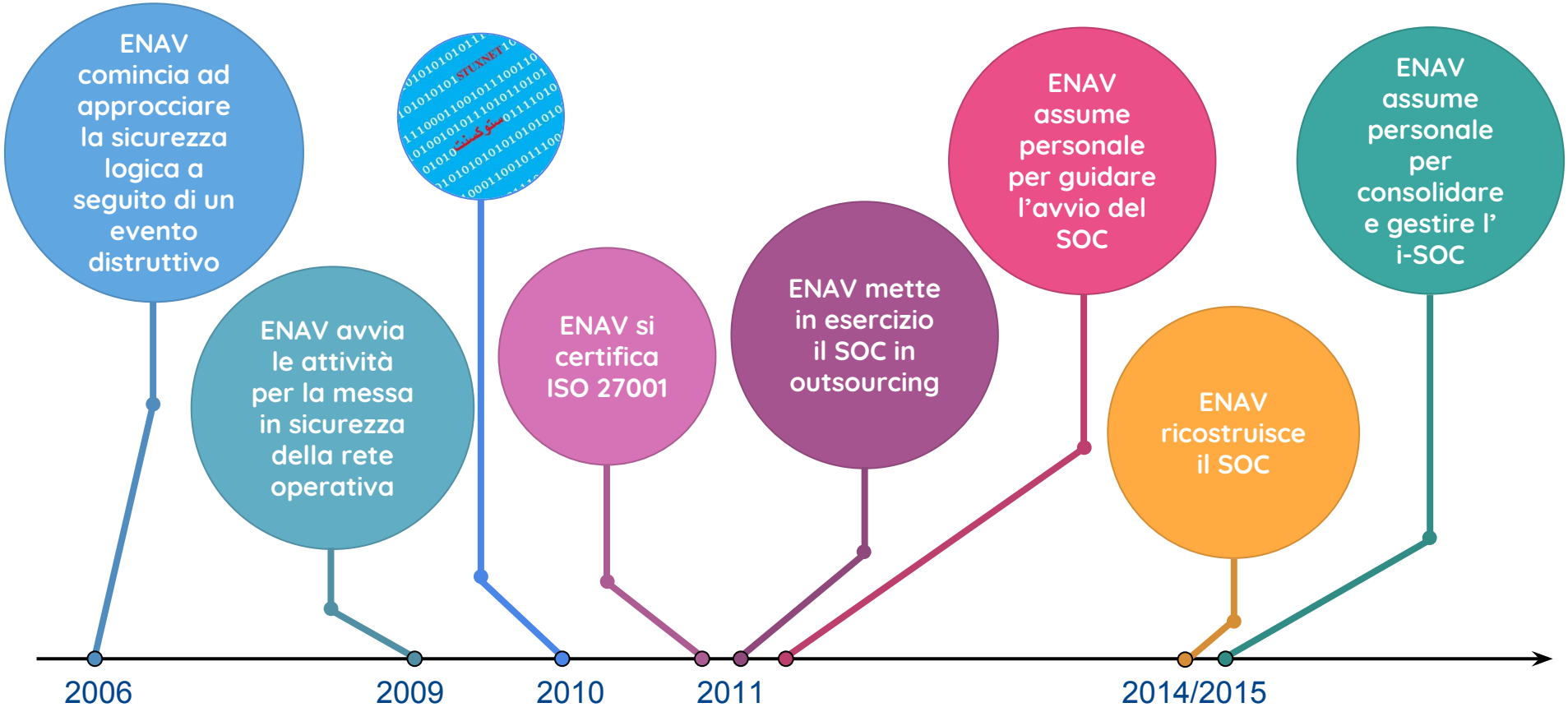
"Proteggere il personale, le infrastrutture, i sistemi tecnologici da atti di interferenza illecita e da azioni od eventi, anche non deliberati, che possano interferire sulla disponibilità, integrità e riservatezza delle informazioni"

Garantire la Sicurezza

- delle persone
- delle infrastrutture fisiche
- delle informazioni, dei sistemi e delle reti



> Timeline


ENAV comincia ad approcciare la sicurezza logica a seguito di un evento distruttivo
ENAV avvia le attività per la messa in sicurezza della rete operativa
STUXNET
ENAV si certifica ISO 27001
ENAV mette in esercizio il SOC in outsourcing
ENAV assume personale per guidare l'avvio del SOC
ENAV ricostruisce il SOC
ENAV assume personale per consolidare e gestire l' i-SOC
2006
2009
2010
2011
2014/2015

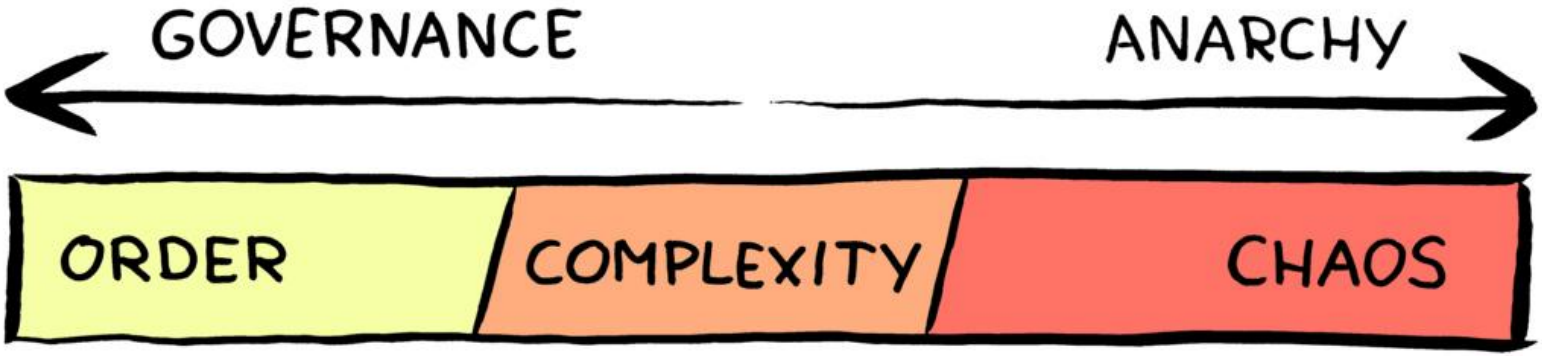
> Come eravamo

- SOC operato da fornitore esterno
- Molte attività non propriamente di Security
- Vincolo di lock-in con vendor di prodotti
- Costi di esercizio non in linea con gli obiettivi riduzione budget

Ripartire imparando dall'esperienza fatta

COSTRUZIONE DI UN MODELLO

> Governance



Assoluta convinzione della necessità di un processo di governance che si affianchi alle attività operative

Certificazione ISO 27001

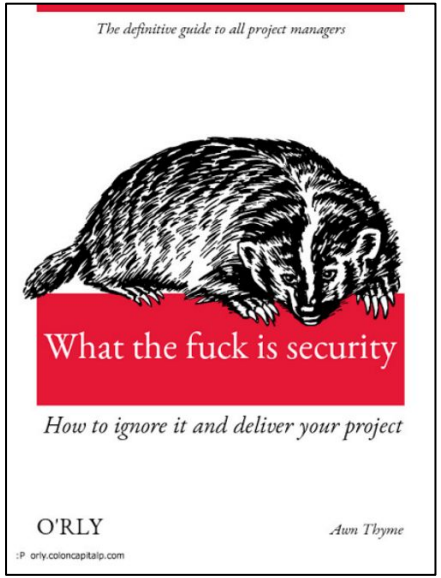
Security Management System

Ciclo di gestione del Rischio

> Rafforzamento

La costruzione di un modello efficace di Security deve passare per la componente di processo oltre che per quella tecnica

- governo centrale della Security
- ciclo di gestione del rischio, da cui deriva il commitment del top management
- identificazione dei rischi e declinazione delle azioni di trattamento ai risk owner



Presidio della Security su tutti i nuovi progetti con requisiti

> Cambiamento

Identificazione dei cardini su cui costruire il nuovo modello

Persone **Passione** **Conoscenza** **Open Source**

Necessità di un focus specifico ed esclusivo sulla Security abbandonando attività “collaterali”

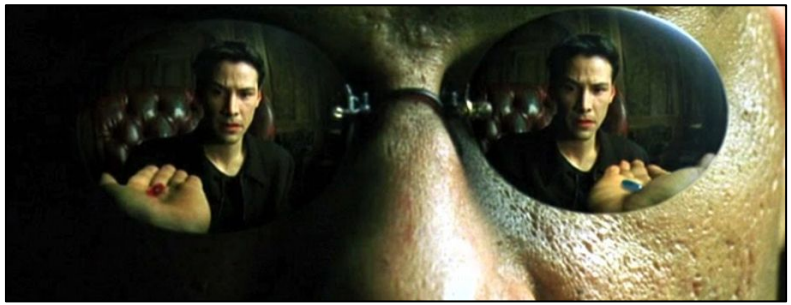
Applicazione del principio della **Segregation of Duties**

Il Security Operation Center è il presidio al SecMS, lo strumento tecnologico di supporto al processo per garantire

- ➔ la compliance alle procedure e le regole e alle normative internazionali
- ➔ il rispetto della mission della F.ne Security per parte di competenza

Consapevolezza che la
responsabilità non può essere delegata
e che la responsabilità è su
cosa si fa prima e non dopo

> Sfida



“You take the red pill - you stay in Wonderland, and I show you how deep the rabbit hole goes. Remember: all I’m offering is the truth. Nothing more. ***Follow me****”*

In una società a partecipazione pubblica con un approccio prudente alla trasformazione ed all’evoluzione dovuto alla natura critica del servizio erogato, affiancare una Security che è sinonimo di innovazione, evoluzione ed identificazione di nuovi trend di minaccia


I-SOC

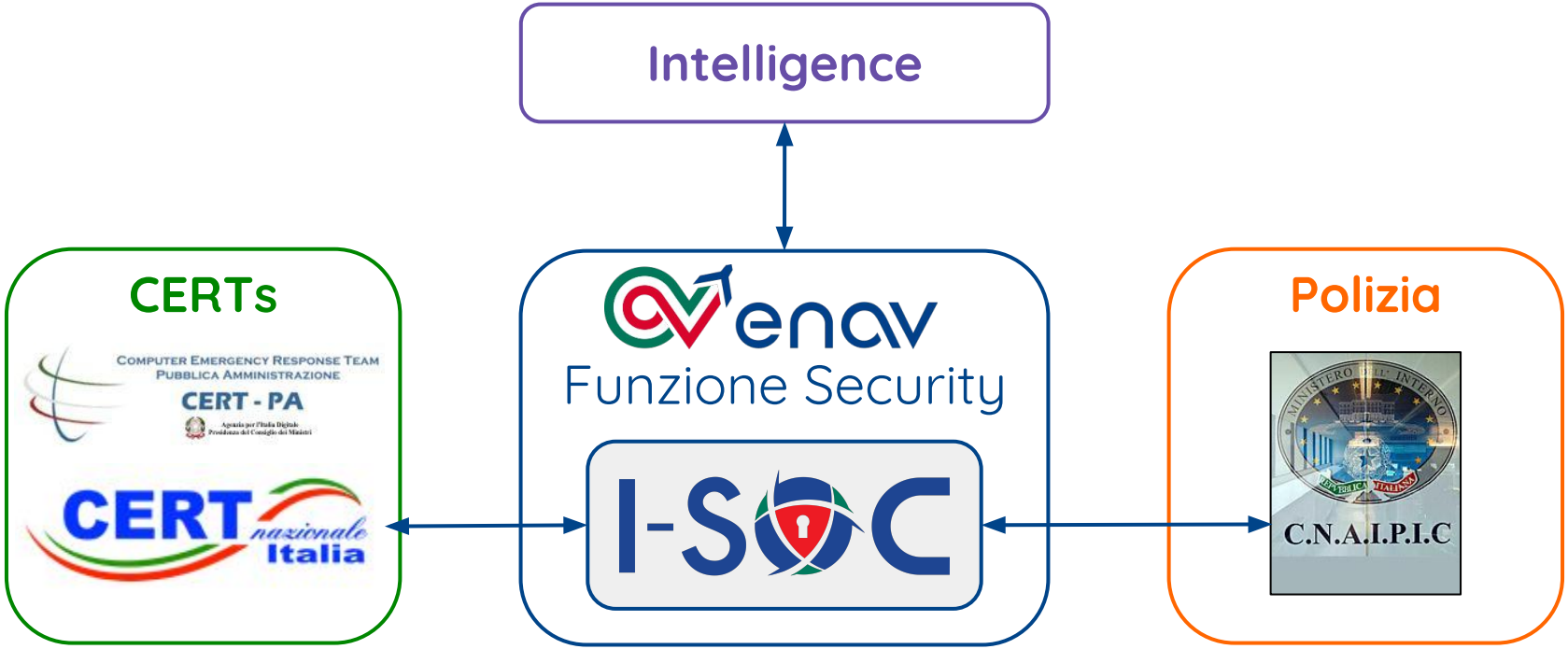
> Vincoli

- i-SOC costruito sul modello strutturale di ENAV che ha differenti “anime” al suo interno
- Necessità di collezionare eventi e log da molti sistemi differenti e di ricondurre tali dati ad un modello comune
- Su questo modello applicare allo stesso modo i controlli previsti dal SecMS
- Superamento del concetto tradizionale di SIEM legato al fornitore ed al prodotto
- Forte integrazione tra tutti i sistemi utilizzando meccanismi standard

> Necessità

Identificazione precisa e puntuale dei domini e punti di monitoraggio con l'obiettivo di comprendere ed utilizzare il dato esclusivamente ai fini della Security

La Funzione Security di ENAV e dunque l'i-SOC inseriti nel sistema di sicurezza cibernetica nazionale



> Criticità

- Coordinamento con altre funzioni/settori ENAV
- Import del dato in maniera non impattante
  - syslog, agent, connessioni su protocolli specifici
- Eliminazione del rumore di fondo
- Capire esattamente cosa si sta importando per associare il dato ai domini di Security corretti

Essenziale il commitment derivato dal processo e dalle regole

Selezione del software

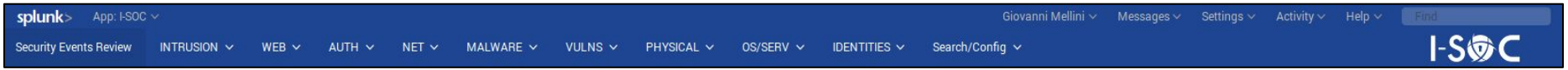
- scelta effettuata dopo aver testato la versione free di Splunk Enterprise
- valutazione di altre soluzioni commerciali per confronto

splunk>

- ➔ base open source, documentazione, community
- ➔ estrema velocità su piattaforme hw legacy
- ➔ interoperabilità facile con altri sistemi
- ➔ strumenti semplici per soddisfare esigenze di creazione di ricerche e dashboard custom

> Identificazione

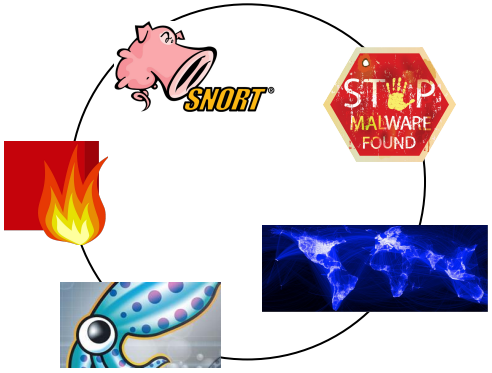
Programma di investimento che ha portato a realizzare un'applicazione custom "on top" del motore Splunk Enterprise



- Costruita sulle necessità ENAV
- Ricalca esattamente il modello aziendale
- Continua evoluzione
- Costi di esercizio ridotti

- Necessità di essere sempre aggiornati e "seguire" i trend di minaccia
- Necessario evolvere gli skill interni

> Identificazione



Ove possibile Security delegata a sistemi specializzati deployati nei punti chiave a seguito di investimenti mirati e spesso derivati da analisi del rischio

- sonde (proprietarie/OS)
- antivirus/antimalware
- proxy
- threat intelligence

Collezionamento del dato (raw o strutturato) per identificazione di pattern anomali e facilitare al massimo analisi e risposta da parte degli analisti i-SOC

Security Events Review | INTRUSION | WEB | AUTH | NET | MALWARE | VULNS | PHYSICAL | OS/SERV | IDENTITIES | Search/Config

I-SOC

Security Events Review

Edit | More Info

Timerange: Last 24 hours | Severity: All | Search: * | Rule: All | Submit

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	15	6	1	3

Security Events Overview

i	_time	Incident	Severity	ticket	Details
>	2017-04-04 04:55:06.000	SIG INTRUSION - HIGH ALERT - OS-OTHER Bash CGI environment variable injection attempt - from 69.50.209.208 - SIG-Sourcefire	HIGH	2017040477000033	View
>	2017-04-04 00:30:07.000	AUTH - VPN DURATION EXCEEDED[redacted]s - VPN[redacted]_GROUP	MEDIUM	2017040477000024	View
>	2017-04-04 00:30:06.000	SIG INTRUSION - HIGH ALERT - OS-OTHER Bash CGI environment variable injection attempt - from 69.50.209.208 - SIG-Sourcefire	HIGH	2017040477000015	View
>	2017-04-03 17:15:40.771	WEB - TOR Exit Node connection detected - from [redacted]4 to 83.228.93.76	HIGH	2017040377000581	View
>	2017-04-03 15:40:06.000	SIG INTRUSION - HIGH ALERT - MALWARE-OTHER TDS Sutra - page redirecting to a SutraTDS - from 88.214.242.107 - SIG-Sourcefire	HIGH	2017040377000553	View

Ticket-2017040477000033 — SIG INTRUSION - HIGH ALERT - OS-OTHER Bash CGI environment variable injection attempt - from 69.50.209.208 - SIG-Sourcefire

Back | Lock | History | Print | Priority | Free Fields | Link | Owner | Responsible | Customer | Note | Phone Call Outbound | Phone Call Inbound | E-Mail Outbound | Merge | Pending | Watch | Spam | Process Enroll | Queue

Article Overview - 2 Article(s)

NO.	TYPE	FROM	SUBJECT	CREATED
2	customer – email-internal	[redacted]@enav.it	[SPLUNK] SIG INTRUSION - HIGH ALE...	04/04/2017 04:55
1	agent – webrequest	[redacted]v.it	Automatic ticket opening from SPLUNK	04/04/2017 04:55

Article #2 – [SPLUNK] SIG INTRUSION - HIGH ALERT - OS-OTHER Bash CGI environment variable injection attempt - from 69.50.209.208 - SIG-Sourcefire — Created: 04/04/2017 04:55

Plain Format | Print | Split | Bounce | Forward | - Reply All - | - Reply -

From: soc-monitoring@enav.it

To: soc@enav.it, soc-otrs@enav.it

Subject: [SPLUNK] SIG INTRUSION - HIGH ALERT - OS-OTHER Bash CGI environment variable injection attempt - from 69.50.209.208 - SIG-Sourcefire

Ticket-2017040477000033 SIG INTRUSION - HIGH ALERT - OS-OTHER Bash CGI environment variable injection attempt - from 69.50.209.208 - SIG-Sourcefire is opened on Security ENAV Service Desk

Ticket Information

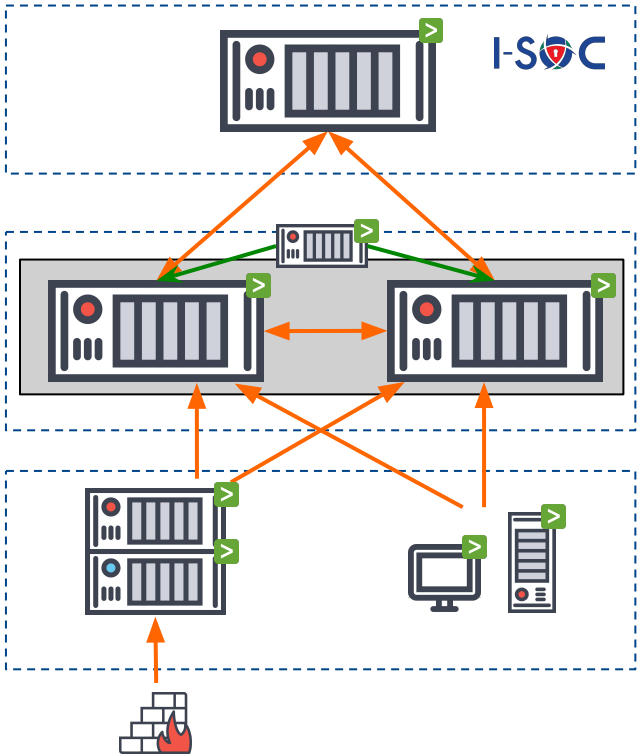
Type: Security Event Monitoring
Age: 46 m
Created: 04/04/2017 04:55
Created by: OTRS Service Account SPLUNK
State: new
Locked: unlock

RAW Search

Posture Value: 69.50.209.208 | Since date time | Tags: Intrusion Detection, Web/Proxy

i	Time	Event
>	4/4/17 4:51:55.000 AM	rec_type=400 rec_type_simple="IPS EVENT" event_sec=1491274315 event_usec=454967 rivilege Gain" class=attempted-admin priority=high src_ip=69.50.209.208 dest_ip b_app=0 client_app="Web browser" app_proto=HTTP fw_rule="ENAV File Policy" fw_p egress=00000000-0000-0000-0000-000000000000 connection_sec=1491274315 instance_ host = soc-splunksh-02 source = eStreamer sourcetype = eStreamer

Ambiente distribuito in alta affidabilità



SEARCH HEAD

- Altre apps ed add-ons
- Ricerche utente e schedulate
- Arricchimento in search time

INDEXER CLUSTER

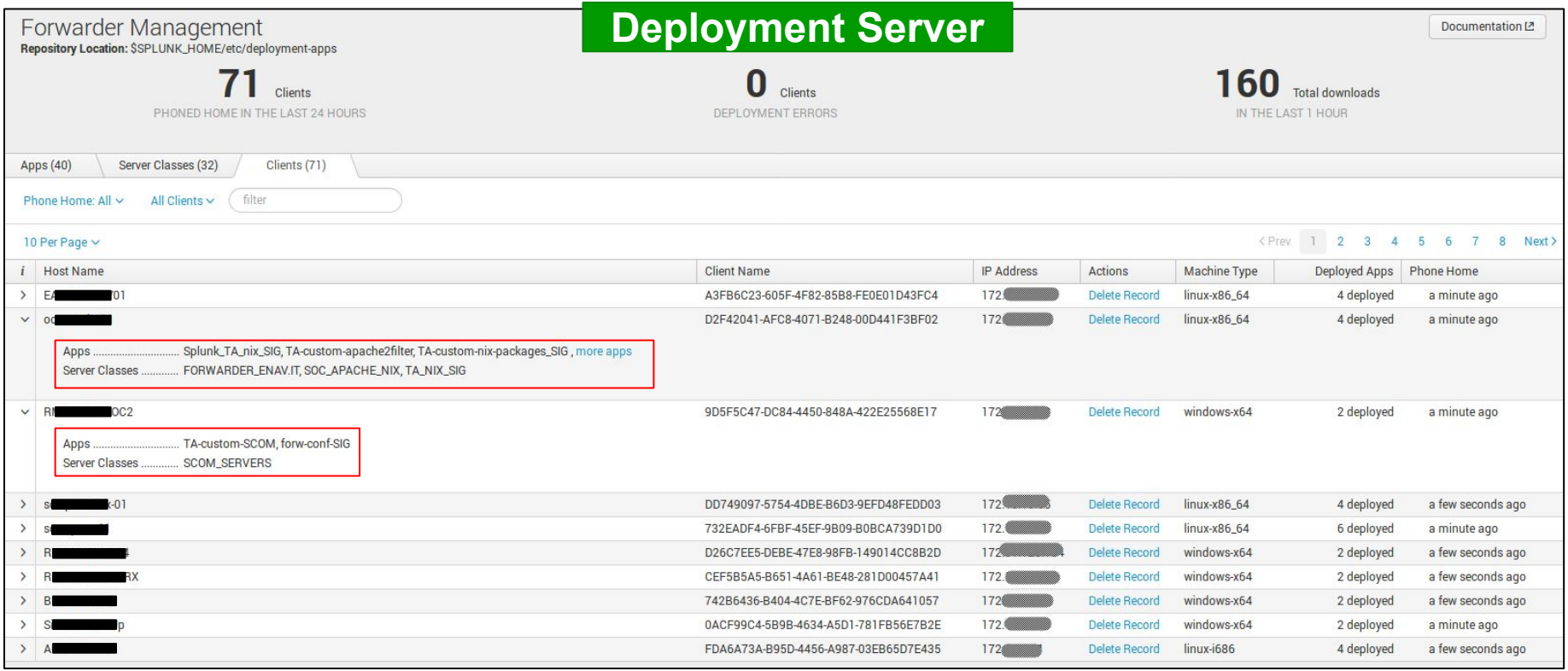
- Replicazione dati indicizzati
- Master Cluster per orchestrazione
- Esecuzione delle ricerche

FORWARD

- Due Forwarder in HA per sistemi no agent
- Agent su server/client

Distribuzione centralizzata

Deployment Server



Forwarder Management

Repository Location: $SPLUNK_HOME/etc/deployment-apps

Documentation

71 Clients — PHONED HOME IN THE LAST 24 HOURS

0 Clients — DEPLOYMENT ERRORS

160 Total downloads — IN THE LAST 1 HOUR

Apps (40) | Server Classes (32) | Clients (71)

Phone Home: All | All Clients | filter

10 Per Page | < Prev 1 2 3 4 5 6 7 8 Next >

Host Name	Client Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
E[redacted]01	A3FB6C23-605F-4F82-85B8-FE0E01D43FC4	172.[redacted]	Delete Record	linux-x86_64	4 deployed	a minute ago
od[redacted]	D2F42041-AFC8-4071-B248-00D441F3BF02	172.[redacted]	Delete Record	linux-x86_64	4 deployed	a minute ago
Apps ..... Splunk_TA_nix_SIG, TA-custom-apache2filter, TA-custom-nix-packages_SIG , more apps Server Classes ..... FORWARDER_ENAV.IT, SOC_APACHE_NIX, TA_NIX_SIG						
R[redacted]OC2	9D5F5C47-DC84-4450-848A-422E25568E17	172.[redacted]	Delete Record	windows-x64	2 deployed	a minute ago
Apps ..... TA-custom-SCOM, forw-conf-SIG Server Classes ..... SCOM_SERVERS						
s[redacted]-01	DD749097-5754-4DBE-B6D3-9EFD48FEDD03	172.[redacted]	Delete Record	linux-x86_64	4 deployed	a few seconds ago
s[redacted]	732EADF4-6FBF-45EF-9B09-B0BCA739D1D0	172.[redacted]	Delete Record	linux-x86_64	6 deployed	a minute ago
R[redacted]	D26C7EE5-DEBE-47E8-98FB-149014CC8B2D	172.[redacted]	Delete Record	windows-x64	2 deployed	a few seconds ago
R[redacted]RX	CEF5B5A5-B651-4A61-BE48-281D00457A41	172.[redacted]	Delete Record	windows-x64	2 deployed	a few seconds ago
B[redacted]	742B6436-B404-4C7E-BF62-976CDA641057	172.[redacted]	Delete Record	windows-x64	2 deployed	a few seconds ago
S[redacted]p	0ACF99C4-5B9B-4634-A5D1-781FB56E7B2E	172.[redacted]	Delete Record	windows-x64	2 deployed	a minute ago
A[redacted]	FDA6A73A-B95D-4456-A987-03EB65D7E435	172.[redacted]	Delete Record	linux-i686	4 deployed	a few seconds ago

Indexer Clustering: Master Node

Master Cluster

Edit | More Info | Documentation

✓ **All Data is Searchable** — **2** searchable **0** not searchable (Peers)

✓ **Search Factor is Met**

✓ **Replication Factor is Met** — **40** searchable **0** not searchable (Indexes)

Peers (2) | Indexes (40) | Search Heads (3)

filter | 10 per page

i	Peer Name	Fully Searchable	Status	Buckets
>	soc[redacted]-01	✓ Yes	Up	3735
>	soc[redacted]-02	✓ Yes	Up	3712

Peers (2) | Indexes (40) | Search Heads (3)

filter | 10 per page | Bucket Status | < Prev

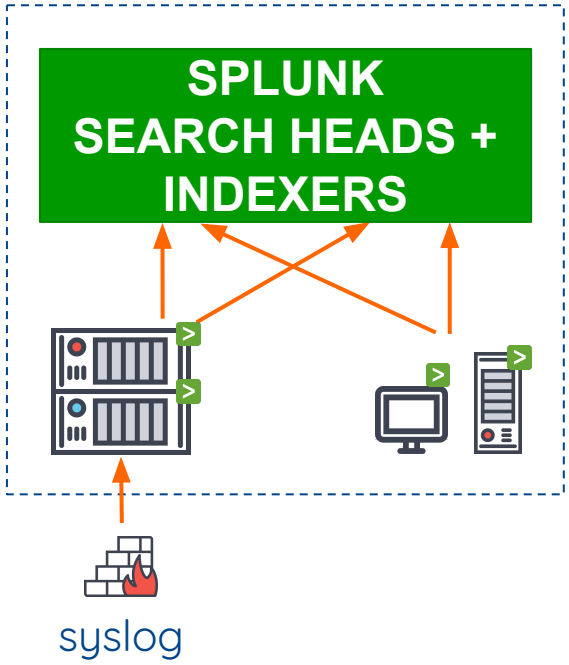
Index Name	Fully Searchable	Searchable Data Copies	Replicated Data Copies	Buckets	Cumulative Raw Data Size
cisco_net_sig	✓ Yes	2	2	780	80.48 GB
squid_sig	✓ Yes	2	2	396	52.71 GB
fortinet	✓ Yes	2	2	484	43.00 GB
wineventlog_sig_operativo	✓ Yes	2	2	312	27.13 GB
netscaler	✓ Yes	2	2	129	15.95 GB
forefront_fw	✓ Yes	2	2	105	12.12 GB
_internal	✓ Yes	2	2	69	10.01 GB
cisco_net_sio	✓ Yes	2	2	94	6.48 GB
apache2	✓ Yes	2	2	65	3.93 GB
iis_sig	✓ Yes	2	2	55	3.74 GB

Indici

(1,n)

Bucket

Layer di Forwarding



Colleziona dati inviati da sistemi agentless (via forwarding intermedio) o dagli agent installati sui client/server remoti

Le applicazioni pushate dal Deployment Server dopo l'installazione del client e la ricezione della *phone home*

Forwarders installati in reti differenti e separate
Visibilità dell'infrastruttura i-SOC (centralità)

Step 1

Installazione sul client/server remoto del pacchetto SPLUNK custom con indirizzo del Deployment Server

```
[08:08:32] root@s[redacted]-01:/opt/splunk/splunkforwarder/etc/system/local # cat deploymentclient.conf
[deployment-client]

[target-broker:deploymentServer]
targetUri= soc-s[redacted].dev:8089
```

i	Host Name	Client Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>	s[redacted]	49F4EC41-F699-4A79-B641-040229222548	172[redacted]	Delete Record	linux-x86_64	5 deployed	a few seconds ago

Step 2

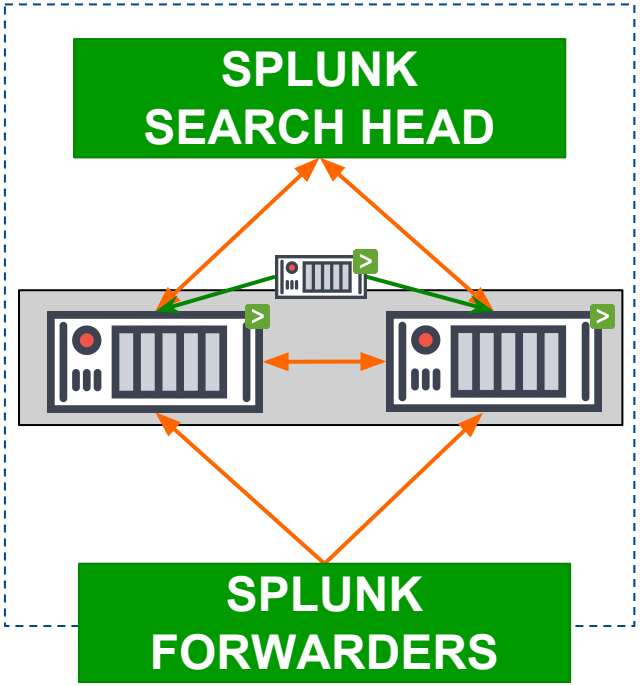
Push dal Deployment Server di un'app specifica che "dice" al forwarder SPLUNK gli IP degli Indexer e di altre applicazioni specifiche per il contesto (es. apache, autenticazione)

```
[08:14:44] root@so[redacted]1:/opt/splunk/splunkforwarder/etc/apps # cat forw-conf/default/outputs.conf
[tcpout]
defaultGroup = default-autolb-group

#indexers
[tcpout:default-autolb-group]
server=soc-[redacted]v:9997,soc-[redacted]v:9997
autoLB = true
```

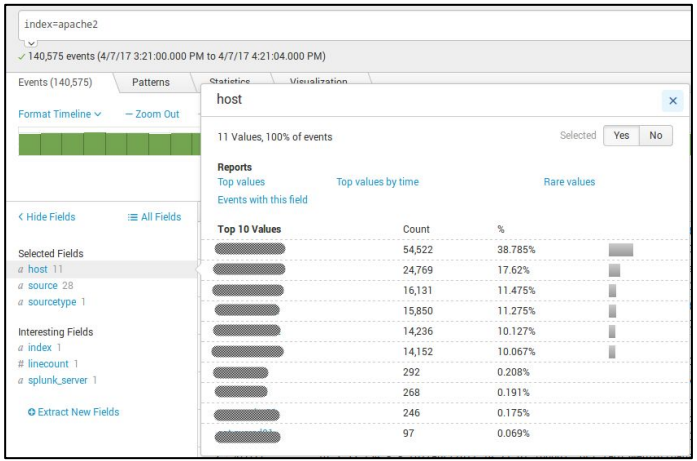
Name	Actions	After Installation	Clients
forw-conf	Edit	Enable App, Restart Splunkd	32 deployed
forw-conf-enet	Edit	Enable App, Restart Splunkd	2 deployed
forw-conf-SIG	Edit	Enable App, Restart Splunkd	37 deployed
Hforw-conf	Edit	Enable App, Restart Splunkd	2 deployed

Layer di Indicizzazione



Dato inviato dal forwarder con attributi impostati: index, sourcetype

```
[16:17:06].{ root@s                    02:/opt/splunk/splunk-sw/etc/deployment-apps/TA-custom-apache2filter/default }. # cat inputs.conf
[monitor:///var/log/apache2/*access.log]
sourcetype = apache2
index= apache2
disabled = 0
```



Gli Indexer arricchiscono con info del forwarder (es. host, source)

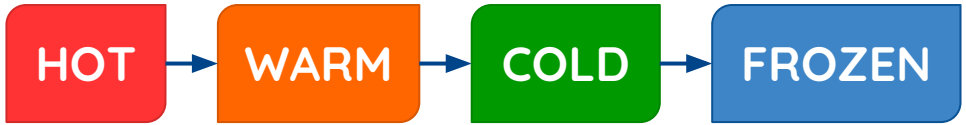
```
[16:15:27].{ root@s[redacted]01:/opt/splunk/splunk-data }. # tree apache2/
apache2/
├── colddb
├── db
│   ├── 207_E56363C4-6AFD-4A24-A759-4FFA43FE9EBB
│   │   ├── 1490722667-1490571601-5462286770270586110.tsidx
│   │   ├── 1490794802-1490722666-5467009788049106968.tsidx
│   │   ├── 1490847154-1490794800-5470441752835266220.tsidx
│   │   ├── 1490878380-1490847153-5472486749534577437.tsidx
│   │   ├── 1490894481-1490878378-5473542637373765445.tsidx
│   │   ├── 1490898312-1490894479-5473793265233943092.tsidx
│   │   ├── 1490898824-1490898310-5473826909267252955.tsidx
│   │   ├── 1490898852-1490898823-5473826910846761459.tsidx
│   │   ├── 1490898886-1490898851-5473834846446731004.tsidx
│   │   ├── Hosts.data
│   │   ├── rawdata
│   │   │   ├── journal.gz
│   │   │   └── slicesv2.dat
│   │   ├── Sources.data
│   │   ├── SourceTypes.data
│   │   ├── splunk-autogen-params.dat
│   │   ├── splunk-need-optimize.dat
│   │   └── Strings.data
│   ├── 208_E56363C4-6AFD-4A24-A759-4FFA43FE9EBB
│   │   ├── 1491159936-1490898887-5490941777714498207.tsidx
│   │   ├── 1491196813-1491159933-5493356836606871225.tsidx
│   │   ├── 1491217650-1491196812-5494721450207678331.tsidx
│   │   ├── 1491221662-1491217649-5494986025679054085.tsidx
│   │   ├── 1491223514-1491221660-5495106001500990390.tsidx
│   │   ├── 1491224562-1491223514-5495177597552622197.tsidx
│   │   ├── 1491224638-1491224561-5495177596117679380.tsidx
│   │   ├── 1491224668-1491224637-5495179533460283323.tsidx
│   │   ├── 1491224758-1491224663-5495185401863166055.tsidx
│   │   ├── 1491224782-1491224756-5495193290324913645.tsidx
│   │   ├── Hosts.data
│   │   ├── rawdata
│   │   │   ├── journal.gz
│   │   │   └── slicesv2.dat
│   │   ├── Sources.data
│   │   ├── SourceTypes.data
│   │   ├── splunk-autogen-params.dat
│   │   ├── splunk-need-optimize.dat
│   │   └── Strings.data
```

BUCKETS

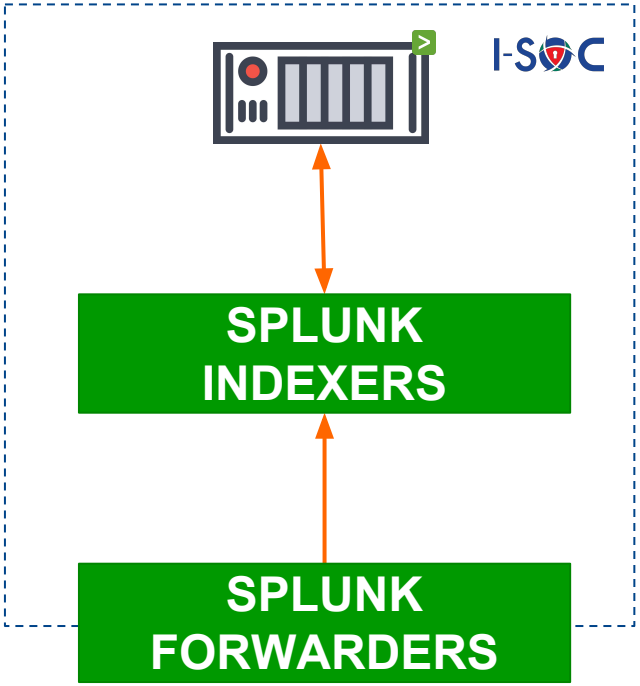
Indice: apache2

Dato memorizzato in bucket

- rawdata
- indici di metadati (tsidx) con puntatori tra chiavi indicizzate ed i rawdata
- info accessorie (sources, sourcetypes,hosts)



Layer di Ricerca



Il Search Head “utilizza” il cluster di Indexer per effettuare ricerche sul dato indicizzato

Flusso bidirezionale che il SH arricchisce con informazioni aggiuntive (search time) da utilizzare nelle ricerche (es. file csv)

Selected Fields
a app 1
a bytes 100+
date_hour 4
date_mday 1
date_minute 16
a date_month 1
date_second 60
a date_wday 1
date_year 1
date_zone 2
a dest 7
a eventtype 2
a host 11
a http_method 4
a http_user_agent 7
a index 1
linecount 1
a punct 62
a source 16
a sourcetype 1
a splunk_server 2
a src 100+
status 100+
a tag 1
a tag::eventtype 1
timeendpos 20
timestartpos 20
a uri_path 100+
uri_port 1
a url 100+
a user 18
a vendor 1

Data Model

astrazione e normalizzazione del dato

accelerazione

Creata su SH una struttura dati con indicizzazione specifica di un sottoinsieme di campi del dato indicizzato

Utile nel caso di dataset molto ampi (es. autenticazione, network)

Network Traffic
Network Traffic Data Model

MODEL

Objects ..... 1 Event Edit
Permissions ..... Shared Globally. Owned by nobody. Edit

ACCELERATION

Rebuild Update Edit
Status ..... 100.00% Completed
Access Count ..... 71112. Last Access: 4/7/17 6:00:15.000 PM
Size on Disk 14984.92MB
Summary Range ..... 604800 second(s)
Buckets 129
Updated ..... 4/7/17 6:12:06.000 PM


7.5M

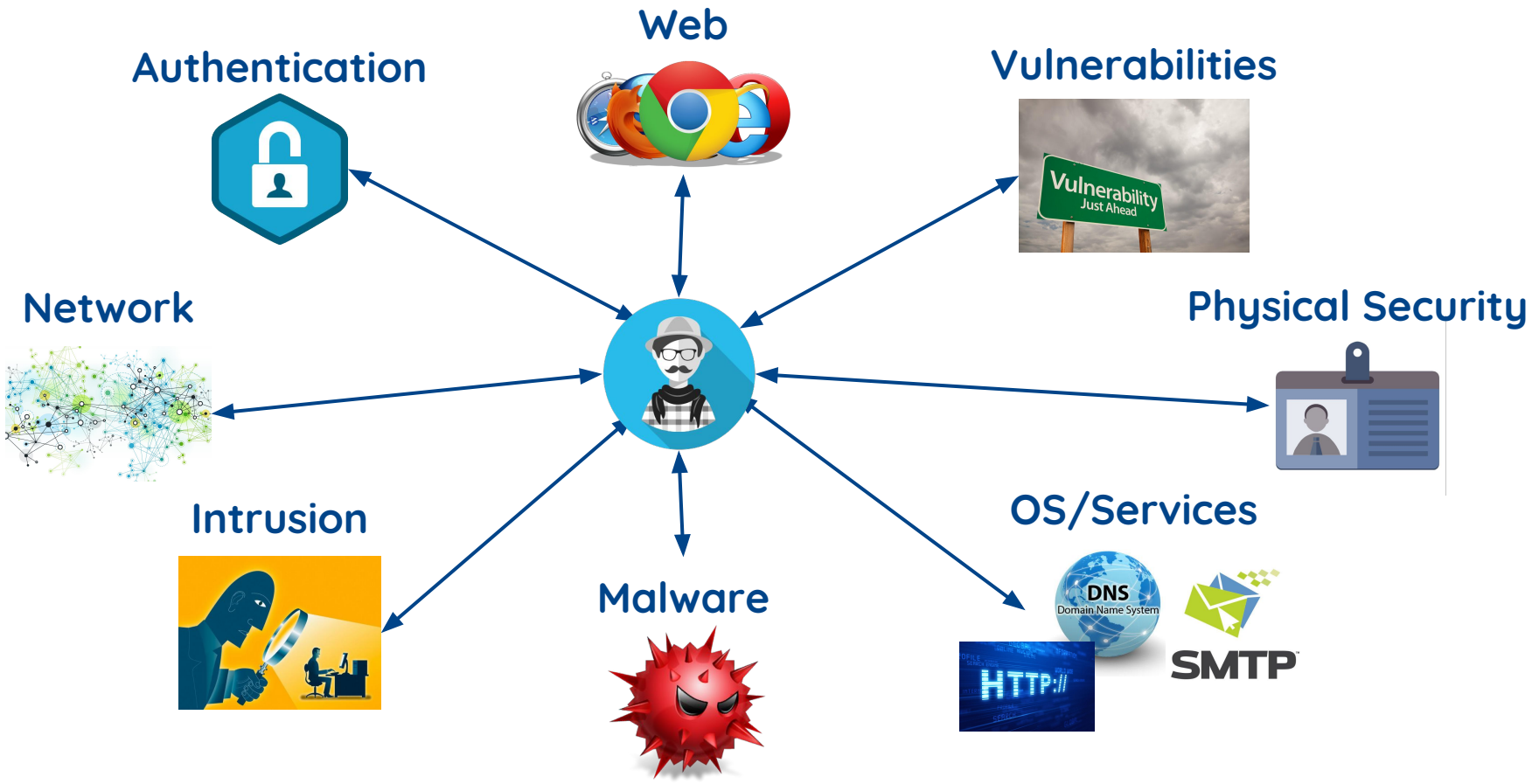
Circa 50GB di dati “puliti” indicizzati ogni giorno

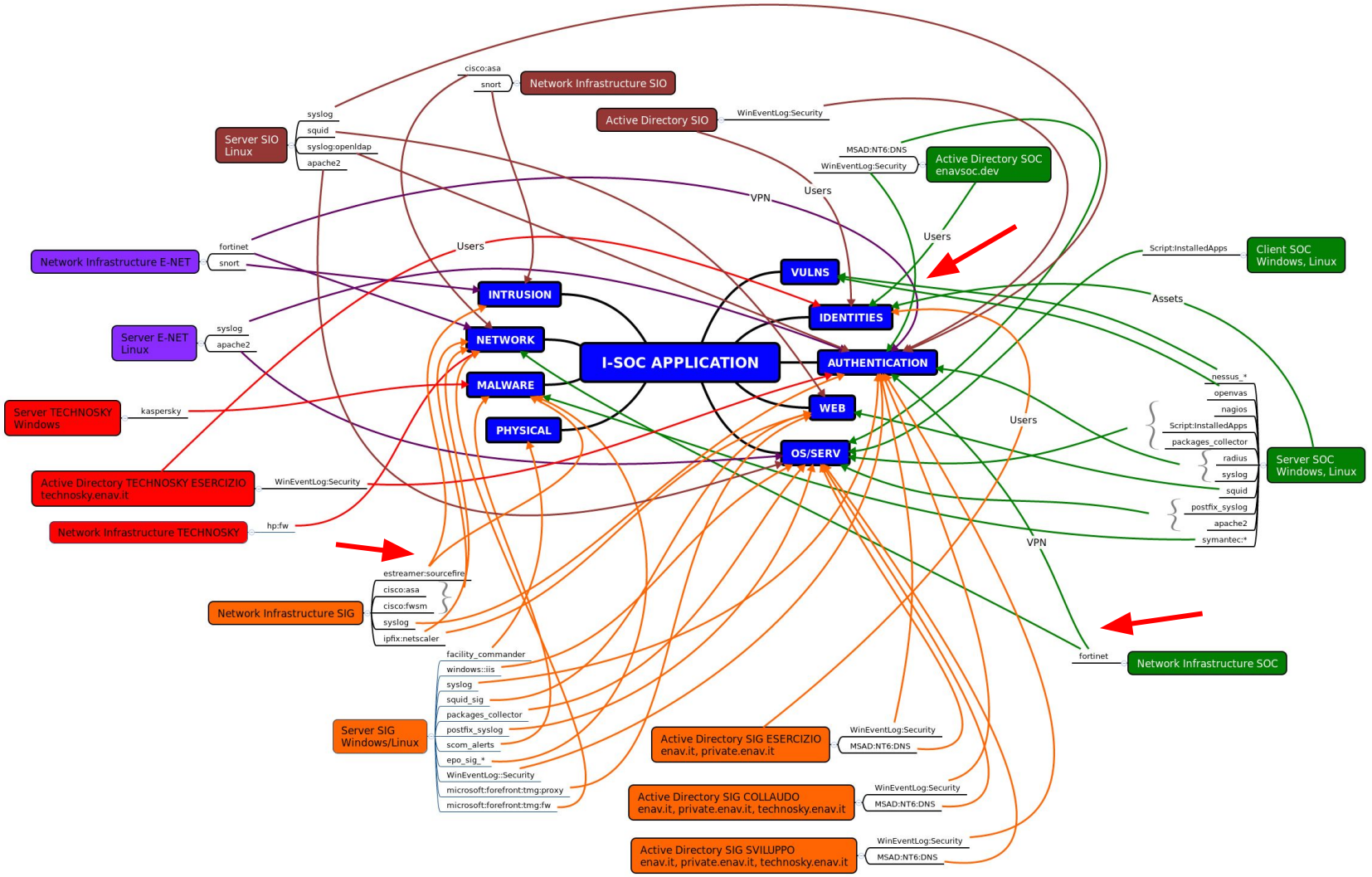
Necessità di “indirizzare” il dato in indici dedicati in base a

- dominio logico di provenienza (es. rete gestionale, rete operativa etc)
- tipo di dato (es. autenticazione, network, web etc)

Granularità / Performance

Stesso criterio dovrà poi essere costruito nell’applicazione i-SOC per tutte le ricerche sui dati indicizzati


Web
Authentication
Vulnerabilities
Vulnerability
Just Ahead
Network
Physical Security
Intrusion
OS/Services
DNS
Domain Name System
HTTP://
SMTP
Malware


I-SOC APPLICATION
INTRUSION
NETWORK
MALWARE
PHYSICAL
VULNS
IDENTITIES
AUTHENTICATION
WEB
OS/SERV
Network Infrastructure SIO
cisco:asa
snort
Active Directory SIO
WinEventLog:Security
Server SIO Linux
syslog
squid
syslog:openldap
apache2
Active Directory SOC enavsoc.dev
MSAD:NT6:DNS
WinEventLog:Security
Network Infrastructure E-NET
fortinet
snort
Server E-NET Linux
syslog
apache2
Server TECHNOSKY Windows
kaspersky
Active Directory TECHNOSKY ESERCIZIO technosky.enav.it
WinEventLog:Security
Network Infrastructure TECHNOSKY
hp:fw
Client SOC Windows, Linux
Script:InstalledApps
Server SOC Windows, Linux
nessus_*
openvas
nagios
Script:InstalledApps
packages_collector
radius
syslog
squid
postfix_syslog
apache2
symantec:*
Network Infrastructure SIG
estreamer:sourcefire
cisco:asa
cisco:fwsm
syslog
ipfix:netscaler
Server SIG Windows/Linux
facility_commander
windows::iis
syslog
squid_sig
packages_collector
postfix_syslog
scom_alerts
epo_sig_*
WinEventLog::Security
microsoft:forefront:tmg:proxy
microsoft:forefront:tmg:fw
Active Directory SIG ESERCIZIO enav.it, private.enav.it
WinEventLog:Security
MSAD:NT6:DNS
Active Directory SIG COLLAUDO enav.it, private.enav.it, technosky.enav.it
WinEventLog:Security
MSAD:NT6:DNS
Active Directory SIG SVILUPPO enav.it, private.enav.it, technosky.enav.it
WinEventLog:Security
MSAD:NT6:DNS
Network Infrastructure SOC
fortinet
VPN
Users
Assets

Creazione di Indici differenziati

```
### INDICI AD SIG OPERATIVO ##
[windows_sig_operativo]
repFactor=auto
homePath   = /opt/splunk/splunk-data/windows_sig_operativo/db
coldPath   = /opt/splunk-dm_summary/splunk-data/windows_sig_operativo/colddb
thawedPath = /opt/splunk-dm_summary/splunk-data/windows_sig_operativo/thaweddb
frozenTimePeriodInSecs = 7776000

[wineventlog_sig_operativo]
repFactor=auto
homePath   = /opt/splunk/splunk-data/wineventlog_sig_operativo/db
coldPath   = /opt/splunk-dm_summary/splunk-data/wineventlog_sig_operativo/colddb
thawedPath = /opt/splunk-dm_summary/splunk-data/wineventlog_sig_operativo/thaweddb
frozenTimePeriodInSecs = 7776000

[perfmon_sig_operativo]
repFactor=auto
homePath   = /opt/splunk/splunk-data/perfmon_sig_operativo/db
coldPath   = /opt/splunk-dm_summary/splunk-data/perfmon_sig_operativo/colddb
thawedPath = /opt/splunk-dm_summary/splunk-data/perfmon_sig_operativo/thaweddb
frozenTimePeriodInSecs = 7776000
```

```
### INDICI AD SIG SVILUPPO ##
[windows_sig_sviluppo]
repFactor=auto
homePath   = /opt/splunk/splunk-data/windows_sig_sviluppo/db
coldPath   = /opt/splunk-dm_summary/splunk-data/windows_sig_sviluppo/colddb
thawedPath = /opt/splunk-dm_summary/splunk-data/windows_sig_sviluppo/thaweddb
frozenTimePeriodInSecs = 7776000

[wineventlog_sig_sviluppo]
repFactor=auto
homePath   = /opt/splunk/splunk-data/wineventlog_sig_sviluppo/db
coldPath   = /opt/splunk-dm_summary/splunk-data/wineventlog_sig_sviluppo/colddb
thawedPath = /opt/splunk-dm_summary/splunk-data/wineventlog_sig_sviluppo/thaweddb
frozenTimePeriodInSecs = 7776000

[perfmon_sig_sviluppo]
repFactor=auto
homePath   = /opt/splunk/splunk-data/perfmon_sig_sviluppo/db
coldPath   = /opt/splunk-dm_summary/splunk-data/perfmon_sig_sviluppo/colddb
thawedPath = /opt/splunk-dm_summary/splunk-data/perfmon_sig_sviluppo/thaweddb
frozenTimePeriodInSecs = 7776000
```

Deploy di applicazioni che collezionano lo stesso tipo di dato che differiscono per gli indici

```
[15:04:09].{ root@s[redacted]2:/opt/splunk/splunk-sw/etc/deployment-apps }. # diff -ur Splunk_TA_windows_SIG_OPERATIVO Splunk_TA_windows_SIG_SVILUPPO
diff -ur Splunk_TA_windows_SIG_OPERATIVO/default/eventgen.conf Splunk_TA_windows_SIG_SVILUPPO/default/eventgen.conf
--- Splunk_TA_windows_SIG_OPERATIVO/default/eventgen.conf       2016-02-24 13:11:15.000000000 +0100
+++ Splunk_TA_windows_SIG_SVILUPPO/default/eventgen.conf        2016-01-21 09:52:11.000000000 +0100
@@ -2,7 +2,7 @@

 #### Default replacement for all DhcpSrvLog logs
 [sample.DhcpSrvLog]
-index = windows_sig_operativo
+index = windows_sig_sviluppo
 source=c:\windows\system32\dhcp\dhcpsrvlog.log
 sourcetype = DhcpSrvLog
 interval = 300
@@ -18,7 +18,7 @@

 #### Default replacements for all WindowsUpdateLog logs
 [.*\.WindowsUpdateLog]
-index = windows_sig_operativo
+index = windows_sig_sviluppo
 source = WindowsUpdateLog
 sourcetype = WindowsUpdateLog
 interval = 7200
@@ -34,7 +34,7 @@
 token.0.replacement = %Y-%m-%d %H:%M:%S
```

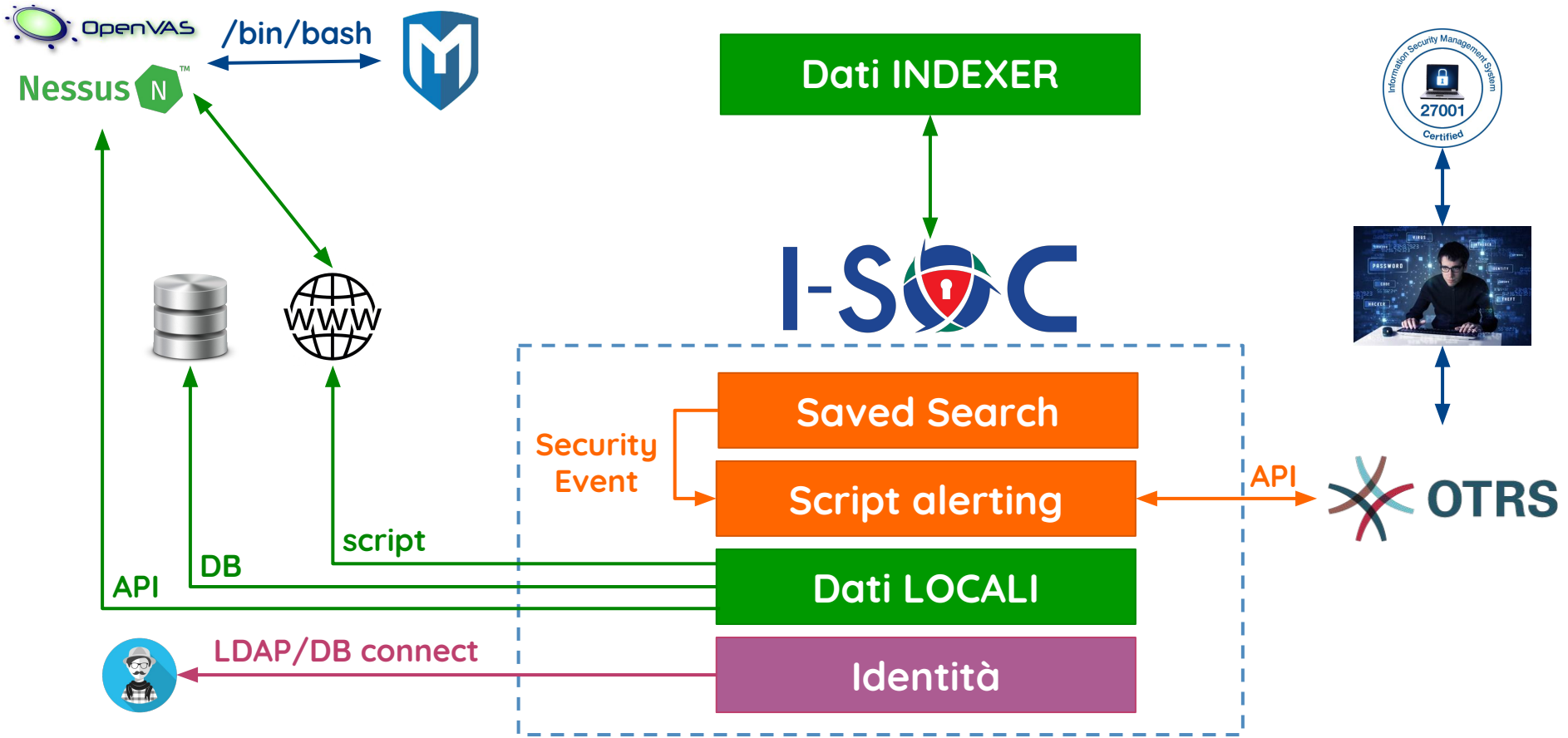
Sarà in carico all'applicazione i-SOC l'ottimizzazione, puntando l'indice corretto

Pulizia del dato eliminando il rumore di fondo con configurazioni specifiche

```
[04:12:34].{ root@s[redacted]1:/opt/splunk/splunk_hf/etc/apps/TA-custom-FortinetFilter/default }. # cat transforms.conf | grep set_null_status -A 3
[set_null_status]
REGEX = status=start|action="perf-stats"
DEST_KEY = queue
FORMAT = nullQueue
```


Integration

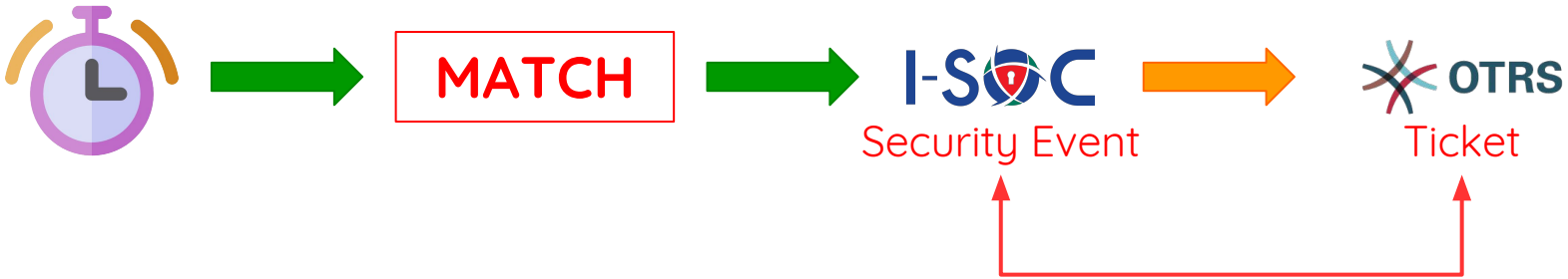
> make integration



> make integration

Nell'applicazione i-SOC sono definite le Saved Search che analizzano ad intervalli definiti il dato alla ricerca di Security Events

Nel caso in cui ci siano dei match si genera un Security Event ed eventualmente ticket OTRS in base a delle regole definite nell'applicazione



Saved Search: **SOC TOR exit nodes**

Search

```
| tstats prestats=true  summariesonly=true  max(_time) as _time,values(All_Traffic.action) as action,count from
datamodel=Network_Traffic by
All_Traffic.dvc,All_Traffic.src,All_Traffic.src_port,All_Traffic.src_interface,All_Traffic.dest,All_Traffic.transport,All
  Traffic.dest_port,All_Traffic.dest_interface | `drop_dm_object_name("All_Traffic")` | search [|inputlookup
soc_tor_list.csv | fields dest] dest_port!=53 | sort - count | table src, dest,count
```

Time range

Start time: -15m@m

Finish time: now

Time specifiers: y, mon, d, h, m, s

Learn more

Schedule and alert

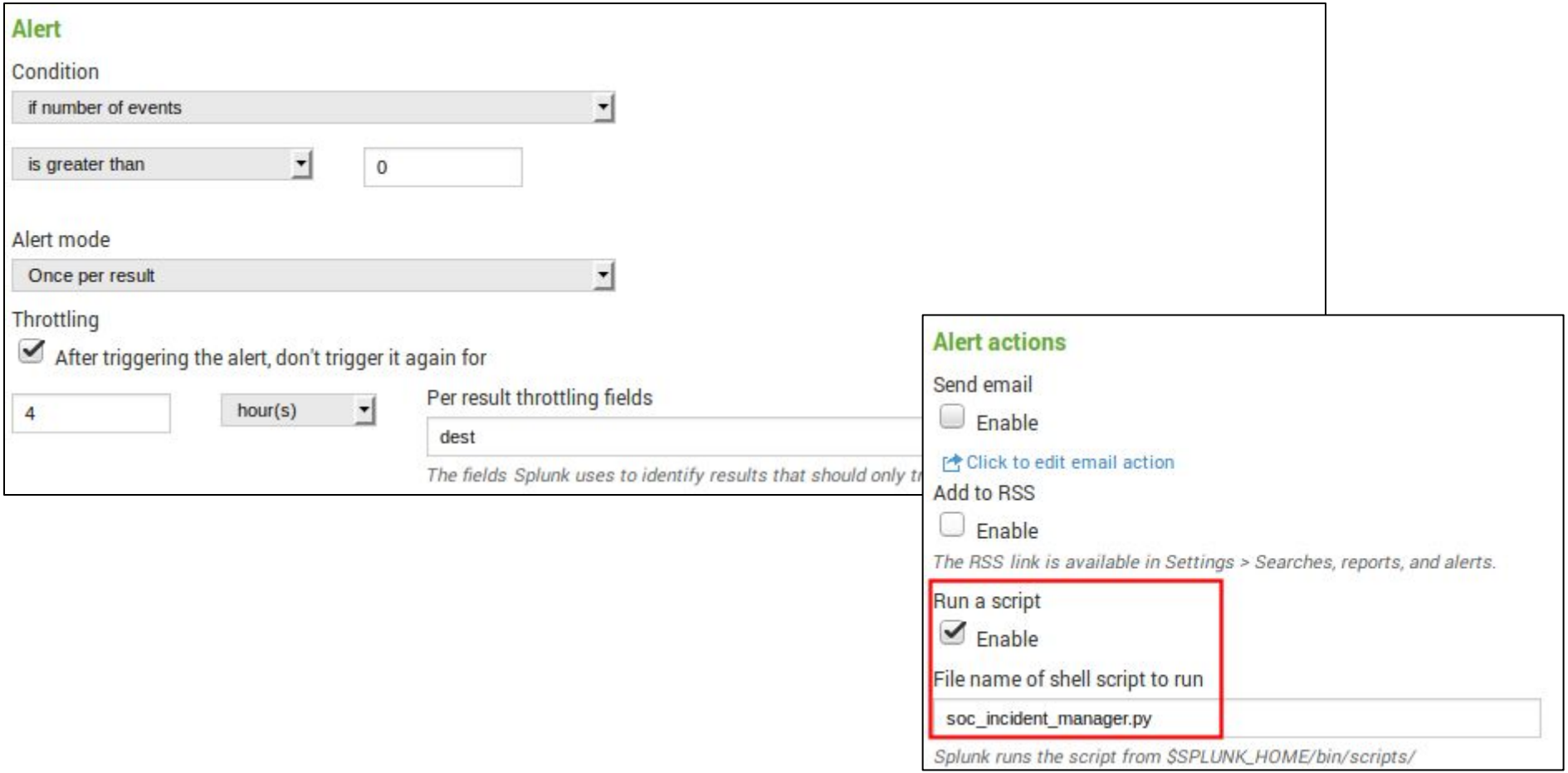
☑ Schedule this search

Schedule type *: Cron

Cron schedule: */15 * * * *

Enter a cron-style schedule.
For example '/5 * * * *' (every 5 minutes) or '0 21 * * *' (every day at 9 PM).*

> make integration



> make integration

*$SPLUNK_HOME/bin/scripts/**soc_incident_manager.py***

Lo script esegue le seguenti azioni

- lettura file di configurazione Alert
- creazione Security Event
- apertura eventuale ticket OTRS
- creazione link drill-down per analisi evento

> make integration

1 def getAlertConfig(search_name):

Edit Lookup File

soc_alerts_config.csv

Right-click the table cells for more editing options

	search_name	alert_format	drill_search
2	SOC Nagios alerts	OS - NAGIOS EVENT - device $dest - event $reason	sourcetype=nagios dest="$dest" | table _time vendor_severity src eventname reason | sort _time desc
3	SOC Password Guessing	AUTH - PASSWORD GUESSING - user $user on device $src - total $failure failures	<<authentication_search>>
4	SOC Snort Events LOW	INTRUSION - LOW ALERT - $signature - from $src to $dest - $dvc	<<posture_search>>
5	SOC Snort Events MEDIUM	INTRUSION - MEDIUM ALERT - $signature - from $src to $dest - $dvc	<<posture_search>>
6	SOC Snort Events MEDIUM only src	INTRUSION - MEDIUM ALERT - $signature - from $src - $dvc	<<posture_search>>
7	SOC Snort Events HIGH	INTRUSION - HIGH ALERT - $signature - from $src to $dest - $dvc	<<posture_search>>

soc_alerts_config.csv

Right-click the table cells for more editing options

	alert_ticket	alert_priority	alert_email
2	false	MEDIUM	
3	true	MEDIUM	soc@enav.it,[redacted]@enav.it
4	true	LOW	soc@enav.it,[redacted]@enav.it
5	true	MEDIUM	soc@enav.it,[redacted]@enav.it
6	true	MEDIUM	soc@enav.it,[redacted]@enav.it
7	true	HIGH	soc@enav.it,[redacted]@enav.it

- granularità nella definizione delle azioni di drill-down
- ogni contesto logico di sicurezza ha la sua ricerca ottimizzata

> make integration

2 def getTicketConfig():

Edit Lookup File

soc_ticket_config.csv

Import from CSV file: Sfoglia...

Right-click the table cells for more editing options

	id	server_uri	webservice	username	password	ticket_queue	ticket_type	ticket_url
2	0	https://[redacted]/otrs/nph-genericinterface.pl/Webservice/GenericTicketConnectorSOAP	http://www.otrs.org/TicketConnector/	otrs.sa[redacted]	[redacted]	SOC	14	https://[redacted]/otrs/index.pl?Action=AgentTicketZoom;TicketID=
3	1	https://[redacted]/otrs/nph-genericinterface.pl/Webservice/GenericTicketConnectorSOAP	http://www.otrs.org/TicketConnector/	otrs.sa[redacted]	[redacted]	SOC	14	https://[redacted]/otrs/index.pl?Action=AgentTicketZoom;TicketID=

3 def getResults(job_path, search_name, alertConfig, browser_url, startTime):

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	1	0	0	0

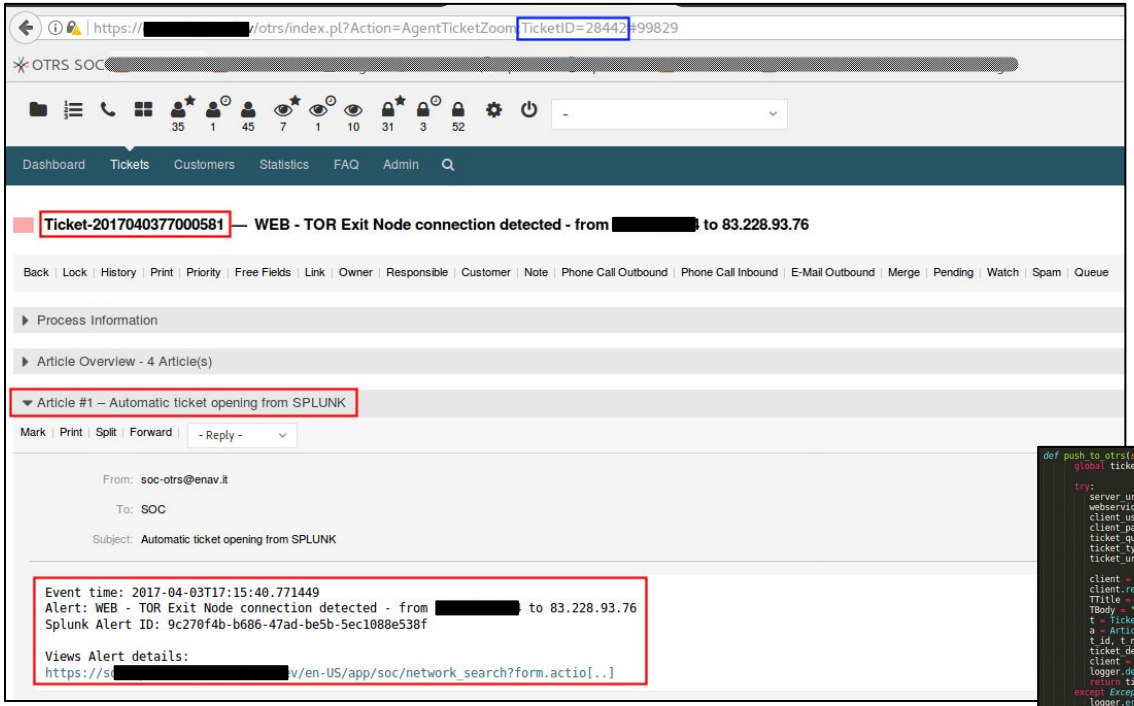
Security Events Overview

i	_time	Incident	Severity	ticket	Details
>	2017-04-03 17:15:40.771	WEB - TOR Exit Node connection detected - from [redacted] to 83.228.93.76	HIGH	2017040377000581	View

Generazione dei Security Events

> make integration

i	Time	Event
>	4/3/17 5:15:40.771 PM	time="2017-04-03T17:15:40.771449" dest="83.228.93.76" alert_id="9c270f4b-b686-47ad-be5b-5ec1088e538f" fired_alert="WEB - TOR Exit Node connection detected - from [redacted] to 83.228.93.76" src="[redacted] .34" drill_search="https://s[redacted]v/en-US/app/soc/network_search?form.action=&form.dvc=&form.src=[redacted]4&form.src_port=_port&form.src_interface=_interface&form.dest=83.228.93.76&form.transport=&form.dest_port=_port&form.dest_interface=_interface&earliest=1491231600.000000000&latest=now" search_name="SOC TOR exit nodes" ticket_link="https://d[redacted]v/otrs/index.pl?Action=AgentTicketZoom;TicketID=28442"
		date_hour = 17 date_mday = 3 date_minute = 15 date_month = april date_second = 40 date_wday = monday date_year = 2017 date_zone = local dest = 83.228.93.76 host = localhost index = soc_fired_alerts linecount = 1 punct = _="--:"_="..."_="---"_="-_____-__...__.."_=" source = soc_alert_handler.py sourcetype = soc_incidents splunk_server = [redacted]2 src = [redacted] timeendpos = 33 timestartpos = 7



Security Event

- Indice dedicato soc_fired_alerts
- Mapping tra evento SPLUNK (**alert_id**) e ticket OTRS (**TicketID**)

```
def push_to_otrs(severity, alert, alert_time,splunk_id,browser_url):
    global ticketConfig

    try:
        server_uri = ticketConfig['server_uri']
        webservice_name  = ticketConfig['webservice']
        client_user  = ticketConfig['username']
        client_pass  = ticketConfig['password']
        ticket_queue  = ticketConfig['ticket_queue']
        ticket_type  = ticketConfig['ticket_type']
        ticket_url  = ticketConfig['ticket_url']

        client = GenericTicketConnector(server_uri, webservice_name)
        client.register_credentials(client_user , client_pass)
        TTitle = alert
        TBody = "Event time: " + alert_time + "\nAlert: "+alert+"\nSplunk Alert ID: "+splunk_id+"\n\nViews Alert details: "+browser_url
        t = Ticket(State='new', Queue=ticket_queue,Priority=severity, Title=TTitle, CustomerUser='soc-otrs@enav.it', TypeID=ticket_type)
        a = Article(Subject='Automatic ticket opening from SPLUNK', Body=TBody, Charset='UTF8', MimeType='text/plain')
        t_id, t_number = client.ticket_create(t, a )
        ticket_detail={'ticket_id': t_id, 'ticket_number': t_number}
        client = GenericTicketConnector(server_uri, webservice_name)
        logger.debug("Ticket created ID  %s Number %s for %s", t_id, t_number, TTitle)
        return ticket_detail
    except Exception as e:
        logger.error("OTRS  Error %s" %e )
        return 0
```

> make integration

Network Search

Edit

Domain	Action	DVC	Source	Source Port	Source Interface	Destination
All	All	ALL	[redacted]	*	*	83.228.93.76

Transport Protocol	Destination Port		Destination Interface	Time Span	Aggregator	
All	*	Date time range	*	5 min	Device	Submit

_time	action	dvc	src	src_port	src_interface	dest	transport	dest_port	dest_interface	count
2017-04-03 17:08:07	allowed	[redacted]	1[redacted]	0	DMZINTERNET_SOC	83.228.93.76	tcp	0	INTERNET_TI	1

i	Time	Event
>	4/3/17 5:08:07.000 PM	Apr 3 17:08:07 [redacted] date=2017-04-03 time=16:08:07 devname=[redacted] device_id=[redacted] log_id=0021000002 subtype=allowed type=traffic pri=notice status=accept vd=INTERNET dir_disp=org tran_disp=snat src=[redacted] srcname=[redacted] src_port=53698 dst=83.228.93.76 dstname=83.228.93.76 dst_country=N/A src_country=N/A dst_port=80 tran_ip=[redacted] tran_port=14666 tran_sip=0.0.0.0 tran_sport=0 service=80/tcp proto=6 app_type=N/A duration=125 rule=1 policyid=1 identidx=0 sent=4321 rcvd=159836 shaper_drop_sent=0 shaper_drop_rcvd=0 perip_drop=0 shaper_sent_name=N/A shaper_rcvd_name=N/A perip_name=N/A sent_pkt=73 rcvd_pkt=111 vpn=N/A vpn_type=N/A vpn_tunnel=N/A src_int=DMZINTERNET_SOC dst_int=INTERNET_TI SN=2124893819 app=N/A app_cat=N/A user=N/A group=N/A carrier_ep=N/A profilegroup=N/A subapp=N/A subappcat=N/A

Drill-down punta la ricerca ottimizzata del contesto logico di sicurezza


NEED FOR SPEED™

> make optimization

Applicazione deve restringere ricerche al dominio logico di provenienza (rete gestionale, operativa etc) ed al tipo di dato (autenticazione, network etc) per velocizzare al massimo i tempi di risposta

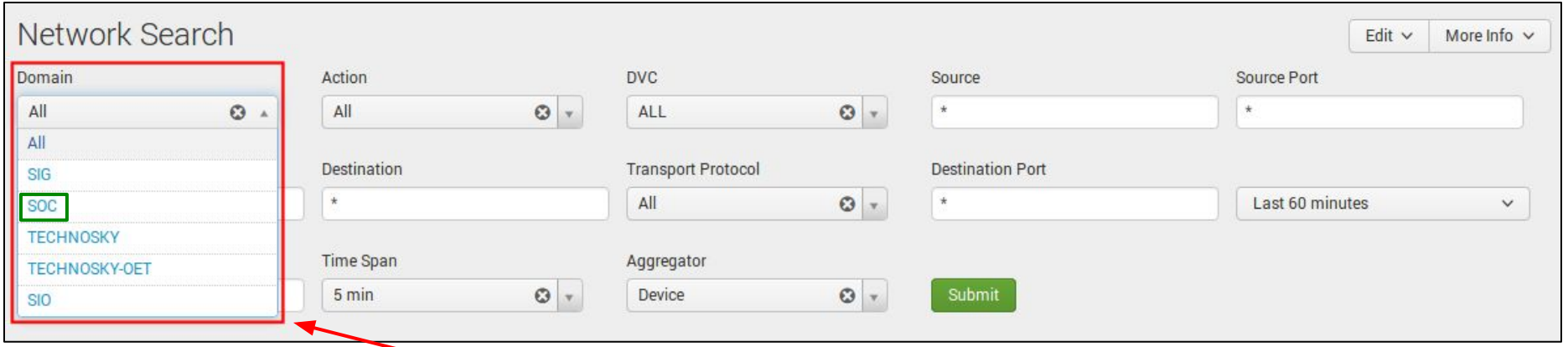
Questo significa selezionare l'indice corretto in fase di ricerca

soc_indexes_domains.csv

Right-click the table cells for more editing options

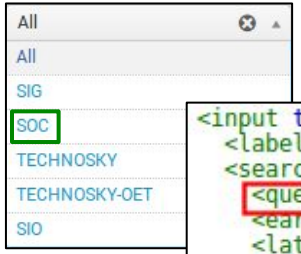
	index_domain	soc_domain	soc_model
2	cisco_net_sig	SIG	network
3	forefront_fw	SIG	network
4	fortinet	SOC	network
5	fortinet_ts	TECHNOSKY	network
6	hp_fw	TECHNOSKY-OET	network
7	squid	SOC	web
8	squid_sig	SIG	web
9	squid_itx	ITX	web
10	forefront	SIG	web
11	apache2	SOC	web_servers
12	snort	SOC	ids
13	estreamer	SIG	ids
14	symantec	SOC	malware

Costruzione del menù dei domini logici dal file di lookup



index_domain	soc_domain	soc_model
cisco_net_sig	SIG	network
forefront_fw	SIG	network
fortinet	SOC	network
fortinet_ts	TECHNOSKY	network
hp_fw	TECHNOSKY-OET	network
cisco_net_sio	SIO	network

> make optimization



Dashboard e Viste costruite in XML

```
<input type="dropdown" token="domain">
  <label>Domain</label>
  <search>
    <query>|inputlookup soc_indexes_domains.csv | WHERE soc_model="network" |  dedup soc_domain |fields soc_domain</query>
    <earliest>-24h@h</earliest>
    <latest>now</latest>
  </search>
  <fieldForLabel>soc_domain</fieldForLabel>
  <fieldForValue>soc_domain</fieldForValue>
  <prefix>[|inputlookup soc_indexes_domains.csv | search soc_domain="</prefix>
  <suffix>" soc_model="network"| eval index=index_domain | table index]</suffix>
  <choice value="*">All</choice>
  <default>*</default>
</input>
```

Esecuzione di una ricerca

```
| tstats `summariesonly` max(_time) as _time,values(All_Traffic.action) as action,count from datamodel=Network_Traffic where * [|inputlookup
soc_indexes_domains.csv | search soc_domain="SOC" soc_model="network"| eval index=index_domain | table index] All_Traffic.action="*"  All_traffic.src="*"
All_traffic.src_port="*" All_traffic.src_interface="*" All_traffic.dvc="*" All_traffic.dest="*" All_traffic.transport="*" All_traffic.dest_port="*" by
All_Traffic.dvc,All_Traffic.src,All_Traffic.src_port,All_Traffic.src_interface,All_Traffic.dest,All_Traffic.transport,All_Traffic.dest_port,All_Traffic.d
est_interface | `drop_dm_object_name("All_Traffic")`  | fields _time,action,dvc,src,src_port,src_interface,dest,transport,dest_port,dest_interface,count
| sort - _time, count
```

index=fortinet


IN
REAL LIFE

> Gestione di un Security Event

SOC SourceFire Event HIGH

Searches, reports, and alerts » SOC SourceFire Ev

[Security Event, ticket OTRS, email]

2017-04-14 09:40:07.000 SIG INTRUSION - HIGH ALERT - FILE-FLASH Adobe Flash Player mp4 size memory corruption attempt - from 104.45.17.225 - SIG-Sourcefire HIGH 2017041477000121 View

Da SOC monitoraggio

Rispondi | Rispondi a tutti | Inoltra | Indesiderata | Elimina | Altro

Oggetto [SPLUNK] SIG INTRUSION - HIGH ALERT - FILE-FLASH Adobe Flash Player mp4 size memory corruption attempt - from 104.45.17.225 - SIG-Sourcefire [Ticket-2017041477000121] 09:40

A SOC, SOC OTRS

Ticket-2017041477000121 SIG INTRUSION - HIGH ALERT - FILE-FLASH Adobe Flash Player mp4 size memory corruption attempt - from 104.45.17.225 - SIG-Sourcefire is opened on Security ENAV Service Desk

You can access the ticket at following addresses

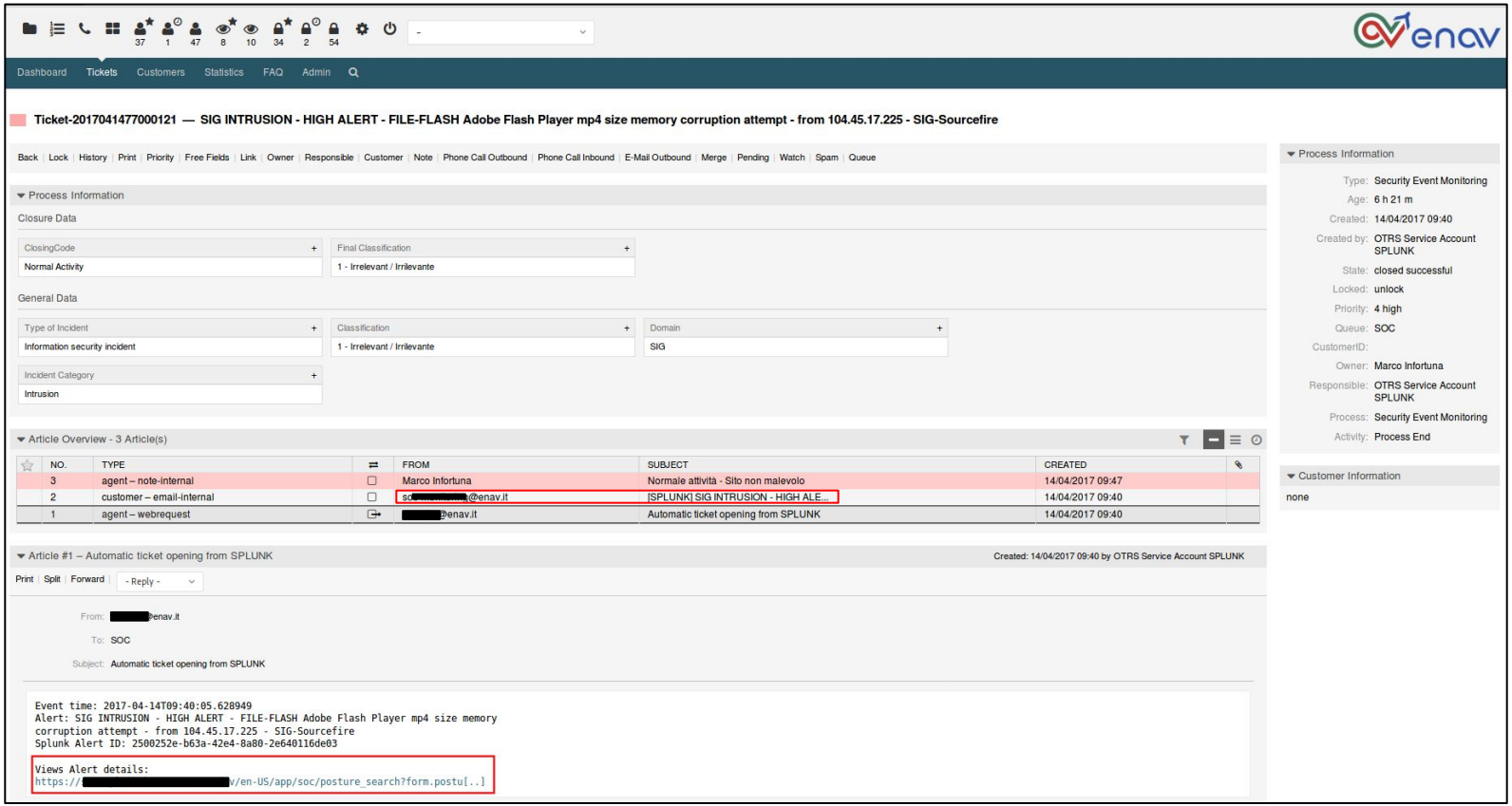
- from SOC network
  https://[redacted]s/index.pl?Action=AgentTicketZoom;TicketID=28965
- from SIG network
  https://[redacted]trs/index.pl?Action=AgentTicketZoom;TicketID=28965

You can access SPLUNK event details only from SOC network at following address:

https://s[redacted]/en-US/app/soc/posture_search?form.posture_value=104.45.17.225&form.posture_tags=tag%3D%22*ids%22&form.posture_tags=tag%3D%22soc_proxy%22&earliest=1492155000.000000000&latest=now

> Gestione di un Security Event

Integrazione completa con OTRS per tracciamento attività con invio email



> Gestione di un Security Event

Drill-down specifica per evento che raggruppa differenti sorgenti (rete + IDS)

RAW Search

Edit | More Info

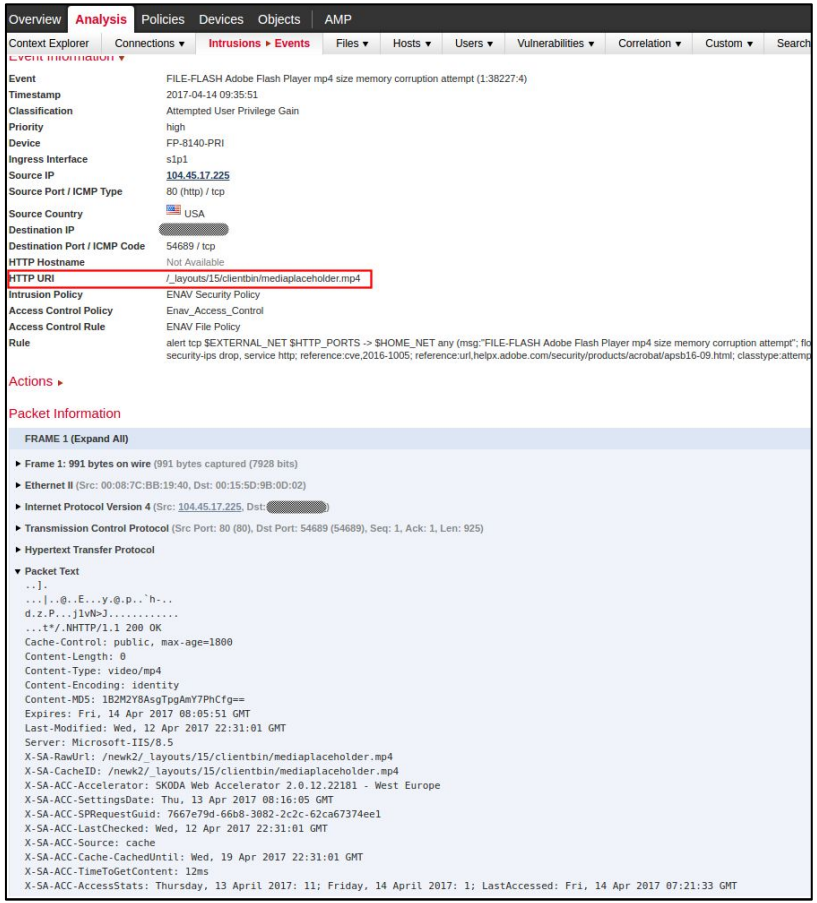
Posture Value: 104.45.17.225 | Date time range | Tags: Intrusion Detection, Web/Proxy | Sourcetype: All | Submit

i	Time	Event
>	4/14/17 9:35:51.000 AM	rec_type=400 rec_type_simple="IPS EVENT" event_sec=1492155351 event_usec=269322 sensor=FP-8140-BCK event_id=357782 msg="FILE-FLASH Adobe Flash Player mp4 size memory corruption attempt" sid=38227 gid=1 rev=4 class_desc="Attempted User Privilege Gain" class=attempted-user priority=high src_ip=104.45.17.225 dest_ip=[redacted] src_port=80 dest_port=54689 ip_proto=6 impact_bits=3 impact=3 blocked=2 mpls_label=0 vlan_id=0 ids_policy="ENAV Security Policy" user=9999997 web_app=0 client_app=Chrome app_proto=HTTP fw_rule="ENAV File Policy" fw_policy=Enav_Access_Control iface_ingress=s1p1 iface_egress=00000000-0000-0000-0000-000000000000 sec_zone_ingress=00000000-0000-0000-0000-000000000000 sec_zone_egress=00000000-0000-0000-0000-000000000000 connection_sec=1492155298 instance_id=6 connection_id=10149 src_ip_country="united states" dest_ip_country=0 num_ioc=0 host = soc-splunksh-02 source = eStreamer sourcetype = eStreamer
>	4/14/17 9:35:51.000 AM	rec_type=400 rec_type_simple="IPS EVENT" event_sec=1492155351 event_usec=286670 sensor=FP-8140-PRI event_id=354848 msg="FILE-FLASH Adobe Flash Player mp4 size memory corruption attempt" sid=38227 gid=1 rev=4 class_desc="Attempted User Privilege Gain" class=attempted-user priority=high src_ip=104.45.17.225 dest_ip=[redacted] src_port=80 dest_port=54689 ip_proto=6 impact_bits=3 impact=3 blocked=2 mpls_label=0 vlan_id=0 ids_policy="ENAV Security Policy" user=9999997 web_app=0 client_app=Chrome app_proto=HTTP fw_rule="ENAV File Policy" fw_policy=Enav_Access_Control iface_ingress=s1p1 iface_egress=00000000-0000-0000-0000-000000000000 sec_zone_ingress=00000000-0000-0000-0000-000000000000 sec_zone_egress=00000000-0000-0000-0000-000000000000 connection_sec=1492155298 instance_id=6 connection_id=6877 src_ip_country="united states" dest_ip_country=0 num_ioc=0 host = soc-splunksh-02 source = eStreamer sourcetype = eStreamer
>	4/14/17 9:35:51.000 AM	Apr 14 09:35:51 [redacted] Apr 14 09:35:51 [redacted] vendor=Forcepoint product=Security product_version=8.2.0 action=permitted severity=1 category=21 user=LDAP://[redacted] OU=[redacted] rc_host=[redacted] src_port=60850 dst_host=www.skoda-auto.it dst_ip=104.45.17.225 dst_port=80 bytes_out=934 bytes_in=925 http_response=200 http_method=GET http_content_type=video/mp4 http_user_agent=Mozilla/5.0_(Windows_NT_6.1;_WOW64)_AppleWebKit/537.36_(KHTML,_like_Gecko)_Chrome/57.0.2987.133_Safari/537.36 http_proxy_status_code=200 reason=- disposition=1026 policy=Super_Administrator**RulePolicy_Default,Super_Administrator**RulePolicy_Default,Super_Administrator**RulePolicy_Default,Super_Administrator**RulePolicy_TopMngt_Dirig role=8 duration=0 url=http://www.skoda-auto.it/_layouts/15/clientbin/mediaplaceholder.mp4 host = 172.31.1.176 source = udp:1530 sourcetype = squid_sig
>	4/14/17 9:35:51.000 AM	Apr 14 09:35:51 [redacted] Apr 14 09:35:50 [redacted] vendor=Forcepoint product=Security product_version=8.2.0 action=permitted severity=1 category=21 user=LDAP://[redacted] OU=[redacted] src_host=[redacted] src_port=60845 dst_host=www.skoda-auto.it dst_ip=104.45.17.225 dst_port=80 bytes_out=970 bytes_in=193582 http_response=200 http_method=GET http_content_type=image/jpeg http_user_agent=Mozilla/5.0_(Windows_NT_6.1;_WOW64)_AppleWebKit/537.36_(KHTML,_like_Gecko)_Chrome/57.0.2987.133_Safari/537.36 http_proxy_status_code=200 reason=- disposition=1048 policy=Super_Administrator**RulePolicy_Default,Super_Administrator**RulePolicy_Default,Super_Administrator**RulePolicy_Default,Super_Administrator**RulePolicy_TopMngt_Dirig role=8 duration=0 url=http://www.skoda-auto.it/modelli/nuova-fabia/PublishingImages/2016/interni/fabia-design-slider-06.jpg host = 172.31.1.176 source = udp:1530 sourcetype = squid_sig

SOC SourceFire Event HIGH - by src	SIG INTRUSION - HIGH ALERT - $signature - from $src - $dvc	<<posture_search>>

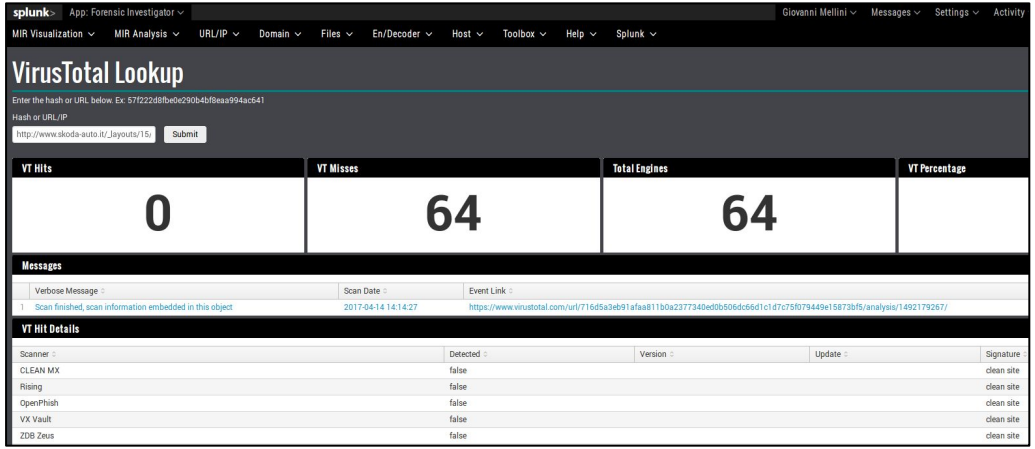
posture_search	form.posture_value=$ext_ip&form.posture_tags=tag%3D%22*ids%22&form.posture_tags=tag%3D%22soc_proxy%22

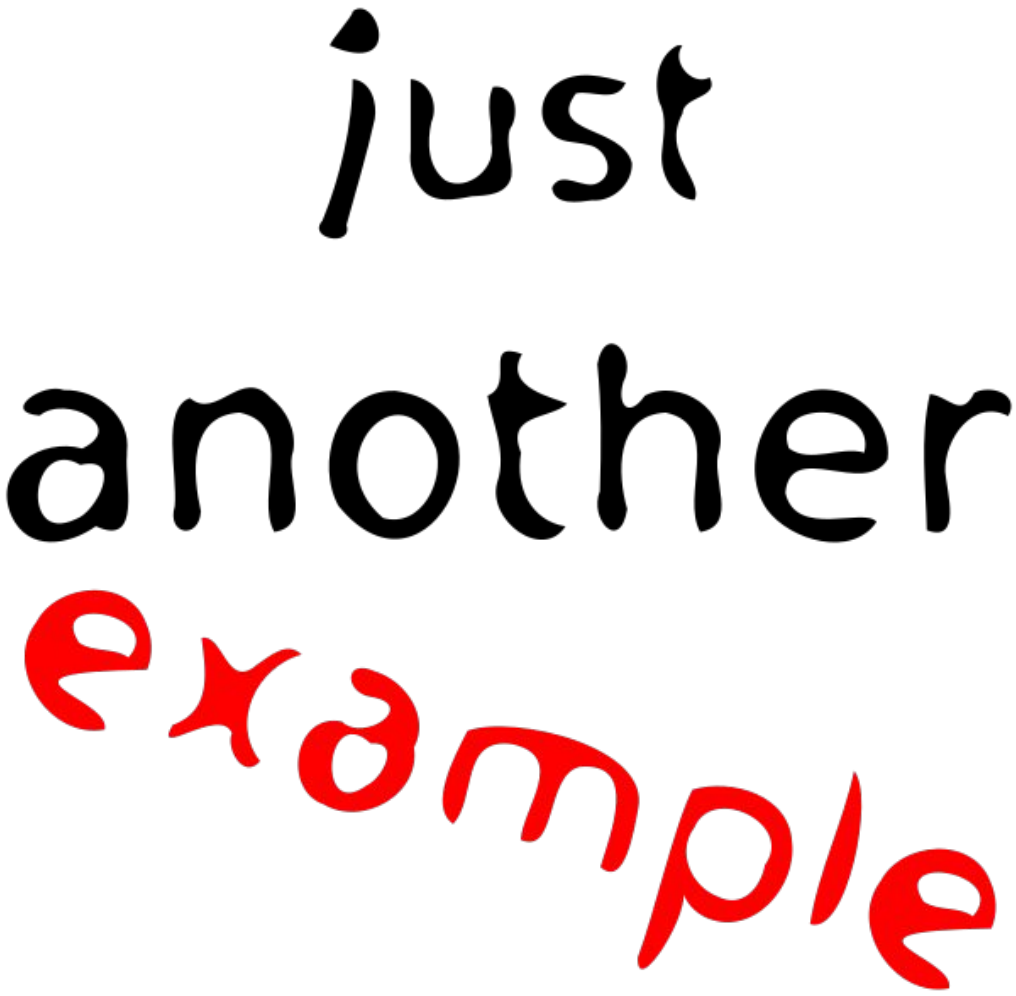
> Gestione di un Security Event



Analisi effettuata su interfaccia della sonda e all'interno dell'istanza SPLUNK usando ad esempio app specifiche

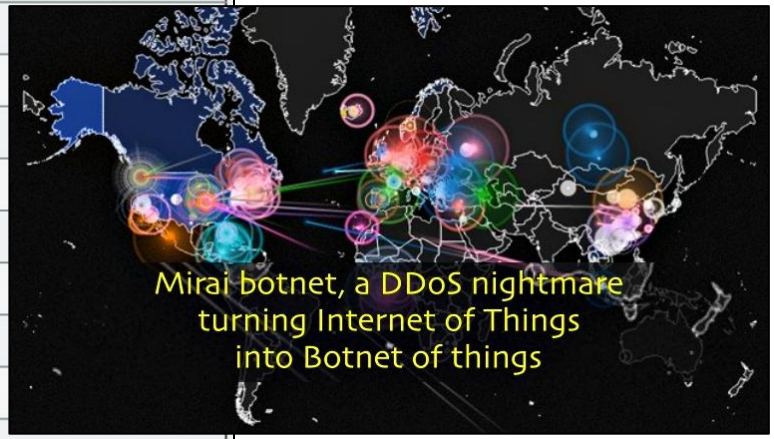
Forensic Investigator




just
another
example

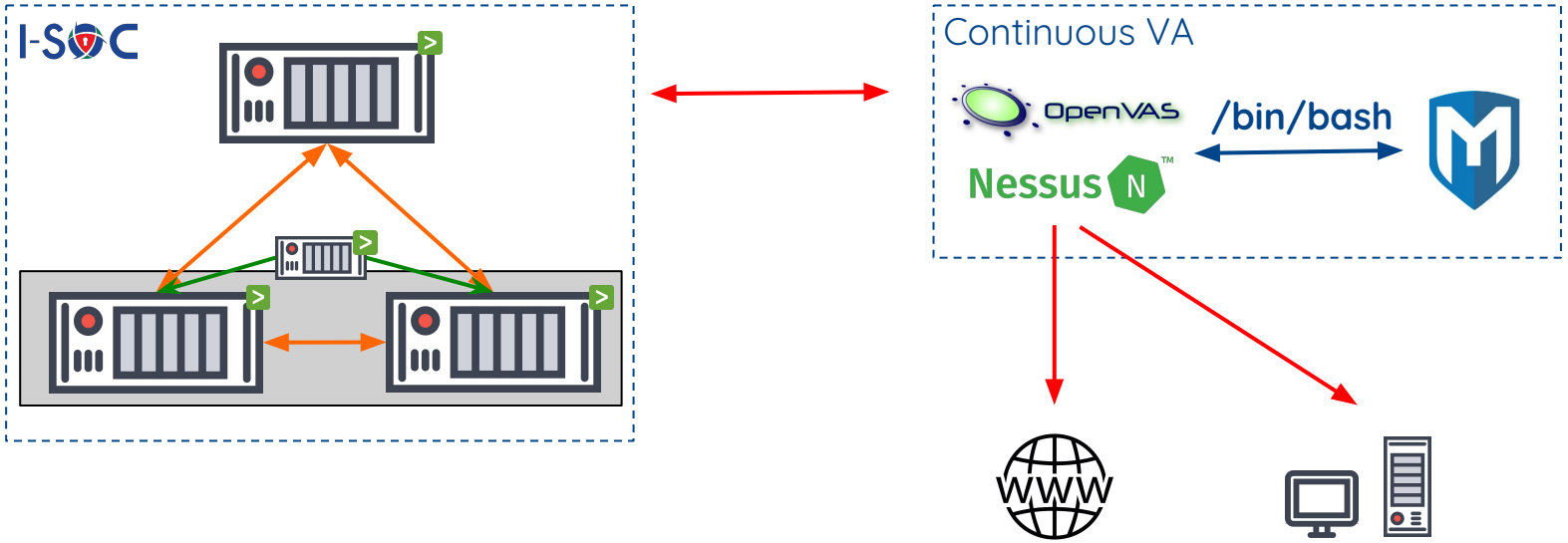
> Continuous VA

Code Name	Solution
"EternalBlue"	Addressed by MS17-010
"EmeraldThread"	Addressed by MS10-061
"EternalChampion"	Addressed by CVE-2017-0146 & CVE-2017-0147
"ErraticGopher"	Addressed prior to the release of Windows Vista
"EsikmoRoll"	Addressed by MS14-068
"EternalRomance"	Addressed by MS17-010
"EducatedScholar"	Addressed by MS09-050
"EternalSynergy"	Addressed by MS17-010
"EclipsedWing"	Addressed by MS08-067

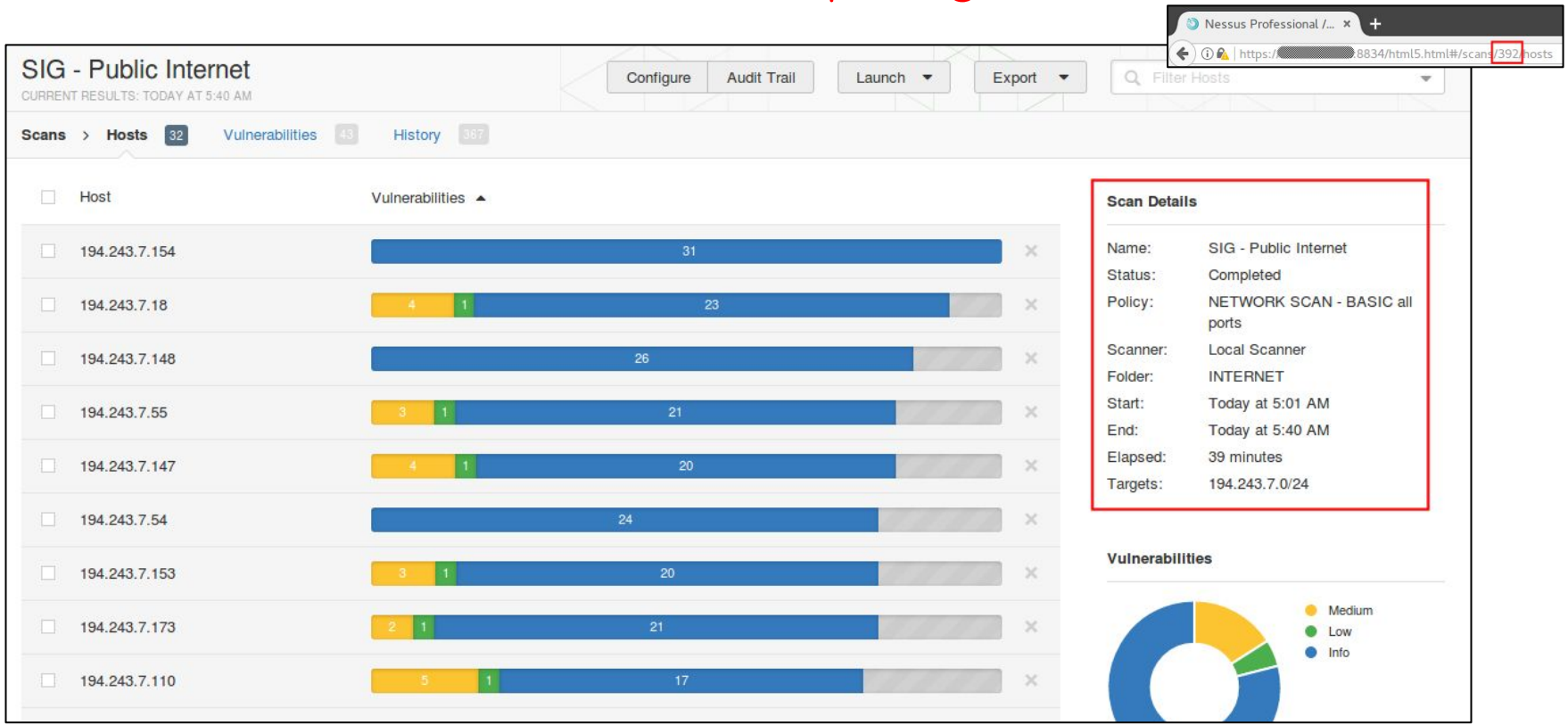


Necessità di conoscere puntualmente quali servizi si espongono su rete Internet e monitoraggio per variazioni non autorizzate

Da i-SOC recupero giornaliero dei dati di scansione Nessus/OpenVAS



Definizione di una policy di VA



Esecuzione scriptata via Metasploit ed import dati

```
## INTERNET
# SIG
00 5 * * * /usr/local/bin/msfpro -- -r /root/scan_execute_sig_public_internet.rc -o /root/scan_execute_sig_public_internet.output
```

```
root@soc-sysva-01:~# cat scan_execute_sig_public_internet.rc
workspace INTERNET
load nessus
nessus_connect msf:[redacted]@127.0.0.1:8834
nessus_scan_launch 392
```

```
## IMPORT IN MSF
0 10 * * * /usr/local/bin/msfpro -- -r /root/scan_import.rc -o /root/scan_import.output
```

```
root@soc-sysva-01:~# cat /root/scan_import.rc
load nessus
nessus_connect msf[redacted]@127.0.0.1:8834
workspace INTERNET
nessus_db_import 392
```

Import dei dati su i-SOC via REST API

```
[06:49:42].{ root@s                    02:/opt/splunk/splunk-sw/etc/apps/Splunk_TA_nessus/default }. # cat inputs.conf
##Modular input for Nessus 6.X

[nessus]
interval = 30 8 * * *
url = https://                         :8834
# msf user
access_key = 498                                                              ac067
secret_key = 3fa                                                              e21ce
start_date = 1999/01/01
page_size = 1000
#start_by_shell = false
```

AddOn+ **Splunk Add-on for Tenable**

don't reinvent
THE WHEEL

Creazione di regole di alert per identificazione servizi non noti

SOC SIG New Public Portal Services

Searches, reports, and alerts » SOC SIG New Public Portal Services

Search

```
index=nessus_scan 194.243.7. ports{}.port!=0 | stats count by host-ip ports{}.port ports{}.transport |
table  host-ip ports{}.port ports{}.transport | search NOT [  inputlookup soc_sig_public_services.csv ]
fields host-ip ports{}.port ports{}.transport | makemv delim=";" ports{}.port allowempty=true | mvexpand
ports{}.port] |  lookup soc_all_assets.csv key as host-ip OUTPUT dns  | eval
host_asset_soc=if(isnull(dns),"n.d.",dns) | lookup dnslookup clientip AS host-ip OUTPUT clienthost  |
eval dns_lookup=if(isnull(clienthost),"n.d.",clienthost) | rename host-ip as host_ip |rename
ports{}.port as port |rename ports{}.transport as transport| stats count by host_ip host_asset_soc
dns_lookup port transport
```

Description

Ricerca di nuovi servizi/IP esposti su rete pubblica SIG

Run as

Owner User

Learn more

Time range

Start time: -24h@h

Finish time: now

soc_sig_public_services.csv

Right-click the table cells for more editing options

	host-ip	ports{}.port	ports{}.transport	host_asset_soc
2	194.243.7.3	53	tcp	dns1.enav.it
3	194.243.7.3	53	udp	dns1.enav.it
4	194.243.7.11	80;443	tcp	enavmail.enav.it

Security Events Overview

i	_time	Incident	Severity	ticket	Details
>	2017-02-02 10:15:09.000	NET - New SIG Public Services: 194.243.7.53 (tcp / 443) - DNS: abs.enav.it	HIGH	2017020277000102	View

Dati delle scansioni arricchiti con dettagli vulnerabilità

Vulnerabilities Center

Modifica | Altre info

Oggi

Scanned IPs	IPs with vulnerabilities detected	Average CSS score (10 max)
74	34	6

Hosts with Vulnerabilities

Please note that Vulnerabilities data are imported daily so today is the default timepicker value. If you don't find any vulnerability listed is possible that: 1. we are very strong in patching 2. you have to wait the nesssus import job at 08:30 AM 3. nessus import job failed

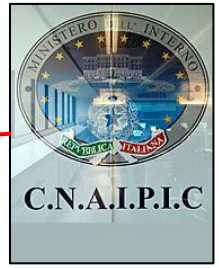
dest	Host	critical	high	medium	low
[redacted]	[redacted]	5	19	14	2
[redacted]	[redacted]	5	19	13	2
[redacted]	[redacted]	4	17	10	2
[redacted]	[redacted]				
[redacted]	[redacted]				

Signatures Details

signature_id	signature	severity	cvss	exploit_available	count
95284	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : python2.7, python3.2, python3.4, python3.5 vulnerabilities (USN-3134-1) (httpoxy)	critical	10.0	false	11
94730	Ubuntu 12.04 LTS : linux vulnerabilities (USN-3126-1)	critical	10.0	false	3
78555	OpenSSL Unsupported	critical	10.0	false	1
73403	OpenSSL 1.0.0 < 1.0.0m Multiple Vulnerabilities	high	9.3	true	1
94954	Ubuntu 14.04 LTS : openjdk-7 vulnerabilities (USN-3130-1)	high	9.3	true	1

> Monitoraggio IoC

CERTs



[IPs, URLs]

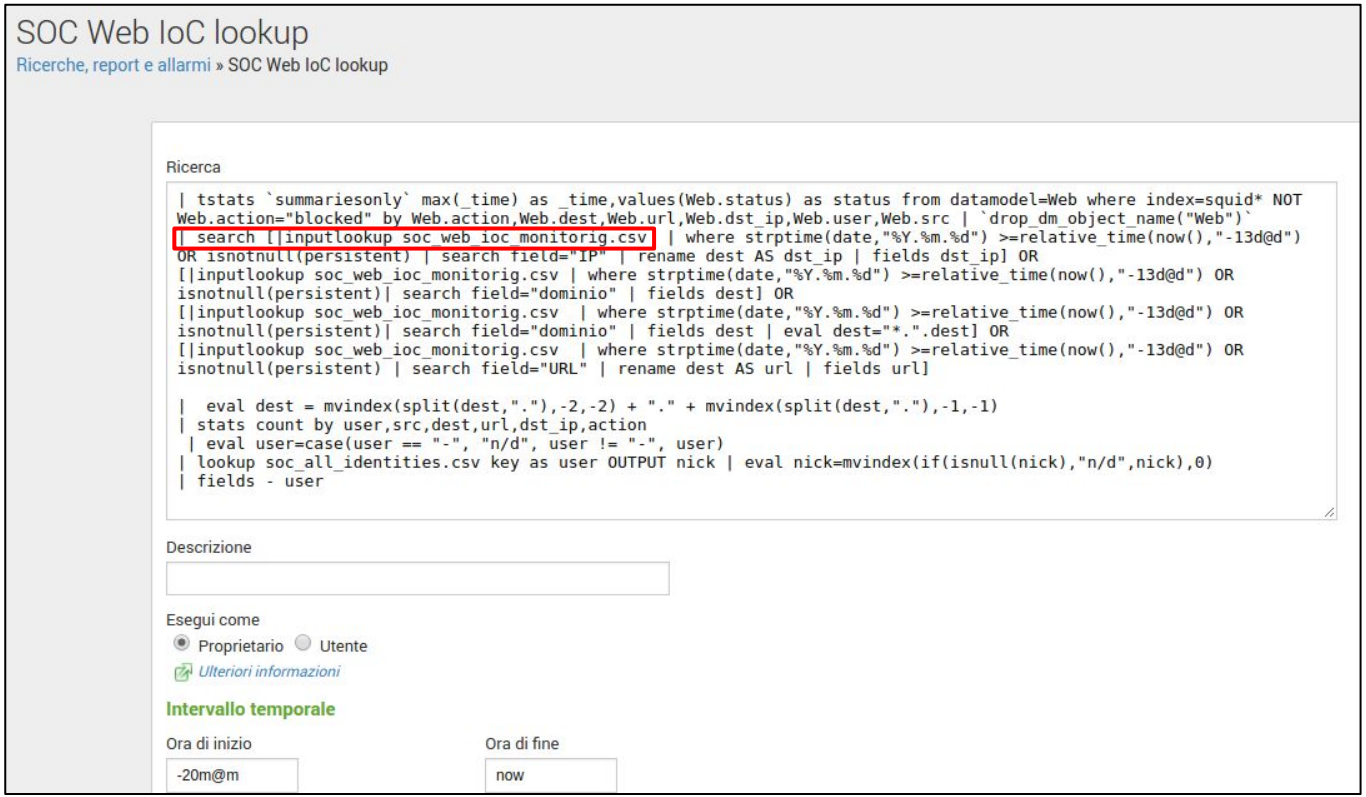
soc_web_ioc_monitorig.csv

Right-click the table cells for more editing options

Revision: Current version

1	field	dest	date	Blocco proxy SIG	persistent	riferimento
216	URL	admin.adoma-jawel-manufact.com/cgi-bin2/kc21.exe	2017.04.07			CIMBL-303
217	URL	all400pples.org.in/molina/fre.php	2017.04.07			CIMBL-303
218	dominio	antiquesonbroad.com	2017.04.07			CIMBL-303
219	URL	antiquesonbroad.com/wp-includes/customize/newchn/index.php	2017.04.07			CIMBL-303
220	dominio	arihanttradersngp.com	2017.04.07			CIMBL-303

Verifica schedulata



> Monitoraggio IoC

Verifica on-demand

Threat Intelligence

Come e da dove ottenere IoC usabili?
Come integrare in maniera automatica al SOC?
Svecchiamento con che criteri?

MineMeld

Grazie, ci vediamo al LAB domani!

@merlos1977

giovannimellini

https://scubarda.wordpress.com