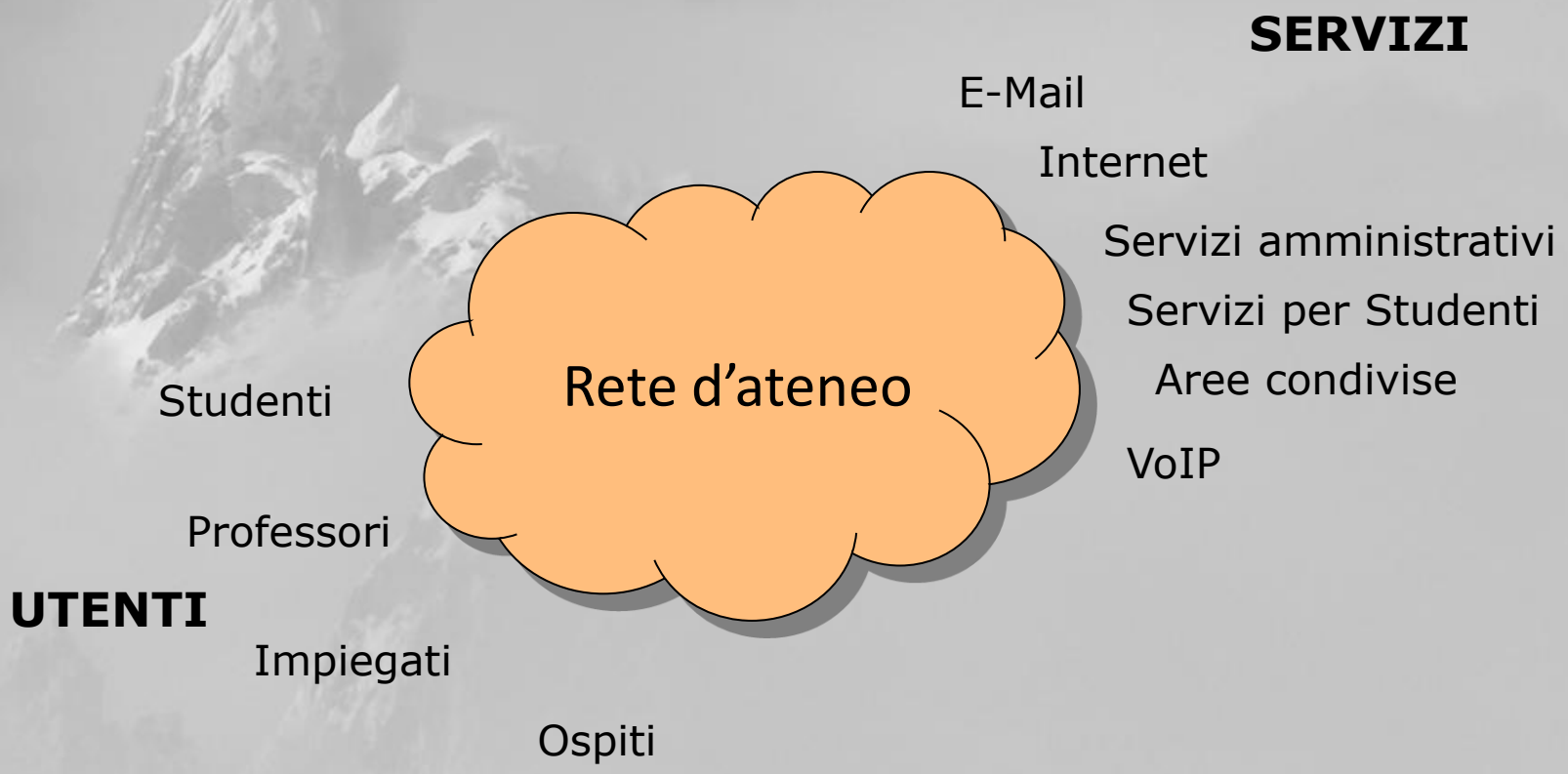
GESTIONE EFFICIENTE DEGLI INCIDENTI DI SICUREZZA IN UNA RETE COMPLESSA ED ETEROGENEA: UN CASO REALE

(Università degli Studi di Milano, Facoltà di Giurisprudenza, 05 GIUGNO 2014)

Nicla Diomede

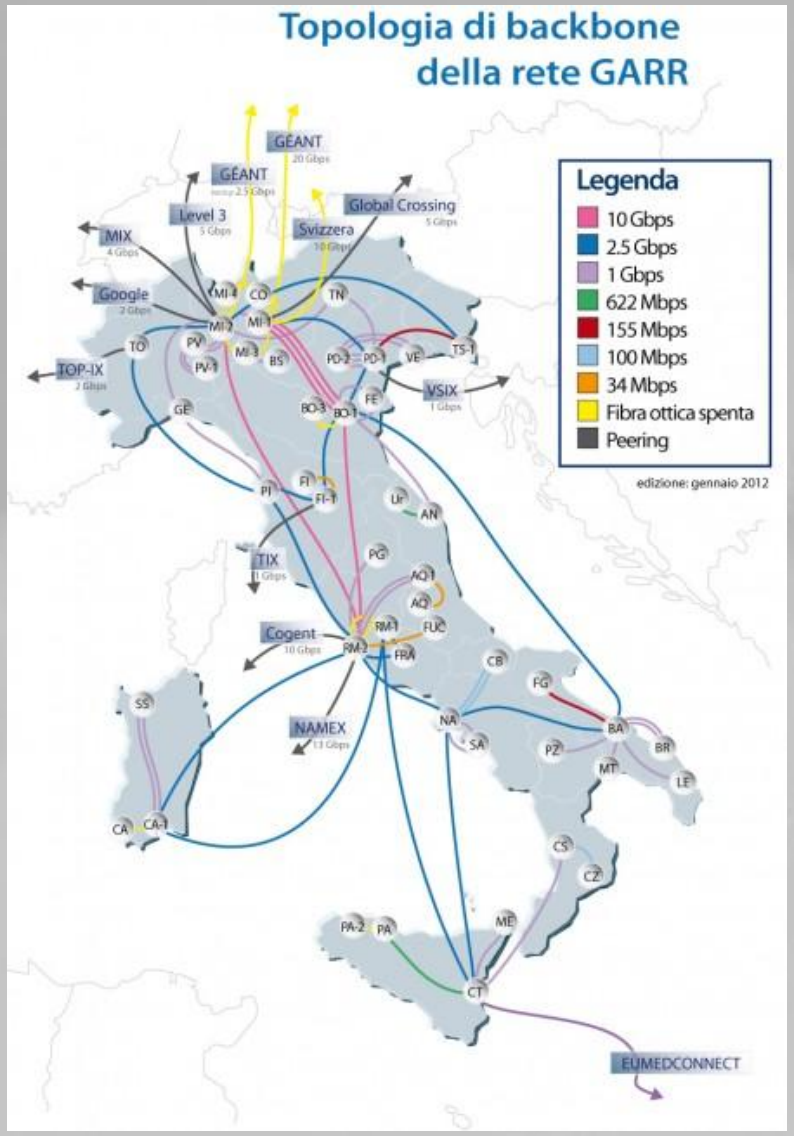
Le Reti Universitarie

Ambiente Universitario



Caratteristiche della rete Universitaria

- Lo scenario considerato è di una rete complessa, estesa ed eterogenea:
  - Unica per Ricerca, Didattica, Amministrazione
  - Elevato (>70) numero di sedi distribuite sul territorio
  - ambienti misti: presenza negli Ospedali
  - 65000 utenti
  - 40.000 punti cablati di cui circa almeno 10.000 attivi
  - Cablata e wireless
  - 65000 utenti wireless (10.000 utenti distinti al giorno)
  - Presenza promiscua nella stessa zona di varie tipologie di utenti appartenenti a strutture diverse
- Caratterizzato da:
  - Alta velocità
  - Affidabilità (ridondanza logica e fisica)
  - Supporto di servizi evoluti
- Interconnessa a Global Internet attraverso la Rete nazionale **GARR**



Consortium GARR

- gli Enti fondatori (CNR, ENEA, INFN e la Fondazione CRUI);
- gli organismi di ricerca vigilati dal MIUR, tra cui ASI, INAF, INGV e altri;
- i Consorzi Interuniversitari per il Calcolo (CASPUR, CILEA, CINECA);
- Organismi culturali e di ricerca afferenti ad altri Ministeri, quali MiBAC e Salute;

- Rete ad altissima velocità collegata a:
  - rete della ricerca Europea
  - Global Internet

- Regolamentata da policy

I beni universitari

- L'università acquisisce, usa e memorizza informazioni relative ai suo utenti: impiegati, docenti, pazienti, studenti, società con cui collabora.
- E' necessario che questi dati siano gestiti in modo appopriato per prevenire la perdita, il danneggiamento, l'accesso o il furto delle informazioni.
- Il cattivo utilizzo, la perdita o compromissione comportano un costo economico, un danno d'immagine e possibili ripercussioni legali/penali.
- DATI UNIVERSITA':
  - Proprietà intellettuale → ricerca, brevetti
  - Dati sensibili: dati medici
  - Dati amministrativi: dati del personale, stipendi, etc..
  - Dati legati al core business: dati carriera scolastica
  - Dati di studio per attività conto terzi
- La rete stessa è un bene

Criticità della sicurezza nelle Università

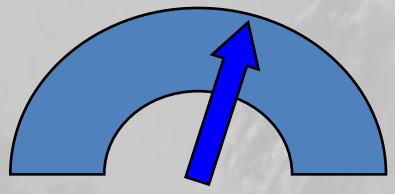
La sicurezza informatica è un problema

- complesso (coinvolge la rete, gli hosts e le persone),
- multilivello (tecnico, organizzativo, legale e sociale),
- in divenire (non è uno status, va costantemente mantenuta).

La sicurezza = protezione dei propri beni

≠ controllo o censura

L'Università NON è un azienda



Sicurezza Facilità d'uso

LE POLICY UNIVERSITARIE (AUP)

- Forniscono un insieme di regole per la tutela della rete, degli host e dei servizi informatici.
- Sensibilizzare e responsabilizzare l'utenza: costituisce una sorta di carta dei diritti e dei doveri dell'utente dell'Università.
- Impedire che la rete universitaria possa essere fonte di attacchi verso l'esterno.

Immagine tratta da:

http://www.thetis.it/projects/transportation-management/urban-mobility-delhi.html

Acceptable Use Policy

- Tutti gli utenti devono essere riconosciuti ed identificabili;
- Uso per sole attività istituzionali

E' VIETATO

- fornire accesso a soggetti non autorizzati;
- Compiere attività (diffusione di virus, etc.) che danneggino, molestino o limitino le attività altrui o i servizi;
- creare o trasmettere materiale che attenti alla dignità umana, se non per motivi di ricerca
- Danneggiare o cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti,
- Pubblicizzare attività proprie per fini di lucro
- Attività vietata da leggi dello Stato
- ------

Il regolamento di Sicurezza

DEFINISCE

- Chi può accedere alla rete
- Come e dove accedervi:
  - LAN cablate
  - HOTSPOT, Wireless LAN, Eduroam
  - Biblioteche
  - Via vpn
  - Aule informatiche
- Protocolli consentiti
- Attività ammesse e non
- Identificazione degli utenti
- Responsabilità personali dei contenuti diffusi
- Sanzioni per trasgressori
- Misure minime per server centrali, locali e postazioni utente
- Ruoli nella gestione della sicurezza

LA REALTA' E' MOLTO COMPLESSA

Immagine Tratta da "Minority Report"

Gestione tecnica dell'infrastruttura simile a quella del provider:

- Estensione e complessità della rete
- Presenza promiscua e contemporanea di diversi tipologie di utenti appartenenti a strutture diverse
- Controllo e gestione totale dell'infrastruttura di rete
- Nessun controllo dei singoli pc/server locali gestiti in autonomia dalle singole strutture
- No controllo sull'accesso fisico alle sedi universitarie

Dal punto di vista giuridico il modello è quello privato:

- Rete riservata ai soli aventi diritto

Difficoltà di adottare policy stringenti di sicurezza:

- Eterogeneità utenti, vastità e molteplicità di utilizzo, libertà di ricerca
- Facilità di uso (autenticazione centralizzata per accesso alla rete solo in zone ad accesso pubblico)

Incidenti Informatici : migliaia all'anno

- **Rete molto veloce, soggetta a continui tentativi di intrusione**
- **10.000 host in rete cablata e altrettanti via wireless**
- **Macchine con alte performance ma non sempre ben gestite**

di cui alcuni con risvolti penali/legali (richiesta A.G.)

RICERCA DEL COMPROMESSO TRA:

- **Necessità di proteggere beni universitari**
- **Garantire livelli di servizio**
- **Tutelare l'ente da responsabilità (D. Lgs 231/2001)**
- **Tutelare la privacy degli utenti**
- **Garantire la conformità allo Statuto dei lavoratori**

INCIDENTI INFORMATICI

INCIDENTE INFORMATICO: DEFINIZIONE

Per Incidente di sicurezza si intende qualsiasi violazione di:

- Politica aziendale
- Legge
- Evento che può compromettere il corretto funzionamento di uno o più computer

Può essere:

- Semplice o complesso (riguardare 1 o più asset)
- Coinvolgere diverse componenti aziendali
- Può avere risvolti giuridico – legali
- A priori deve essere gestito in modo da poter essere utilizzato in ambito giudiziario

LA GESTIONE DEGLI INCIDENTI

Presuppone come elemento fondante l'esistenza di:

- Politiche di sicurezza
- La conoscenza delle stesse in azienda
- Procedure da mettere in atto in caso di incidente

LA GESTIONE DEGLI INCIDENTI

Si compone di varie fasi:

1. Individuazione dell'Incidente tramite
   - Strumenti automatici (Firewall, IDS, SIEM, AV) e analisi
   - Fonti terze parti (AG, CERT esterni, …)
2. Risposta informativa all'incidente:
   - Formazione della Fonte di Prova attraverso:
     - Acquisizione delle immagini disco, log eventi, flussi
3. Escalation informativa (eventuale AG, management, esterna ad altre aziende)

LA GESTIONE DEGLI INCIDENTI (2/2)

4. Effettuazione dell'analisi dell'incidente
   - Esame Post mortem
   - Analisi dei logs, flussi e correlazione degli eventi
5. Reporting e Conclusioni:
   - Doc contenente report e conclusioni sull'incidente da inoltrare al management o AG
     - Acquisizione delle immagini disco, log eventi, flussi
6. Risoluzione dell'incidente
   - Attività di ripristino,
   - Messa a punto di meccanismi migliorativi sulla base dell'esperienza appresa

GESTIONE DEGLI INCIDENTI: DALLA TEORIA ALLA PRATICA

SICUREZZA E MONITORAGGIO DEL TRAFFICO

- La rete in ambito universitario è un BENE essenziale per consentire il buon funzionamento della didattica, ricerca e amministrazione
  - Necessità di proteggere la rete e i suoi hosts :
    - per evitare il blocco parziale o totale delle attività;
    - per prevenire la perdita, il danneggiamento, l'accesso o il furto delle informazioni degli hosts
    - Che gli host della rete possano essere fonte di attacchi all'esterno (anche con risvolto legale)
  - Gestione e razionalizzazione nell'uso della banda

Gestione della Sicurezza: problematiche

- Elevato Numero di host in rete (wireless e wired)
- Utilizzo di Indirizzamento Pubblico
- Non Controllo delle postazioni utente
- Presenza di numerosi Server Locali
- Non applicabilità di filtri stringenti per Non limitare l'attività di ricerca
- non esistenza Firewall Perimetrale posto sul link di Collegamento GARR
- continui tentativi di attacco e compromissione dall'esterno

Gestione della Sicurezza: problematiche

- Attacchi e minacce sempre più sofisticate e multivettoriali,
  - Molteplicità Spyware, worm, attacchi, virus veicolati attraverso:
    - comuni applicazioni “consentite” (ad es. web)
    - mutevoli nel tempo
    - dispositivi mobili
- Limitate risorse in termini di personale attività SOC-IRT
- Esiguità di referenti locali interni o esterni formati sui temi di sicurezza
- Poca Sensibilità dell’utenza sui temi di sicurezza

Premessa

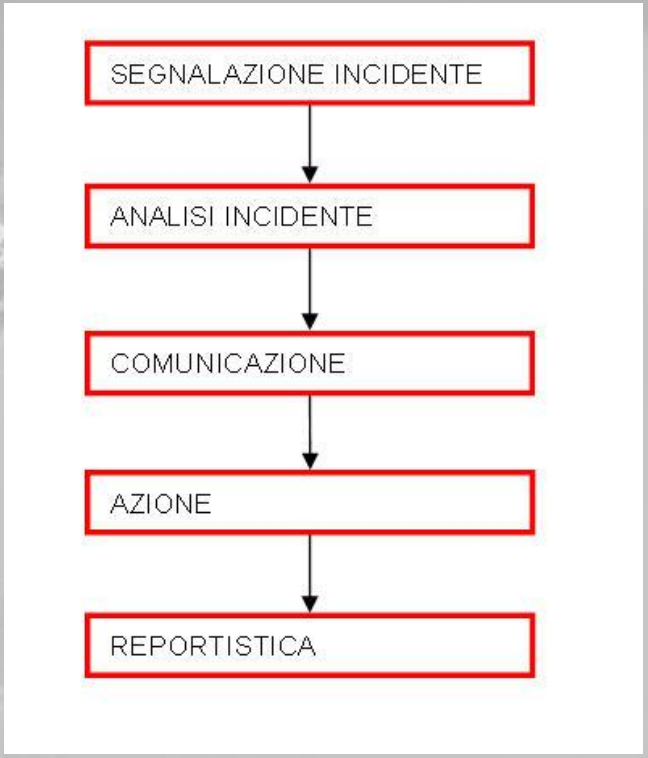
La gestione della sicurezza è il giusto
COMPROMESSO TRA

- complessità dello scenario,
- costi economici
- risorse umane

E

- probabilità di riuscita di un attacco verso una delle componenti della infrastruttura
- scopi della gestione e raccolta stessa.

Le fasi di gestione di un incidente



Gestione della Sicurezza: Cosa FARE

Un processo di gestione efficiente della sicurezza presuppone tempestività nella fase di:

- Individuazione incidente
- azione per limitarne i danni causati.

Gestione della Sicurezza: Cosa FARE

- Dotarsi di strumenti e di un'infrastruttura di gestione centralizzata della sicurezza in grado di analizzare sia gli eventi di sicurezza che il comportamento degli hosts allo scopo di
  - individuare in automatico i possibili incidenti di sicurezza
  - Ridurre i falsi positivi
  - Supportare l'attività di analisi del SOC
- Attivazione di Meccanismi di integrazione tra i vari strumenti in modo da attivare il trattamento automatico per alcune tipologie di incidenti

Gestione della Sicurezza: Cosa FARE

- Migliorare il processo che governa la gestione degli incidenti e dunque migliorando l'organizzazione del lavoro del personale preposto al SOC.

- promuovere l'utilizzo costante e avanzato degli strumenti

Gestione della sicurezza

- Organizzazione del SOC: compiti e obiettivi;
- Definire le modalità di gestione dell'incidente e in particolare:
  - Linee guida per operatività ordinaria e non
  - Proto policies: contromisure in base alla gravità incidente, Modalità di gestione dei recidivi
  - comunicazione verso utente/referente e studio di possibili meccanismi di automazione
  - DB di registrazione degli incidenti di sicurezza gestiti e reportistica
  - Procedure per riammissione HOST

Gestione della Sicurezza: Cosa FARE

- Individuazione degli elementi facilitatori per l'operatività del SOC
- Individuazione degli indicatori per valutare la bontà del processo e adozione del sistema di valutazione;
- Affiancamento ai colleghi e monitoraggio dell'utilizzo delle nuove procedure
- Verifica dei risultati attraverso l'analisi dei dati, lo studio dei report statistici ed il confronto periodico con il SOC

Gestione della Sicurezza: compiti SOC

- Rilevazione incidenti e loro gestione;
- Tuning degli strumenti e verifica funzionamento (HW e SW)
- Redazione di reportistica
- messa in atto delle procedure e meccanismi per il rispetto del regolamento di Sicurezza, con particolare rilievo per la registrazione dei server/asset:
  - Scan periodici
  - Meccanismi sinergici con NOC: DNS, DHCP, cambio indirizzamento
- funzione di prevenzione e allerta dei possibili problemi di sicurezza: diffusione di informazioni sulle vulnerabilità o le tipologie di attacchi più comuni e/o recenti e linee guida sulle strategie di difesa
- fornire e promuovere best practises in materia di sicurezza
- sensibilizzazione e formazione dell'utenza o dei referenti locali

Gestione della Sicurezza: Obiettivi del SOC

- Aumento del numero di incidenti individuati e gestiti dal SOC (automatico, manuale, analisi)
- Riduzione del numero di incidenti segnalati dall'esterno
- Riduzione dei tempi tra la segnalazione e intervento
  - Riduzione dei possibili danni
- Riduzione delle compromissioni dall'esterno
- In generale aumento del livello di sicurezza della rete e degli host

Gestione della Sicurezza: Linee guida operative

- Cadenza giornaliera:
  - gestione degli incidenti di sicurezza segnalati:
    - da fonti esterne;
    - Gestione incidenti segnalati da tool di alert automatico
    - Consultazione offese, eventi e flussi
  - Tuning strumenti:
    - Configurazione eventuali signatures, regole per individuazione automatica di traffico anomalo
    - alert automatici

Gestione della Sicurezza: Linee guida operative

- Riduzione falsi positivi
- Verifica funzionamento strumenti

Cadenza Periodica

- Verifica funzionamento di script custom per integrazione
- Scan di sottoreti
- Aggiornamenti strumenti (configurazione di alert)
- Report

Gestione della Sicurezza: Proto -policies

- Definizioni di classi di incidente (molto grave, gravi, medi, bassi)
- Associazione tipi di incidente a gravità es:
  - molto grave: attacchi DOS-DDOS, rilevanza penale, compromissioni, spam
  - Gravi: attacchi, port scan
  - Medi: malconfigurazioni, open relay etc, server non registrato
  - Bassa: malconfigurazione host
- Azioni differenziate:
  - base gravità, esistenza referente, tipologia di HOST
  - Tipo di intervento (chiusura, contenimento, alert e delega di azione)
  - Tempi di risposta minimi
  - Gestione di recidivi e riammissione

Gestione della Sicurezza: es. Proto -policies

- Se incidente molto grave, coinvolge server ed esiste referente
  - Richiesta al referente di messa in sicurezza host entro 3 ore altrimenti
  - Isolamento host ad opera SOC nel punto più vicino
- Se molto grave ma riguarda client
  - Richiesta isolamento entro 1 ora se referente
  - Chiusura immediata se non referente

INDICATORI DI QUALITA' DEL PROCESSO

- Percentuale di incidenti rilevati direttamente/attivamente rispetto altre fonti:
  - via analisi diretta degli strumenti di sicurezza d'Ateneo
  - Via altri strumenti (scansioni di sottoreti su servizi sospetti o su servizi non registrati
  - via tool di allarmistica degli strumenti automatici;
- Percentuale di incidenti gestiti automaticamente
- Numero medio di incidenti gestiti al giorno
- Tempi intercorso:
  - tra individuazione e azione
  - tra individuazione e risoluzione
- Numero di incidenti causati da ciascun Recidivo
- Numero di sottoreti analizzate
- Numero di offese sul console gestione contemporaneamente attive in media al giorno;
- Numero di interventi di tuning sugli strumenti automatici

Esempio di Infrastruttura

Infrastruttura di monitoraggio e raccolta di Dati relativi alla sicurezza provenienti da diverse fonti

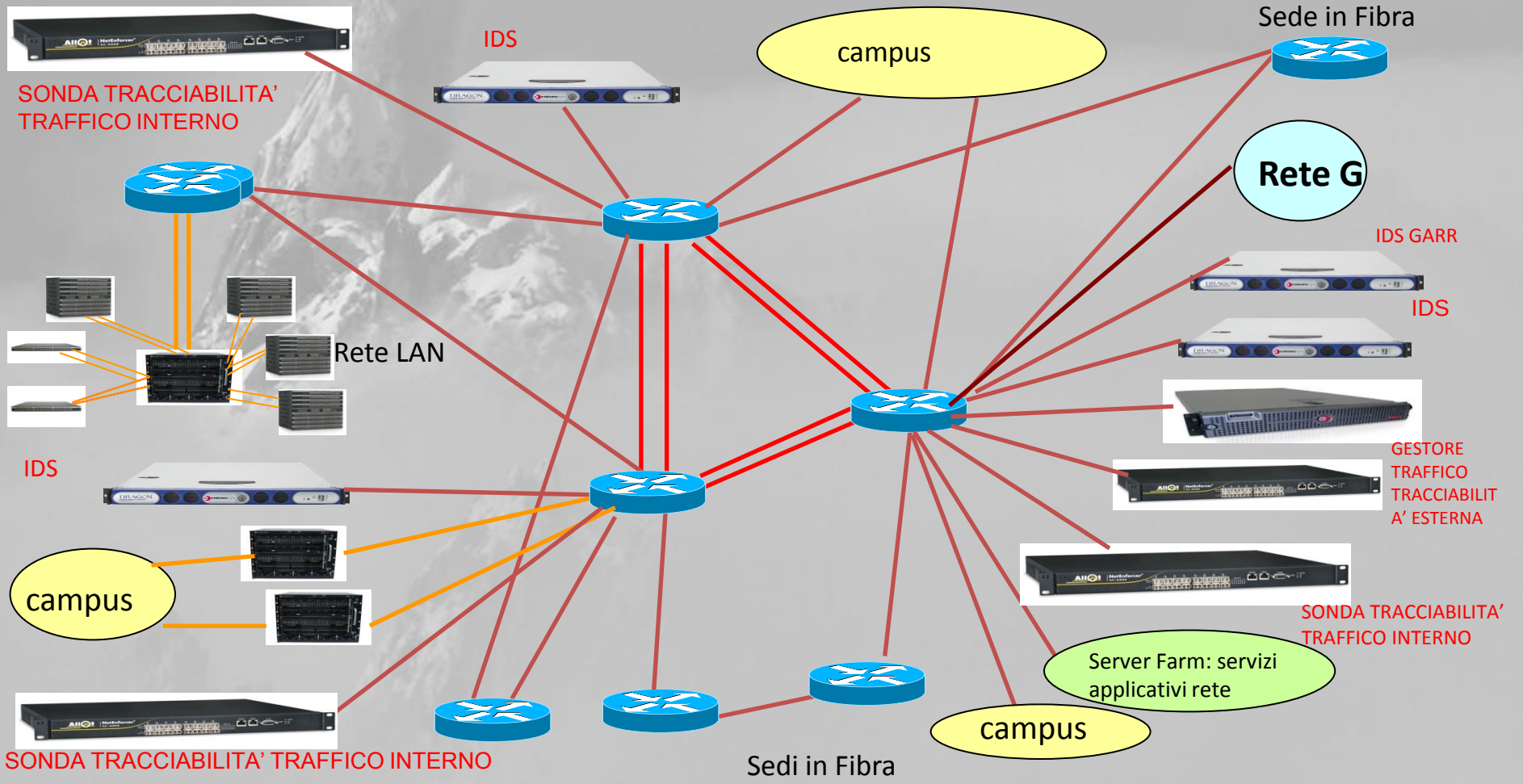
Ha lo scopo di:

- individuare tempestivamente gli incidenti informatici attraverso sofisticate metodologie di detection e blocco automatico per alcuni di essi (limitare l'impatto all'esterno)
- Eventuali indagini interne
- Fornire le opportune risposte in caso di richiesta dell'AG

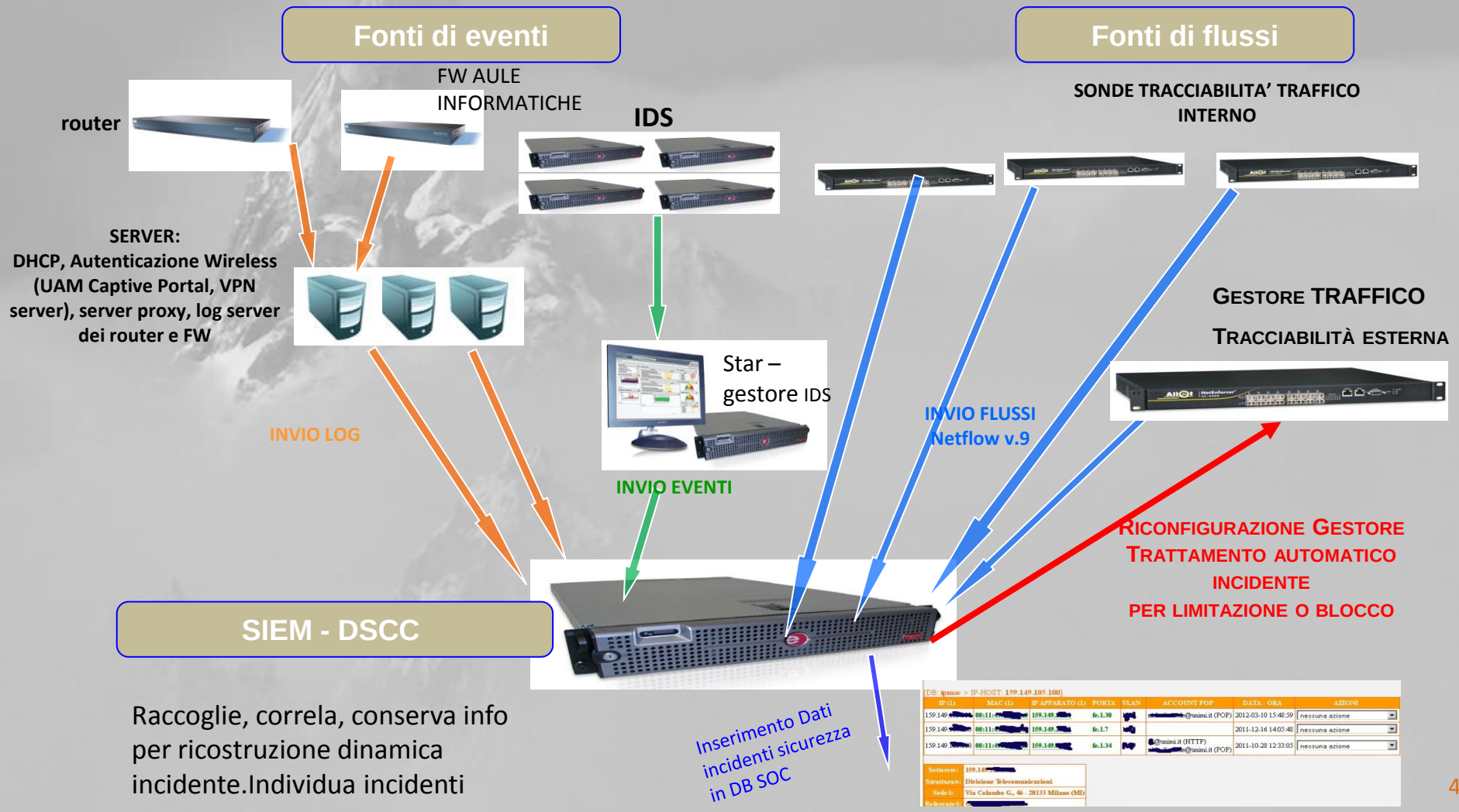
Correla, normalizza e prioritizza le informazioni provenienti da più punti di osservazione al fine di ricostruire la dinamica dell'incidente/illecito

- Eventi di sicurezza IDS distribuiti in rete (analizzano tutto il traffico su rete geografica)
- Log server (DHCP, DNS, ..), log dei firewall e router,
- Analisi comportamentale degli host attraverso l'analisi traffico
  - Traffico backbone rete e server farm (Netflow v. 9)
  - Traffico IN/OUT verso la rete esterna GARR (netflow v.9)

Schema esemplificativo infrastruttura Sicurezza e Gestione di Traffico



Architettura SIEM (Console di Sicurezza) d'Ateneo + Gestore Banda



Raccoglie, correla, conserva info per ricostruzione dinamica incidente.Individua incidenti

Segnalazione Incidente 1/2

Esempio di notifica di incidente:

Offense 359

Magnitude	[redacted]		Relevance	4	Severity	5	Credibility	3
Description	Multiple Login Failures for the Same User preceded by Multiple Login Failures from the Same Source	Offense Type	Source IP					
		Event/Flow count	439 events and 5073 flows in 4 categories					
Source IP(s)	187.141.[redacted]	Start	2012-03-13 15:11:08					
Destination IP(s)	Local (2132)	Duration	38m 49s					
Network(s)	Multiple (102)	Assigned to	Not assigned					

Offense Source Summary

IP	187.141.231.140	Location	Mexico
Magnitude		Vulnerabilities	0
User	root	MAC	Unknown
Host Name	customer-187-141-231-140-sta.uninet-ide.com.mx.		
Asset Name	Unknown	Asset Weight	0
Offenses	2	Events/Flows	5520

Last 5 Notes

Notes	User Name	Create Date

No results were returned.

Top 5 Source IPs

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
187.14[redacted]		Mexico	Unknown	root	Unknown	0	2	2132	2d 36m 19s	5520

Top 5 Destination IPs

Destination IP	Magnitude	Location	Vulnerability	Chained	User	MAC	Weight	Offenses	Source(s)	Last Event/Flow	Events/Flows
159.[redacted]		ScienzeDellaInformazione[redacted]	Unknown	No	Unknown	Unknown	0	8	8	1h 53m 11s	16
159.[redacted]		[redacted]	Unknown	No	Unknown	:c6:c0:36:6c	0	9	31	15m 25s	68
159.[redacted]		[redacted]Ospedale[redacted]	Unknown	No	Unknown	:4d:a1:d8:b9	0	8	8	2h 28m 53s	15
159.[redacted]		[redacted]	Unknown	No	Unknown	:7e:f0:fc:2b	0	11	29	1h 54m 21s	37
159.[redacted]		[redacted]MedicinaLavoro	Unknown	No	Unknown	:e3:38:8e:d6	0	10	10	11h 45m 57s	91

Segnalazione Incidente 2/2

Top 5 Log Sources

Name	Description	Group	Events/Flows	Offenses	Total Events/Flows
IOS @ 159.	IOS device		332	5	3681
IOS @ 159.	IOS device		99	5	3254
Custom Rule Engine-8 :: dscc-unimi	Custom Rule Engine		8	524	5409

Top 5 Users

Name	Events/Flows	Offenses	Total Events/Flows
root	316	4	5800
bin	7	3	205
www	6	2	55
oracle	6	3	105
mircte	4	2	53

Top 5 Categories

Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow		
Misc Login Failed		2	4	03-13 15:14:45	03-13 15:47:52		
User Login Failure		2	4	03-13 15:14:43	03-13 15:37:19		
SSH Login Failed		2	431	03-13 15:14:33	03-13 15:49:52		
Remote Access		2132	5073	03-13 15:11:45	03-13 15:40:17		

Top 10 Events

Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:48:27
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:48:13
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:48:20
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:47:59
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:49:52
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:49:47
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:49:28
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:49:38
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:49:11
%SSH-5-SSH2_USERAUTHfailed		IOS @ 159.149	SSH Login Failed	159.	0	03-13 15:48:57

Top 10 Flows

Application	Source IP	Source Port	Destination IP	Destination Port	Total Bytes	Last Packet Time
RemoteAccess.SSH_TCP_Allot	187.141	40281	159.	22	2	2012-03-13 15:40:45
RemoteAccess.SSH_TCP_Allot	187.141	35964	159.	22	2	2012-03-13 15:40:17
RemoteAccess.SSH_TCP_Allot	187.141	39447	159.	22	2	2012-03-13 15:40:17
RemoteAccess.SSH_TCP_Allot	187.141	36115	159.	22	2	2012-03-13 15:40:17

Dettaglio Flusso

Esempio dettaglio flusso sospetto connesso all'incidente con annesso l'elenco delle regole che si son verificate e che hanno partecipato allo scatenarsi della segnalazione dell'incidente

Esempio di flusso sospetto, correlato all'incidente

Flow Information

Protocol:	tcp_ip	**Application:**	RemoteAccess.SSH_TCP_Allot				
Magnitude:	(8)	**Relevance:**	10	**Severity:**	5	**Credibility:**	10
First Packet Time:	2012-01-23 23:36:45	**Last Packet Time:**	2012-01-24 00:36:15	**Storage Time:**	2012-03-13 15:40:45		
Event Name:	Terminals___SSH_TCP						
Low Level Category:	Remote Access						
Event Description:	Application detected with Signature						
allot_group (custom):	Terminals						
allot_application (custom):	SSH						

Source and Destination Information

Source IP:	187.141	**Destination IP:**	159.
Source Asset Name:	N/A	**Destination Asset Name:**	N/A
IPv6 Source:	0:0:0:0:0:0:0:0	**IPv6 Destination:**	0:0:0:0:0:0:0:0
Source Port:	40281	**Destination Port:**	22
Source Flags:	S,Illegal8	**Destination Flags:**	P,U,Illegal8
Source QoS:	Best Effort	**Destination QoS:**	Best Effort
Source ASN:	0	**Destination ASN:**	0
Source If Index:	0	**Destination If Index:**	0
Source Payload:	0 packets, 1 bytes	**Destination Payload:**	0 packets, 1 bytes

Source Payload
Destination Payload

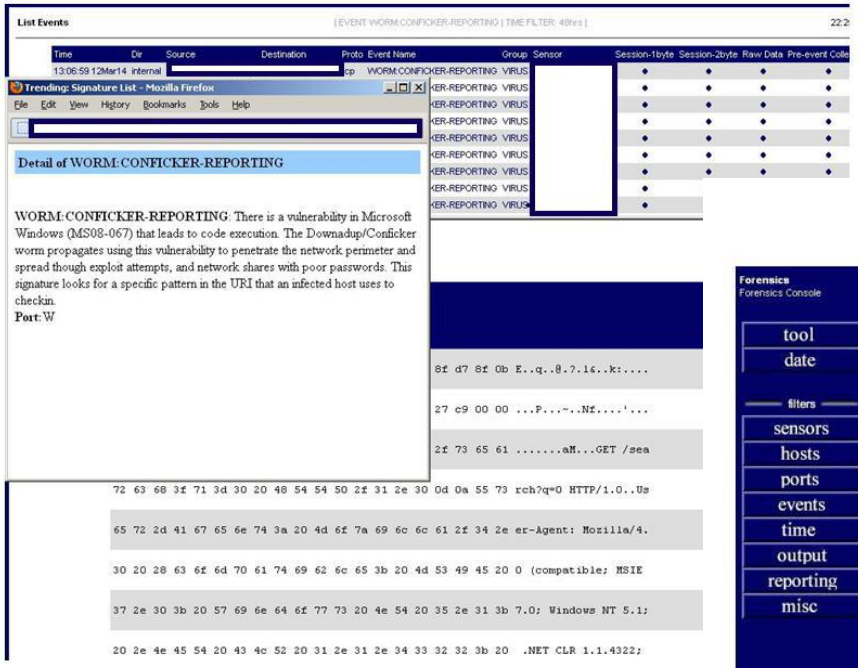
utf | hex | base64
Wrap Text
FLOWS=1;IP_PROTOCOL_VERSION=4;Vendor65=SSH.Terminals;

utf | hex | base64
Wrap Text

Additional Information

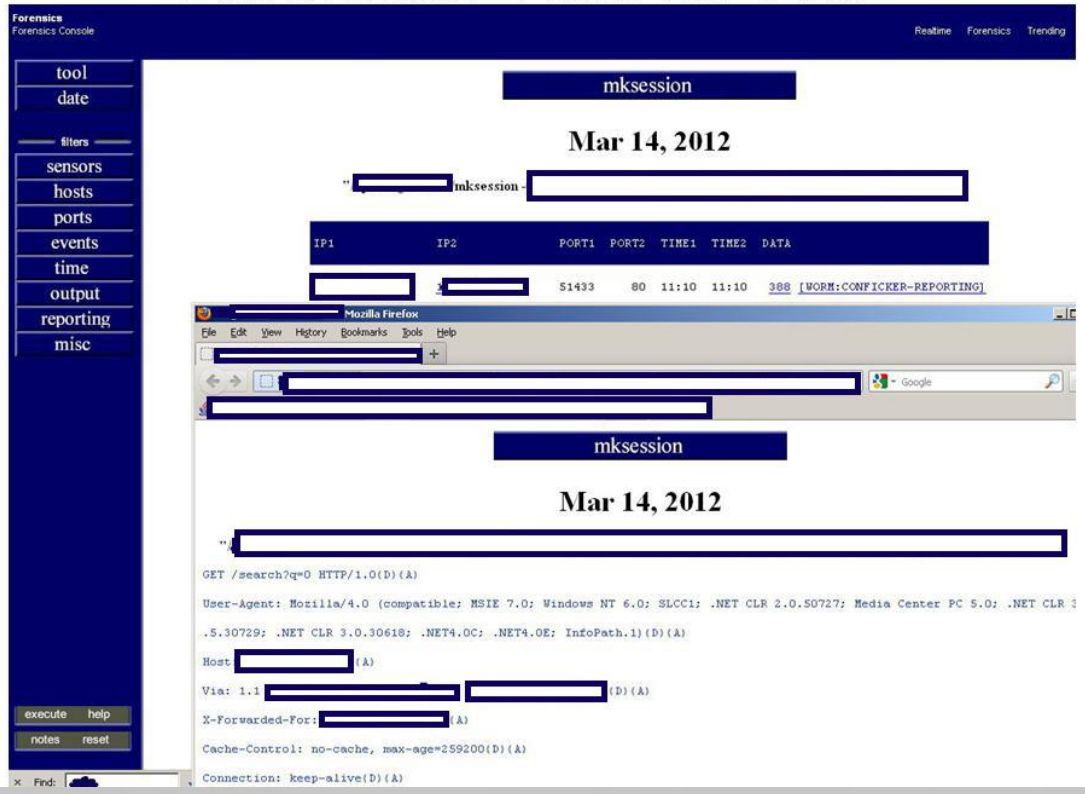
Flow Type:	Standard Flow	**Flow Source/Interface:**	
Flow Direction:	R2L		
Custom Rules:	BB:PortDefinition: SSH Ports BB:CategoryDefinition: Any Flow Magnitude Adjustment: Destination Network Weight is Low Recon: Remote SSH Server Scanner Unimi Magnitude Adjustment: Destination Asset Exists Magnitude Adjustment: Source Network Weight is Low Magnitude Adjustment: Context is Remote to Local BB:NetworkDefinition: Client Networks BB:PortDefinition: Authorized L2R Ports BB:NetworkDefinition: Inbound Communication from Internet to Local Host BB:NetworkDefinition: Untrusted Network Segment		
Custom Rules Partial Matched :	System: Flow Source Stopped Sending Flows		
Annotations:	Relevance has been decreased by 2 because the destination network weight is low. Relevance has been increased by 8 because the destination asset exists. Relevance has been decreased by 2 because the source network weight is low. Relevance has been increased by 2 because the context is Remote to Local.		

Eventi catturati da IDS



Per gli eventi IDS è possibile consultarne i dettagli attraverso la console di visualizzazione del sistema IDS

Forensics Tool su IDS



COSA E' STATO FATTO: SICUREZZA E MONITORAGGIO DEL TRAFFICO

- Sistema centrale di gestione della sicurezza (SIEM)
- Sistema di Monitoraggio (tracciabilità) del traffico interno ed esterno:
- Integrazione ad hoc dei due strumenti per realizzare:

  - VISIBILITA' per la SIEM del traffico classificato a LIVELLO 7 da Gestore di Banda e possibilità di effettuare analisi comportamentale granulare e regole ad hoc per individuazione degli incidenti sulla SIEM;
  - Blocco automatico degli IP interni "infetti" e dei tentativi di compromissione di IP esterni (es SSH SCAN) sul gestore di traffico verso esterno sulla base delle segnalazioni SIEM
  - Gestione automatica di politiche di traffico (limitazione o blocco) per determinate tipologie di Traffico (es P2P) o particolarmente stringenti per host che si comportano come server P2P.

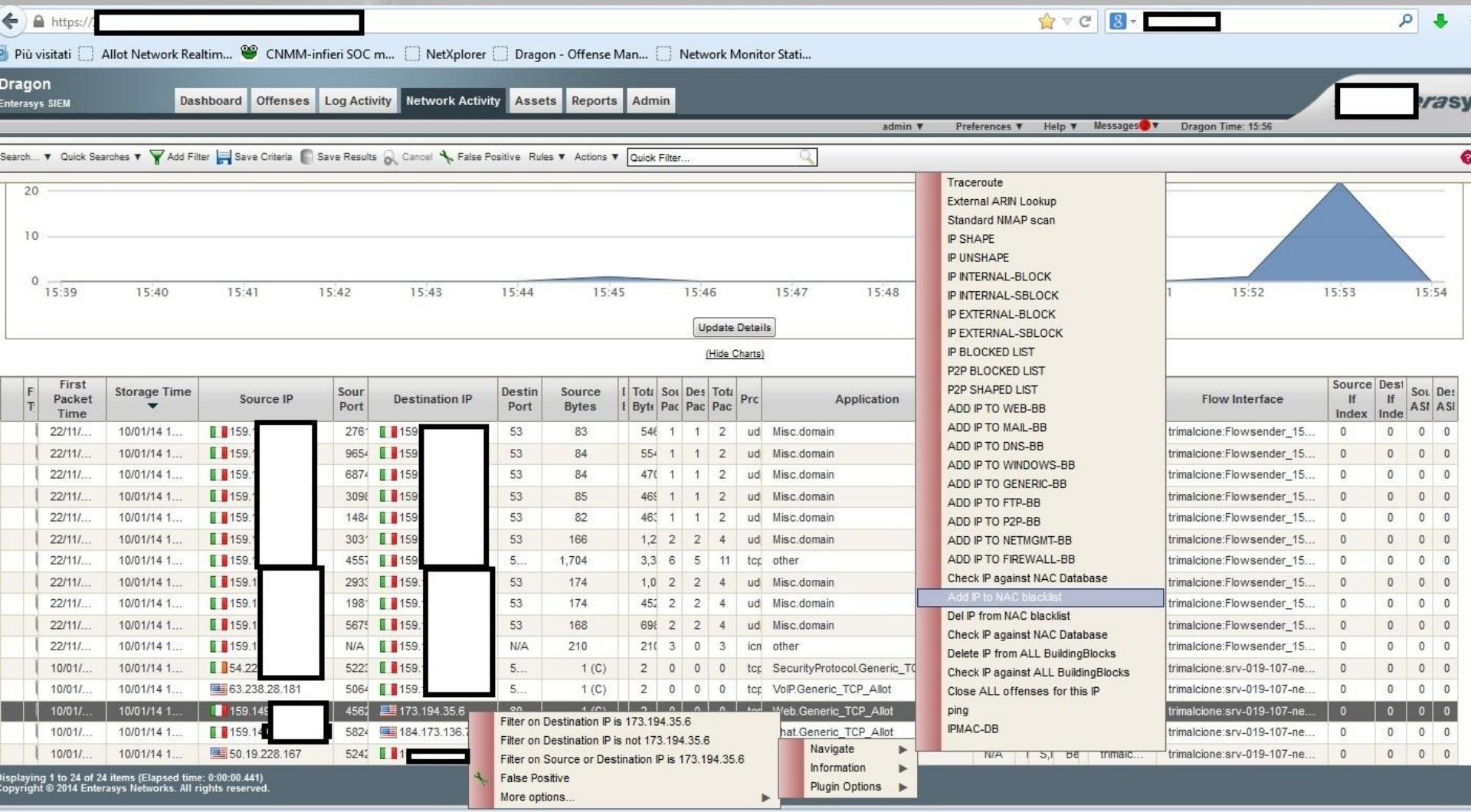
OTTIMIZZAZIONI

- Per ridurre le ore uomo richieste all'operatore nella gestione SIEM e per garantire l'allineamento delle configurazioni si è proceduto a:
  - Automatizzare le attività procedurali (es Aggiornamento automatico degli IP dei router, firewall, server registrati x ridurre i falsi positivi; aggiornamento sottoreti-strutture, cancellazione delle offese più vecchie di una certa data)
  - Predisporre degli script per l'esecuzione in modo immediato e semplice, adatto anche a personale non esperto, di azioni su determinati host (es. azioni di blocco o di limitazione, check server). Predisposizione per l'attivazione automatica di tali azioni con valenza temporale.
  - Potenziamento dell'allarmistica per l'invio automatico di segnalazioni relative a possibili incidenti
  - Automatizzazione del trattamento automatico di determinati tipi di offese (Tentativi di compromissione, Conficker e altri tipi di worm) con successiva cancellazione delle stesse

OTTIMIZZAZIONI SIEM –GESTORE BANDA

- Customizzazione della SIEM: corrispondenza tra classi di applicazioni
  - Migliorata detection
  - Visibilità tipo di traffico per SOC
  - Possibilità di scrivere regole e scatenare eventi offesa su base applicazione
- Realizzazione di 4 plugin richiamabili dall'operatore mediante tasto dx del mouse che dato l'IP effettuano:
  - Riduzione della banda in entrata ed uscita sul link di frontiera (-SHAPE)
  - Blocco totale del traffico relativo all'IP sul link di frontiera (BLOCK)
  - Sblocco della politica di shaping (UNSHAPE)
  - Riammissione del traffico sul link di frontiera (BLOCK)
  - Lista di IP bloccati interni ed esterni
- Contenimento traffico alla sola rete interna: consente di non propagare danni ad esterno e a host di aggiornarsi con AV e S.O.;
- Il plugin rende non necessario l'accesso dell'operatore al gestore di banda
- Scrittura di SCRIPT x riconfigurazione GESTORE per alcune tipologie di traffico

PLUGIN

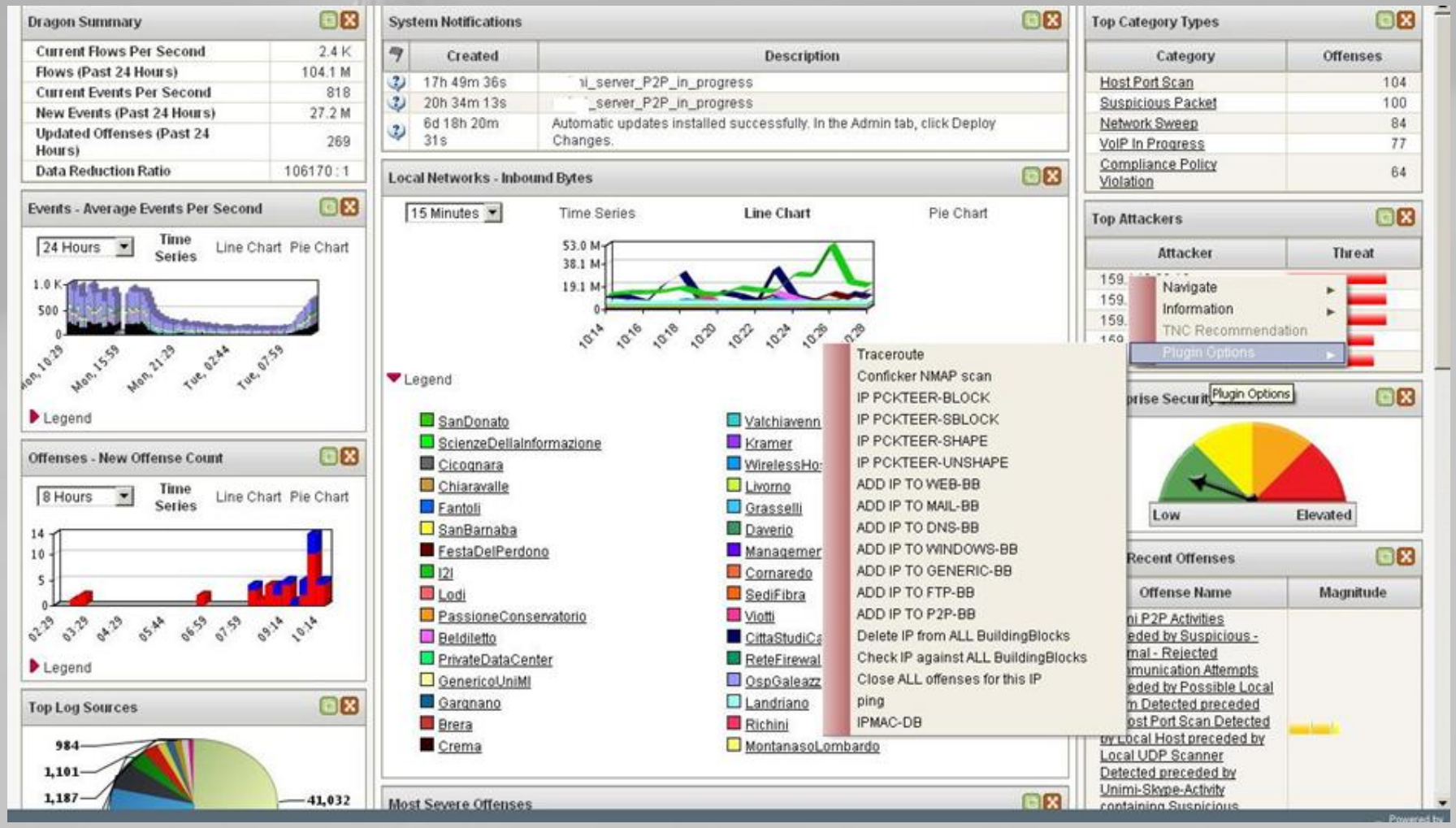

Più visitati
Allot Network Realtim...
CNMM-infieri SOC m...
NetXplorer
Dragon - Offense Man...
Network Monitor Stati...
Dragon
Enterasys SIEM
Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
Admin
admin
Preferences
Help
Messages
Dragon Time: 15:56
Search...
Quick Searches
Add Filter
Save Criteria
Save Results
Cancel
False Positive
Rules
Actions
Quick Filter...
Update Details
(Hide Charts)
Traceroute
External ARIN Lookup
Standard NMAP scan
IP SHAPE
IP UNSHAPE
IP INTERNAL-BLOCK
IP INTERNAL-SBLOCK
IP EXTERNAL-BLOCK
IP EXTERNAL-SBLOCK
IP BLOCKED LIST
P2P BLOCKED LIST
P2P SHAPED LIST
ADD IP TO WEB-BB
ADD IP TO MAIL-BB
ADD IP TO DNS-BB
ADD IP TO WINDOWS-BB
ADD IP TO GENERIC-BB
ADD IP TO FTP-BB
ADD IP TO P2P-BB
ADD IP TO NETMGMT-BB
ADD IP TO FIREWALL-BB
Check IP against NAC Database
Add IP to NAC blacklist
Del IP from NAC blacklist
Check IP against NAC Database
Delete IP from ALL BuildingBlocks
Check IP against ALL BuildingBlocks
Close ALL offenses for this IP
ping
IPMAC-DB
Filter on Destination IP is 173.194.35.6
Filter on Destination IP is not 173.194.35.6
Filter on Source or Destination IP is 173.194.35.6
False Positive
More options...
Navigate
Information
Plugin Options
Displaying 1 to 24 of 24 items (Elapsed time: 0:00:00.441)
Copyright © 2014 Enterasys Networks. All rights reserved.

Integrazione con DB server registrati

- script:
  - per allineamento server registrati con ASSET in SIEM
  - riconfigura in modo appropriato i BB a seconda dei servizi registrati
- Riduzione Falsi positivi
- Regole ad hoc per servizi
- Regole per individuazione di UNAUTHORIZED SERVER
- Esclusione di azioni automatiche per i server registrati
- script richiamabili in modalità right click che consentono al SOC di aggiungere/modificare/cancellare un IP dal Building Block specifico per i principali servizi di rete direttamente dalla dashboard: + semplicità

  - ADD IP TO WEB-BB (aggiunge l'IP specificato al servizio Web)
  - ADD IP TO MAIL-BB , ADD IP TO DNS-BB, ADD IP TO WINDOWS-BB, ADD IP TO GENERIC-BB
  - ADD IP TO FTP-BB, ADD IP TO P2P-BB, DELETE IP FROM ALL Building Block, CHECK IP FROM ALL Building Block
  - CLOSE ALL OFFENSES FOR THIS IP

Es. plugin


Dragon Summary
Current Flows Per Second 2.4 K
Flows (Past 24 Hours) 104.1 M
Current Events Per Second 818
New Events (Past 24 Hours) 27.2 M
Updated Offenses (Past 24 Hours) 269
Data Reduction Ratio 106170 : 1
Events - Average Events Per Second
24 Hours
Time Series
Line Chart
Pie Chart
Legend
Offenses - New Offense Count
8 Hours
Top Log Sources
984
1,101
1,187
41,032
System Notifications
Created
Description
17h 49m 36s
20h 34m 13s
6d 18h 20m 31s
Automatic updates installed successfully. In the Admin tab, click Deploy Changes.
Local Networks - Inbound Bytes
15 Minutes
Time Series
Line Chart
Pie Chart
53.0 M
38.1 M
19.1 M
Legend
SanDonato
ScienzeDellaInformazione
Cicognara
Chiaravalle
Fantoli
SanBarnaba
FestaDelPerdono
I2I
Lodi
PassioneConservatorio
Beldiletto
PrivateDataCenter
GenericoUniMI
Gargnano
Brera
Crema
Valchiavenn
Kramer
Livorno
Grasselli
Daverio
Comaredo
SediFibra
Viotti
Landriano
Richini
MontanasoLombardo
Traceroute
Conficker NMAP scan
IP PCKTEER-BLOCK
IP PCKTEER-SBLOCK
IP PCKTEER-SHAPE
IP PCKTEER-UNSHAPE
ADD IP TO WEB-BB
ADD IP TO MAIL-BB
ADD IP TO DNS-BB
ADD IP TO WINDOWS-BB
ADD IP TO GENERIC-BB
ADD IP TO FTP-BB
ADD IP TO P2P-BB
Delete IP from ALL BuildingBlocks
Check IP against ALL BuildingBlocks
Close ALL offenses for this IP
ping
IPMAC-DB
Most Severe Offenses
Top Category Types
Category
Offenses
Host Port Scan 104
Suspicious Packet 100
Network Sweep 84
VoIP In Progress 77
Compliance Policy Violation 64
Top Attackers
Attacker
Threat
Navigate
Information
TNC Recommendation
Plugin Options
Plugin Options
Low
Elevated
Recent Offenses
Offense Name
Magnitude
Local UDP Scanner Detected preceded by Unimi-Skype-Activity

ASSET SIEM- SERVER REGISTRAZIONE

Id	IP Address	Asset Name	Risk Score	Vulnerabilities	
51778	159....	ad1	0.0	0	7
51777	159....	data...	0.0	0	1
88389	159....	DC-I...	0.0	0	0
88388	159....	VDC...	0.0	0	0
51776	159....	nov...	0.0	0	15
51775	159....	BIBL...	0.0	0	0
51774	159....	man...	0.0	0	100
51773	159....	UNI...	0.0	0	0
51772	159....	Malli...	0.0	0	1
51771	159....	eolo2	0.0	0	0
51770	159....	DISC	0.0	0	0
51769	159....	GIS...	0.0	0	1
51768	159....	SER...	0.0	0	1
51767	159....	serv...	0.0	0	1
51766	159....	serv...	0.0	0	0
51765	159....	san...	0.0	0	0
51764	159....	ana...	0.0	0	1
51763	159....	man...	0.0	0	0
51762	159....	hon...	0.0	0	0
51761	159....	hon...	0.0	0	0
51760	159....	hon...	0.0	0	0
51759	159....	hon...	0.0	0	3
51758	159....	hon...	0.0	0	0
51757	159....	hon...	0.0	0	1
51756	159....	hon...	0.0	0	0
51755	159....	hon...	0.0	0	0
51754	159....	hon...	0.0	0	0
51753	159....	arel-...	0.0	0	1

Individuazione server non registrati

Block Name	Group	Rule Category	Block Type	Event/Flow Count	...	Origin	Creation Date	Modification Date
BB[redacted] Unauthorized WEB Server	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 17:24	27/mag/2014 16:38
BB[redacted] Unauthorized MAIL Server	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 16:57	27/mag/2014 16:38
BB[redacted] Unauthorized LDAP Server	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 16:54	27/mag/2014 16:38
BB[redacted] Unauthorized FTP Server	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 16:48	27/mag/2014 16:38
BB[redacted] Unauthorized DNS Server	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 16:07	27/mag/2014 16:38
BB[redacted] Unauthorized DB Server	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 17:07	27/mag/2014 16:38
BB[redacted] Unauthorized WEB Server False Positive	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 18:04	17/apr/2014 18:12
BB[redacted] Unauthorized MAIL Server False Positive	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 18:02	17/apr/2014 18:11
BB[redacted] Unauthorized LDAP Server False Positive	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 18:01	17/apr/2014 18:10
BB[redacted] Unauthorized FTP Server False Positive	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 17:59	17/apr/2014 18:09
BB[redacted] Unauthorized DNS Server False Positive	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 17:58	17/apr/2014 18:07
BB[redacted] Unauthorized DHCP Server False Positive	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 17:57	17/apr/2014 18:06
BB[redacted] Unauthorized DB Server False Positive	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 17:55	17/apr/2014 18:05
BB[redacted] Unauthorized DHCP Server	Host Definitions	Custom Rule	COMMON	0	0	User	17/apr/2014 15:59	17/apr/2014 17:35
BB:HostDefinition: Web Servers	Host Definitions	Custom Rule	COMMON	0	0	Modified	29/giu/2011 13:24	16/apr/2014 12:01
BB:HostDefinition: FTP Servers	Host Definitions	Custom Rule	COMMON	0	0	Modified	29/giu/2011 13:24	01/apr/2014 13:35
BB:HostDefinition: Mail Servers	Host Definitions	Custom Rule	COMMON	0	0	Modified	29/giu/2011 13:22	01/apr/2014 13:25

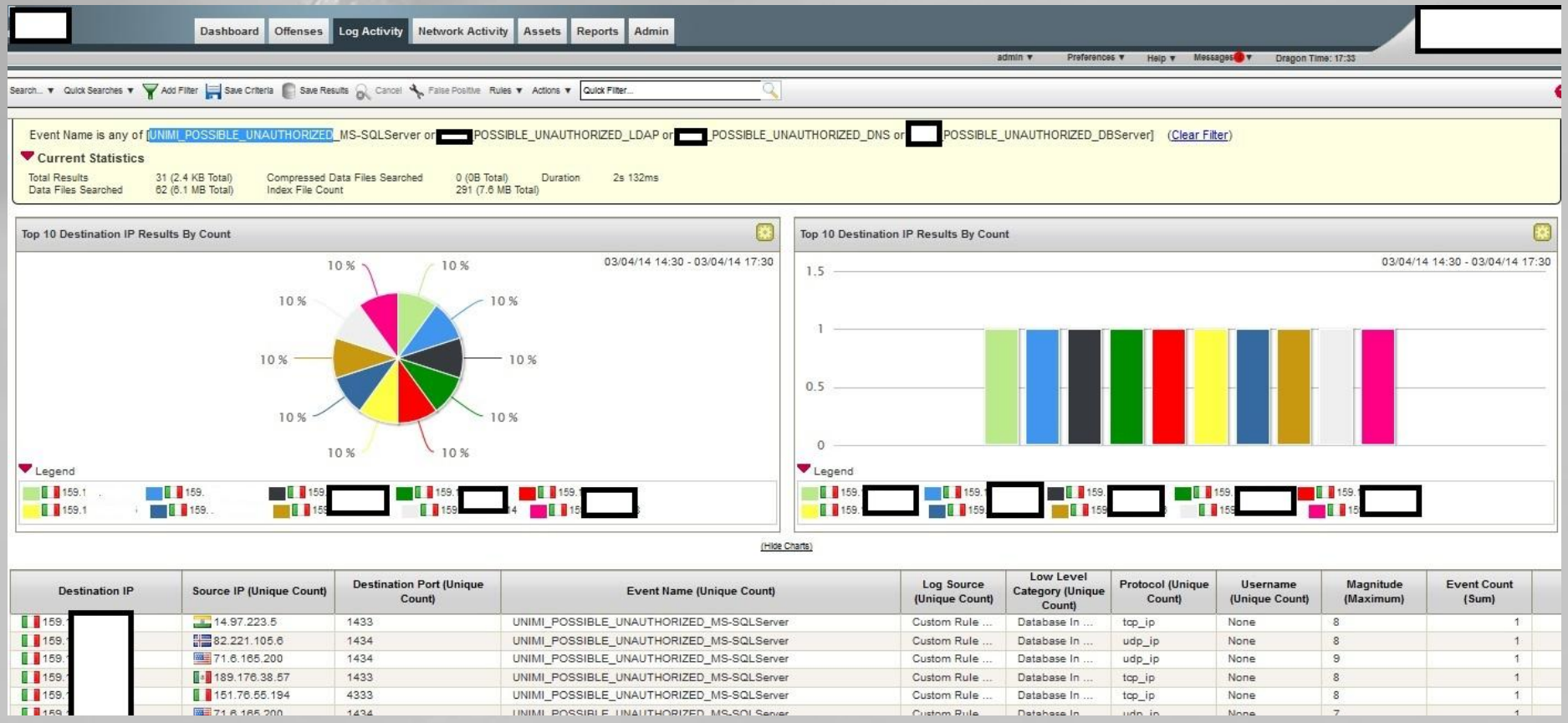
Rule

Apply BB:HostDefinition: FTP Servers on events or flows which are detected by the Local system
and when a flow or an event matches any of the following BB:PortDefinition: FTP Ports
and when the destination IP is one of the following 127.0.0.2, 159.[redacted]
159.
159.
159.
159.

Notes

Edit this BB to define typical FTP servers. This BB is used in conjunction with the BB:False Positive: FTP Server False Positives Categories and BB:FalsePositve: FTP Server False Positive Events building blocks.

Unauthorized Server



Destination IP	Source IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)
159.[redacted]	14.97.223.5	1433	UNIMI_POSSIBLE_UNAUTHORIZED_MS-SQLServer	Custom Rule ...	Database In ...	tcp_ip	None	8	1
159.[redacted]	82.221.105.6	1434	UNIMI_POSSIBLE_UNAUTHORIZED_MS-SQLServer	Custom Rule ...	Database In ...	udp_ip	None	8	1
159.[redacted]	71.6.165.200	1434	UNIMI_POSSIBLE_UNAUTHORIZED_MS-SQLServer	Custom Rule ...	Database In ...	udp_ip	None	9	1
159.[redacted]	189.176.38.57	1433	UNIMI_POSSIBLE_UNAUTHORIZED_MS-SQLServer	Custom Rule ...	Database In ...	tcp_ip	None	8	1
159.[redacted]	151.76.55.194	4333	UNIMI_POSSIBLE_UNAUTHORIZED_MS-SQLServer	Custom Rule ...	Database In ...	tcp_ip	None	8	1
159.[redacted]	71.6.165.200	1434	UNIMI_POSSIBLE_UNAUTHORIZED_MS-SQLServer	Custom Rule ...	Database In ...	udp_ip	None	7	1

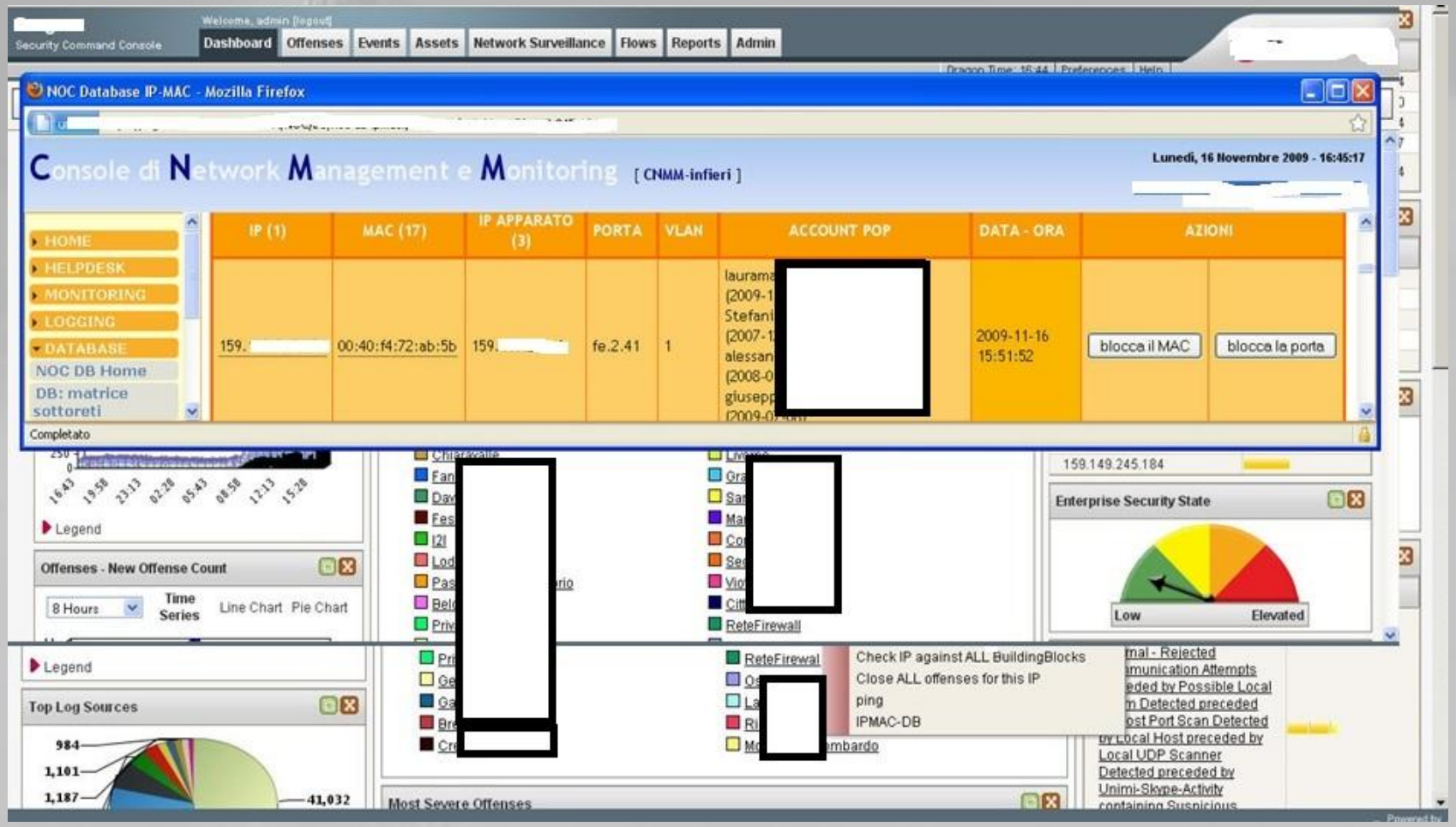
OTTIMIZZAZIONI SIEM –CONSOLE NOC

- Integrazione realizzata tramite plugin attivabile dal tasto dx da parte dell'operatore DSCC che sull'IP selezionato effettua una query sul DB IPMAC ottenendo le seguenti info:

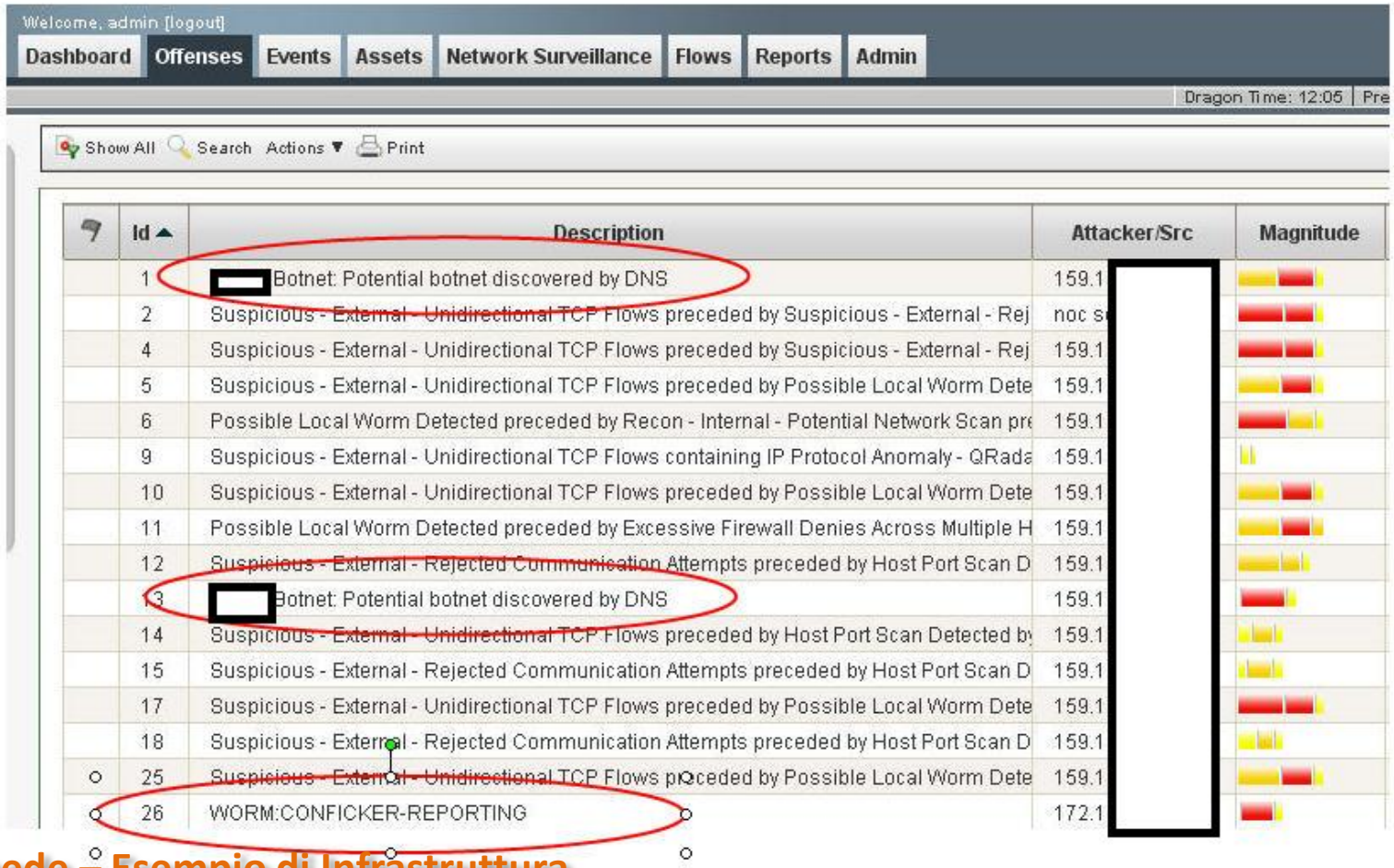
  Ip, MAC, ip apparato, porta, vlan, account pop su cui si può agire bloccando l'Ip o il Mac address sull'apparato più vicino.

- Inserimento/aggiornamento automatico di Tutti ip dei router d'Ateneo tratti dalla console di MGMT nel relativo BB del DSCC → riduzione dei falsi positivi: cadenza settimanale
- Script di integrazione tra Network Hierarchy SIEM sulla base di Console di gestione del piano di indirizzamento

OTTIMIZZAZIONI SIEM –CONSOLE NOC



Realizzazione di meccanismi per la creazione di offese customizzate contenenti la "diagnosi"



GESTIONE AUTOMATICA

- Individuazione di classi di incidenti critici
- Analisi, scrittura regole «affidabili» per individuazione automatica, tuning
- Generazione Offesa contenente «diagnosi»
- Check per escludere IP SERVER; firewall, router,..
- Definizione delle azioni da intraprendere in automatico differenziate sulla base di incidente
- Riconfigurazione sistema di gestione traffico
- Scrittura in apposito BB
- Scrittura in DB gestione degli incidenti
- Chiusura offesa
- Eventuale svuotamento liste IP
- Mail giornaliera contenente la lista di azioni automatiche intraprese
- Es. tipi di incidenti trattati: Ip interni affetti da alcuni tipi di worm, tentativi di compromissione da esterno, server p2p, attacchi DDOS su DNS, ..

Es. offesa trattata:

All Offenses > Offense 197 (Summary)

Offense 197

Summary Display ▼ Events Flows Actions ▼ Print

Magnitude		Status		Relevance	7	Severity	4	Credibility	4
Description	Remote Intrusion Attempt	Offense Type	Source IP						
		Event/Flow count	1,327 events and 726 flows in 5 categories						
Source IP(s)	58.83.146.252	Start	28/mag/2014 19:41:07						
Destination IP(s)	Local (853) Remote (178)	Duration	5d 15h 35s						
Network(s)	Multiple (57)	Assigned to	Unassigned						

Offense Source Summary

IP	58.83.146.252	Location	China
Magnitude		Vulnerabilities	0
User	Unknown	MAC	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	1	Events/Flows	2.053

Last 5 Notes

Notes Add Note

Notes	Username	Creation Date

No results were returned.

Top 5 Source IPs

Sources

Source IP	Magn...	Location	Vuln...	User	MAC	Weight	Offen...	Destination...	Last Event/Flow	Events/Flows
58.83.146.252		China	No	Unknov	Unknown NIC	0	1	853	9h 11m 24s	2.053

Es. offesa trattata:

All Offenses > Offense 197 (Summary)

Top 5 Destination IPs

Destinations

Destination IP	Magnitude	Location	Vulnerability	Chained	User	MAC	Weight	Offenses	Source(s)	Last Event/Flow	Events/Flows
159. ...		DIPARTIMENTI.DIP_...	No	No	Unknown	Unknown NIC	0	7	10.023	25s	368.601
159. ...		DIPARTIMENTI.DIP_...	No	No	Unknown	Unknown NIC	0	7	10.010	25s	196.212
android-8...		SERVIZI.EduRoam	No	No	amanda.cruzsilva	84:DD:20:CB:6	0	5	10	1d 16h 31m 24s	17
159. ...		SOTTORETI_INFIER...	No	No	Unknown	Unknown NIC	0	8	12	13h 32m 3s	308
159. ...		SOTTORETI_INFIER...	No	No	Unknown	Unknown NIC	0	7	9	4h 47m 52s	53

Top 5 Log Sources

Log Sources

Name	Description	Group	Events/Flows	Offenses	Total Events/Flows
Custom Rule En...	Custom Rule Engine		1.233	1.096	1.418.839
NSeries @ 159....	NSeries device		47	21	3.566
IOS @ 159. ...	IOS device		24	3	388
K/N/S Series @...	K/N/S Series device		19	24	6.047
K/N/S Series @...	K/N/S Series device		3	20	5.445

Top 5 Users

Users

Name	Events/Flows	Offenses	Total Events/Flows
root	94	94	18753

Top 5 Categories

Categories

Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow		
SSH Login Failed		4	93	28/mag/2014 19...	28/mag/2014 19...		
User Login Failure		1	1	28/mag/2014 19...	28/mag/2014 19...		
Misc Recon Event		532	534	28/mag/2014 19...	03/giu/2014 10:...		
ACL Deny		521	699	28/mag/2014 19...	03/giu/2014 10:...		
Remote Access		544	726	28/mag/2014 19...	03/giu/2014 10:...		

Last 10 Events

Events

Event Name	Magnitude	Log Source	Category	Destina...	Dst Port	Time
Remote Intrusion Attempt		Custom Rule ...	Misc Recon Event	159....	22	03/giu/2014 10:40:02
Remote Intrusion Attempt		Custom Rule ...	Misc Recon Event	159....	22	03/giu/2014 10:40:01
Remote Intrusion Attempt		Custom Rule	Misc Recon Event	159	22	03/giu/2014 10:41:00

Es. offesa trattata:

All Offenses > Offense 197 (Summary)

ACL Deny	521	699	28/mag/2014 19...	03/giu/2014 10:...	
Remote Access	544	726	28/mag/2014 19...	03/giu/2014 10:...	

Last 10 Events Events

Event Name	Magnitude	Log Source	Category	Destina...	Dst Port	Time
Uni Remote Intrusion Attempt		Custom Rule ...	Misc Recon Event	159....	22	03/giu/2014 10:40:02
Unir Remote Intrusion Attempt		Custom Rule ...	Misc Recon Event	159....	22	03/giu/2014 10:40:01
Unir Remote Intrusion Attempt		Custom Rule ...	Misc Recon Event	159....	22	03/giu/2014 10:41:00
Remote SSH Scanner Detected		Custom Rule ...	ACL Deny	159....	22	03/giu/2014 10:40:03
Remote SSH Scanner Detected		Custom Rule ...	ACL Deny	159....	22	03/giu/2014 10:40:02
Remote SSH Scanner Detected		Custom Rule ...	ACL Deny	159....	22	03/giu/2014 10:40:02
Remote SSH Scanner Detected		Custom Rule ...	ACL Deny	159....	22	03/giu/2014 10:40:01
Remote SSH Scanner Detected		Custom Rule ...	ACL Deny	159....	22	03/giu/2014 10:41:00
Remote SSH Scanner Detected		Custom Rule ...	ACL Deny	159....	22	03/giu/2014 10:41:00
Remote SSH Scanner Detected		Custom Rule ...	ACL Deny	159....	22	03/giu/2014 10:41:00

Last 10 Flows Flows

Application	Source IP	Source Port	Destination IP	Destination Port	Total Bytes	Last Packet Time
RemoteAccess.SSH_TCP_Allot	58.83.146.252	30211	159 ..	22	2	03/giu/2014 10:41:43
RemoteAccess.SSH_TCP_Allot	58.83.146.252	30211	159 ..	22	2	03/giu/2014 10:41:13
RemoteAccess.SSH_TCP_Allot	58.83.146.252	30211	159 ..	22	2	03/giu/2014 10:41:13
RemoteAccess.SSH_TCP_Allot	58.83.146.252	30211	159 ...	22	2	03/giu/2014 10:40:43
RemoteAccess.SSH_TCP_Allot	58.83.146.252	30211	159 ..	22	2	03/giu/2014 10:40:43
RemoteAccess.SSH_TCP_Allot	58.83.146.252	30211	159 ..	22	2	03/giu/2014 10:40:43
RemoteAccess.SSH_TCP_Allot	58.83.146.252	30211	15[illegible] .	22	2	03/giu/2014 10:40:43
RemoteAccess.SSH_TCP_Allot	58.83.146.252	30211	15[illegible] ..	22	2	03/giu/2014 10:40:13
RemoteAccess.SSH_TCP_Allot	58.83.146.252	30211	159 ...	22	2	03/giu/2014 10:40:13
RemoteAccess.SSH_TCP_Allot	58.83.146.252	30211	159. ..	22	2	03/giu/2014 10:40:13

Top 5 Annotations Annotations

Annotation	Tin
"Offense Chaining". This offense has 22 destinations (destination IPs), which are the source (attacker)in other offenses	29/mag/2014
"CRE Event". CRE Rule description: [Unimi Remote Intrusion Attempt] Detected a remote host attempting reconnaissance or suspicious connections on common SSH ports to more than 20 hosts in 10 minutes.	28/mag/2014
[4] "Destination/Event Analysis". The number of events this source generated during this attack, was deemed worth a value of 4 on a scale of 0-10, with higher values indicating high volumes of events generated, and lower numbe...	03/giu/2014 1
"CRE Event". CRE Rule description: [Multiple Login Failures for the Same User] Detected multiple (10) authentication failures for the same user name in a 5 minute period.	28/mag/2014
"CRE Event". CRE Rule description: [Unimi Remote Intrusion Attempt] Detected a remote host attempting reconnaissance or suspicious connections on common SSH ports to more than 20 hosts in 10 minutes.	31/mag/2014

Es. offesa trattata: eventi

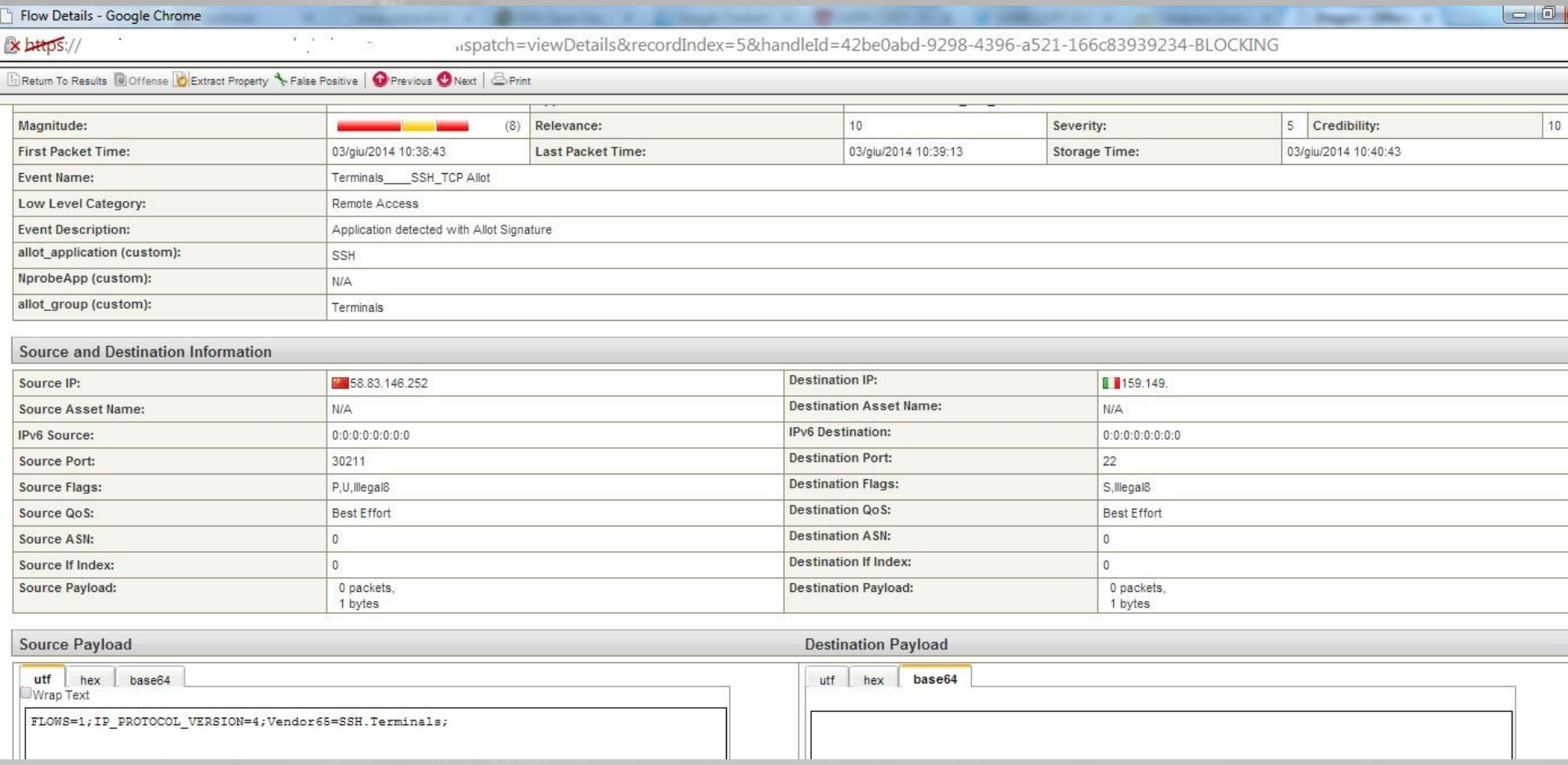
Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destin Port	Usernam	Magnitude
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:41:00	ACL Deny	58.83.146.252	30211	159. [redacted] 27	22	N/A	
Remote Intrusion Attempt	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:41:00	Misc Recon Event	58.83.146.252	30211	159. [redacted] 78	22	N/A	
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:41:00	ACL Deny	58.83.146.252	30211	159. [redacted] 0	22	N/A	
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:41:00	ACL Deny	58.83.146.252	30211	159 [redacted] 255	22	N/A	
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:59	ACL Deny	58.83.146.252	30211	159. [redacted] 255	22	N/A	
Remote Intrusion Attempt	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:59	Misc Recon Event	58.83.146.252	30211	159. [redacted] 255	22	N/A	
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:58	ACL Deny	58.83.146.252	30211	159. [redacted] 51	22	N/A	
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:58	ACL Deny	58.83.146.252	30211	159. [redacted] 4	22	N/A	
Remote Intrusion Attempt	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:57	Misc Recon Event	58.83.146.252	30211	159. [redacted] 34	22	N/A	
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:57	ACL Deny	58.83.146.252	30211	159. [redacted] 11	22	N/A	
Remote Intrusion Attempt	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:57	Misc Recon Event	58.83.146.252	30211	159. [redacted] 255	22	N/A	
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:57	ACL Deny	58.83.146.252	30211	159. [redacted] 32	22	N/A	
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:56	ACL Deny	58.83.146.252	30211	159. [redacted] 179	22	N/A	
Remote Intrusion Attempt	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:56	Misc Recon Event	58.83.146.252	30211	159. [redacted] 3	22	N/A	
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:55	ACL Deny	58.83.146.252	30211	159. [redacted] 220	22	N/A	
Remote Intrusion Attempt	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:55	Misc Recon Event	58.83.146.252	30211	159. [redacted] 5	22	N/A	
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:55	ACL Deny	58.83.146.252	30211	159. [redacted] 104	22	N/A	
Remote Intrusion Attempt	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:55	Misc Recon Event	58.83.146.252	30211	159. [redacted]	22	N/A	
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:54	ACL Deny	58.83.146.252	30211	159. [redacted] 5	22	N/A	
Remote Intrusion Attempt	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:54	Misc Recon Event	58.83.146.252	30211	159. [redacted] 39	22	N/A	
Remote SSH Scanner Detected	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:53	ACL Deny	58.83.146.252	30211	159. [redacted] 41	22	N/A	
Remote Intrusion Attempt	Custom Rule Engine-107 :: trimalci...	1	03/06/14 10:40:53	Misc Recon Event	58.83.146.252	30211	159. [redacted] 45	22	N/A	

Es. offesa trattata: flussi

(Hide Charts)

First Packet Time	Storage Time	Source IP	Source Port	Destination IP	Destination Port	Source Bytes	Destination Bytes	Total Bytes
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]27	22	1 (C)	1	2
03/06/14 10:39...	03/06/14 1...	58.83.146.252	30211	159.[redacted]0	22	1 (C)	1	2
03/06/14 10:39...	03/06/14 1...	58.83.146.252	30211	159.[redacted]255	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]41	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]214	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]6	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]207	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]230	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]0	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]32	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]4	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]15	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]7	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]207	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]91	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]61	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]32	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]7	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]4	22	1 (C)	1	2
03/06/14 10:38...	03/06/14 1...	58.83.146.252	30211	159.[redacted]53	22	1 (C)	1	2

Es. offesa trattata: flussi


Flow Details - Google Chrome

https://...spatch=viewDetails&recordIndex=5&handleId=42be0abd-9298-4396-a521-166c83939234-BLOCKING

Return To Results | Offense | Extract Property | False Positive | Previous | Next | Print

Magnitude:	(8)	Relevance:	10	Severity:	5	Credibility:	10
First Packet Time:	03/giu/2014 10:38:43	Last Packet Time:	03/giu/2014 10:39:13	Storage Time:	03/giu/2014 10:40:43		
Event Name:	Terminals____SSH_TCP Allot						
Low Level Category:	Remote Access						
Event Description:	Application detected with Allot Signature						
allot_application (custom):	SSH						
NprobeApp (custom):	N/A						
allot_group (custom):	Terminals						

Source and Destination Information

Source IP:	58.83.146.252	Destination IP:	159.149.
Source Asset Name:	N/A	Destination Asset Name:	N/A
IPv6 Source:	0:0:0:0:0:0:0:0	IPv6 Destination:	0:0:0:0:0:0:0:0
Source Port:	30211	Destination Port:	22
Source Flags:	P,U,Illegal8	Destination Flags:	S,Illegal8
Source QoS:	Best Effort	Destination QoS:	Best Effort
Source ASN:	0	Destination ASN:	0
Source If Index:	0	Destination If Index:	0
Source Payload:	0 packets, 1 bytes	Destination Payload:	0 packets, 1 bytes

Source Payload

utf | hex | base64

Wrap Text

```
FLOWS=1;IP_PROTOCOL_VERSION=4;Vendor65=SSH.Terminals;
```

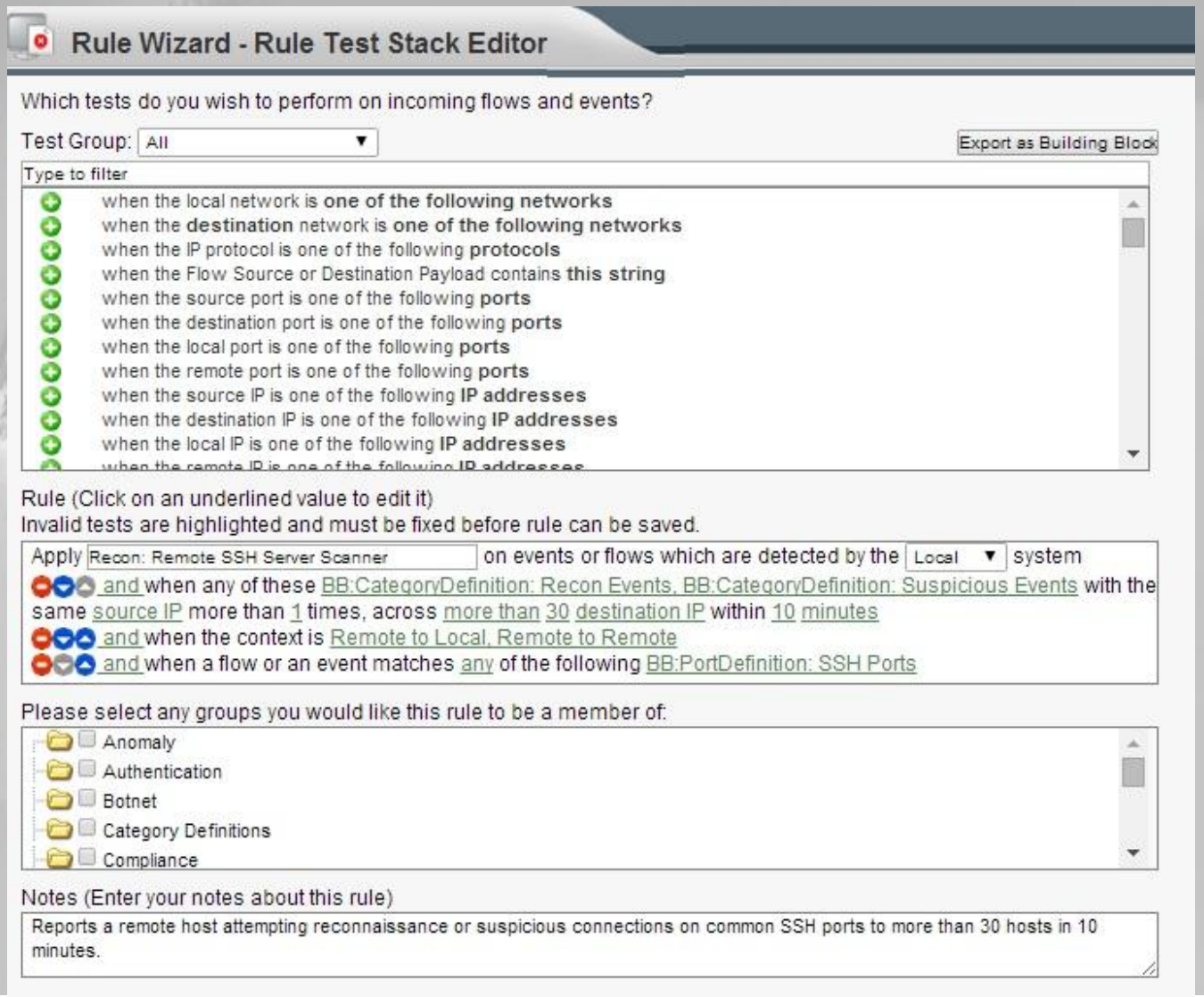
Destination Payload

utf | hex | base64

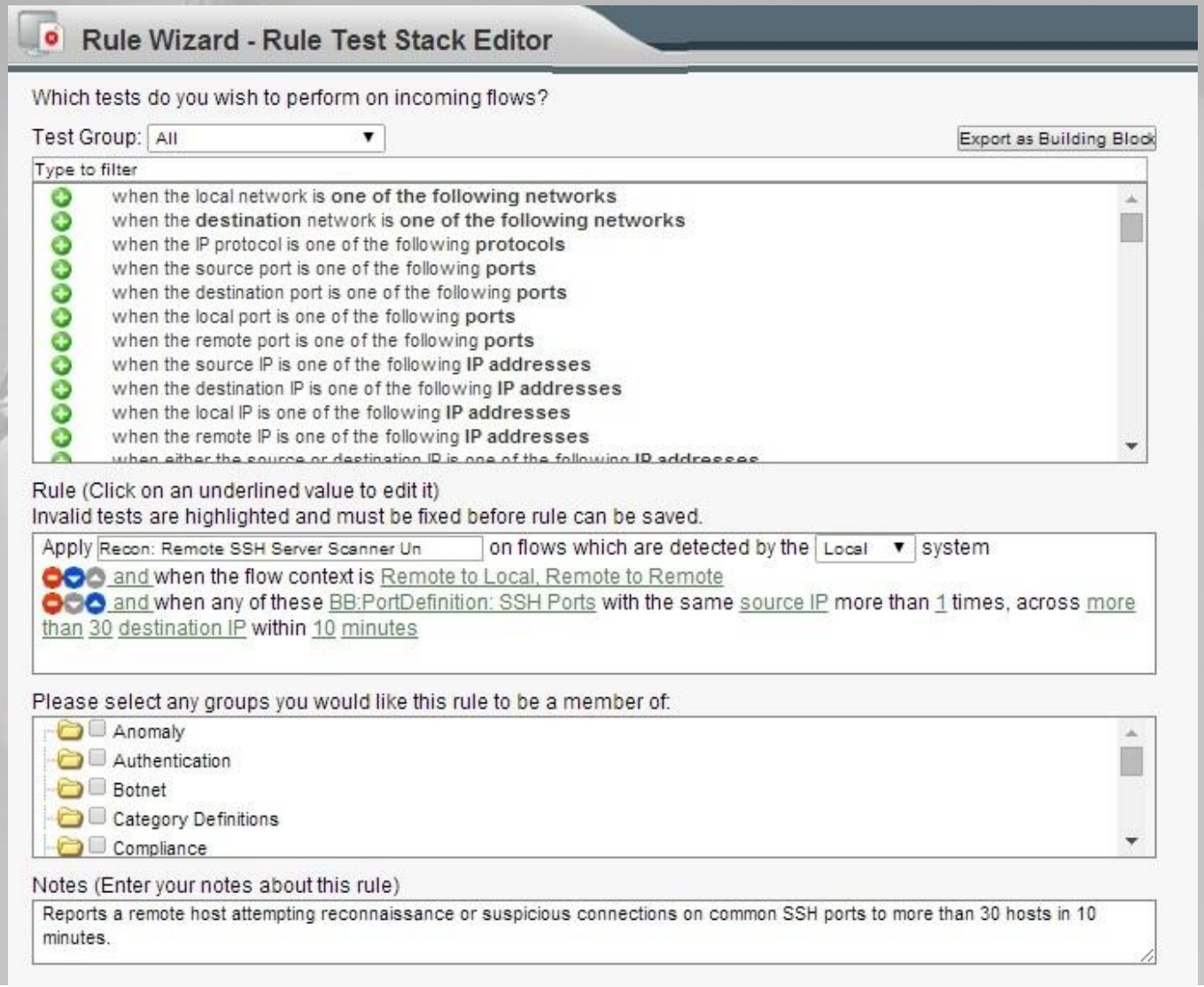
Es. offesa trattata: Regole

Additional Information			
Flow Type:	Standard Flow	Flow Source/Interface:	tri
Flow Direction:	R2L		
Custom Rules:	BB:NetworkDefinition: Honeypot like Addresses BB:CategoryDefinition: Suspicious Flows BB:CategoryDefinition: Suspicious Events BB:PortDefinition: SSH Ports BB:CategoryDefinition: Any Flow Magnitude Adjustment: Destination Network Weight is Low Magnitude Adjustment: Destination Asset Exists Magnitude Adjustment: Source Network Weight is Low Magnitude Adjustment: Context is Remote to Local BB:NetworkDefinition: Client Networks BB:PortDefinition: Authorized L2R Ports BB:NetworkDefinition: Inbound Communication from Internet to Local Host BB:CategoryDefinition: Regular Office Hours BB:NetworkDefinition: Untrusted Network Segment BB:CategoryDefinition: Countries/Regions with no Remote Access		
Custom Rules Partially Matched:	System: Flow Source Stopped Sending Flows Recon: Remote SSH Server Scanner Recon: Host Port Scan Detected by Remote Host Recon: Remote SSH Server Scanner Uni		
Annotations:	Relevance has been decreased by 2 because the destination network weight is low. Relevance has been increased by 8 because the destination asset exists. Relevance has been decreased by 2 because the source network weight is low. Relevance has been increased by 2 because the context is Remote to Local.		

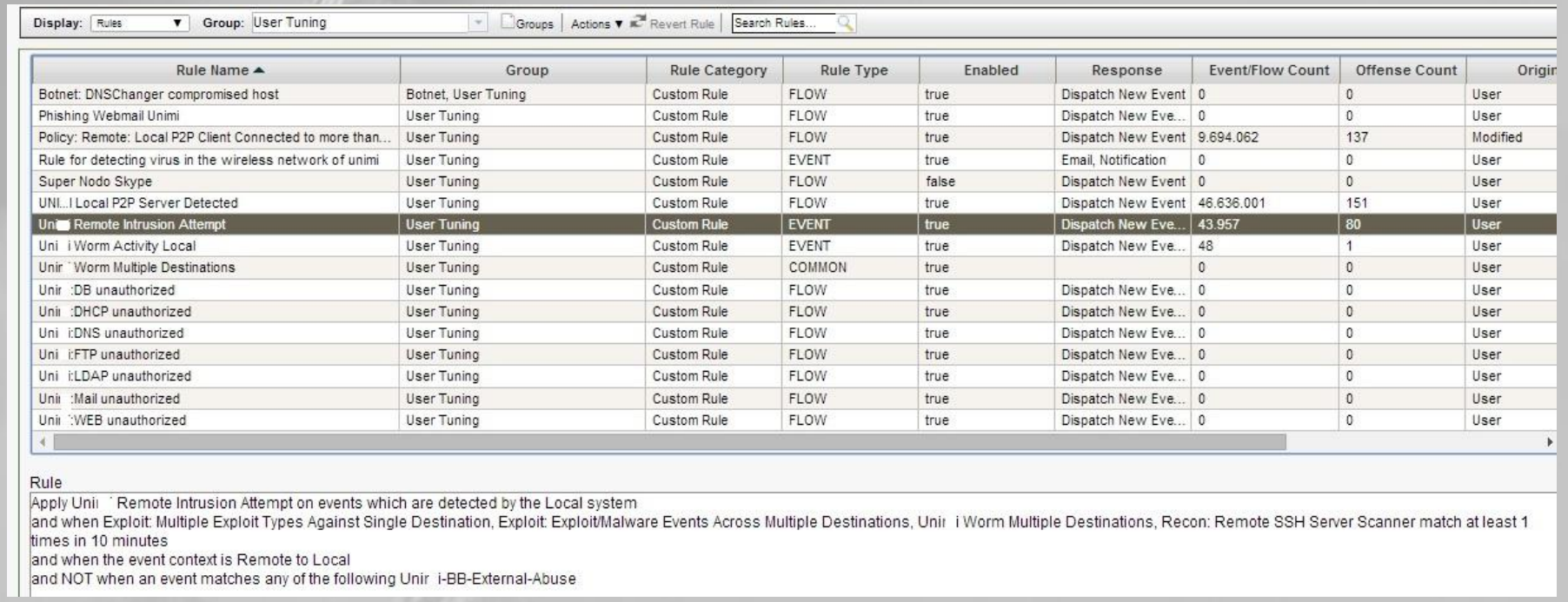
Es. offesa trattata: Def Regole



Es. offesa trattata: Def Regole



Regola che genera offesa



Display: Rules | Group: User Tuning | Groups | Actions | Revert Rule | Search Rules...

Rule Name	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count	Origin
Botnet: DNSChanger compromised host	Botnet, User Tuning	Custom Rule	FLOW	true	Dispatch New Event	0	0	User
Phishing Webmail Unimi	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Policy: Remote: Local P2P Client Connected to more than...	User Tuning	Custom Rule	FLOW	true	Dispatch New Event	9.694.062	137	Modified
Rule for detecting virus in the wireless network of unimi	User Tuning	Custom Rule	EVENT	true	Email, Notification	0	0	User
Super Nodo Skype	User Tuning	Custom Rule	FLOW	false	Dispatch New Event	0	0	User
UNI...l Local P2P Server Detected	User Tuning	Custom Rule	FLOW	true	Dispatch New Event	46.636.001	151	User
Un Remote Intrusion Attempt	User Tuning	Custom Rule	EVENT	true	Dispatch New Eve...	43.957	80	User
Uni i Worm Activity Local	User Tuning	Custom Rule	EVENT	true	Dispatch New Eve...	48	1	User
Unir Worm Multiple Destinations	User Tuning	Custom Rule	COMMON	true		0	0	User
Unir :DB unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Unii :DHCP unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Uni i:DNS unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Uni i:FTP unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Uni i:LDAP unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Unii :Mail unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Unii :WEB unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User

Rule

Apply Unii Remote Intrusion Attempt on events which are detected by the Local system
and when Exploit: Multiple Exploit Types Against Single Destination, Exploit: Exploit/Malware Events Across Multiple Destinations, Unir i Worm Multiple Destinations, Recon: Remote SSH Server Scanner match at least 1 times in 10 minutes
and when the event context is Remote to Local
and NOT when an event matches any of the following Unir i-BB-External-Abuse

BB: elenco IP esterni attaccanti

Display: Building Blocks | Group: User Tuning | Groups | Actions | Revert Rule | Search Rules...

Block Name	Group	Rule Category	Block Type	Event/Flow Count	...	Origin	Creation Date	Modification Date
BB:DownadupHosts	User Tuning	Custom Rule	EVENT	0	0	User	23/gen/2012 17:17	23/gen/2012 17:17
BB-SKYPESUPERNODE	User Tuning	Custom Rule	EVENT	0	0	User	20/gen/2012 16:52	20/gen/2012 16:57
BB-External-Abuse	User Tuning	Custom Rule	EVENT	0	0	User	20/gen/2012 11:34	03/giu/2014 20:03
BB-VIRUS	User Tuning	Custom Rule	EVENT	0	0	User	18/gen/2012 17:31	03/giu/2014 14:03
BB:WebExploit	User Tuning	Custom Rule	EVENT	0	0	User	18/gen/2012 17:03	18/gen/2012 17:04
BB:TrafficConverter	User Tuning	Custom Rule	EVENT	0	0	User	13/gen/2012 16:30	13/gen/2012 16:49
BB:ConfickerHosts	User Tuning	Custom Rule	EVENT	0	0	User	13/gen/2012 15:23	13/gen/2012 15:30
BB:PortDefinition:Ldap Source Ports	User Tuning	Custom Rule	COMMON	0	0	User	13/set/2011 16:03	13/set/2011 16:04
BB:PortDefinition:Windows Source Ports	User Tuning	Custom Rule	COMMON	0	0	User	13/set/2011 16:02	13/set/2011 16:03
BB:PortDefinition:Web Source Ports	User Tuning	Custom Rule	COMMON	0	0	User	13/set/2011 16:01	13/set/2011 16:01
BB-PortDefinition:DHCP Source Ports	User Tuning	Custom Rule	COMMON	0	0	User	13/set/2011 15:56	13/set/2011 15:57
BB:PortDefinition:DNS Source Port	User Tuning	Custom Rule	COMMON	0	0	User	13/set/2011 15:36	13/set/2011 15:37
BB:PortDefinition:Mail Source Ports	User Tuning	Custom Rule	COMMON	0	0	User	22/lug/2011 16:36	22/lug/2011 16:38
BB-ShaperAllot: Null Flow	User Tuning	Custom Rule	FLOW	0	0	User	01/lug/2011 18:05	19/apr/2013 14:16
BB-P2P	User Tuning	Custom Rule	EVENT	0	0	User	01/lug/2011 11:28	03/giu/2014 20:03
BB-Skype	User Tuning	Custom Rule	FLOW	0	0	User	30/giu/2011 17:13	05/gen/2012 11:54
BB-FalsePositive: User Defined False Positiv...	User Tuning	Custom Rule	COMMON	0	0	Modified	30/giu/2011 13:05	12/mar/2012 15:14

Rule

Apply Unimi-BB-External-Abuse on events which are detected by the Local system
and when the local IP is one of the following 127.0.0.2, 125.211.211.61, 119.73.217.77, 1.93.34.226, 111.160.179.66, 1.93.33.2, 69.89.14.31, 216.154.221.228, 113.106.93.58, 202.69.15.149, 60.173.11.28, 223.4.99.36, 66.155.3.88, 82.221.102.185, 187.191.71.222, 187.204.189.167, 183.62.139.139, 1.93.34.210, 1.93.37.229, 101.231.194.137, 200.186.145.218, 115.47.7.237, 69.129.31.26, 186.74.215.238, 204.16.241.202, 115.238.45.163, 211.25.206.34, 218.108.18.89, 193.105.134.170, 41.225.169.44, 191.238.84.17, 1.93.29.137, 59.16.254.2, 151.1.216.110, 192.245.88.223, 50.19.137.10, 2.179.102.212, 2.2.2.2

Altro tipo offesa gestita

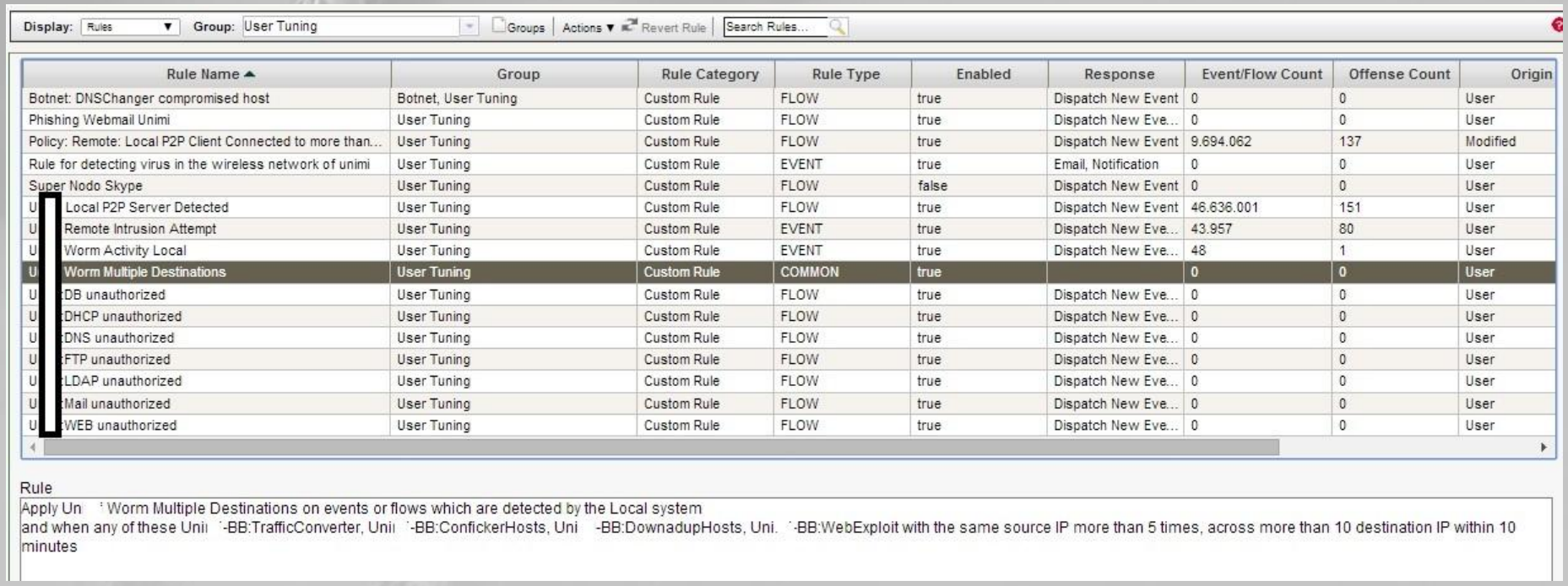
Display: Rules Group: User Tuning Groups Actions Revert Rule Search Rules...

Rule Name	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count	Origin
Botnet: DNSChanger compromised host	Botnet, User Tuning	Custom Rule	FLOW	true	Dispatch New Event	0	0	User
Phishing Webmail Unimi	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Policy: Remote: Local P2P Client Connected to more than...	User Tuning	Custom Rule	FLOW	true	Dispatch New Event	9.694.062	137	Modified
Rule for detecting virus in the wireless network of unimi	User Tuning	Custom Rule	EVENT	true	Email, Notification	0	0	User
Super Nodo Skype	User Tuning	Custom Rule	FLOW	false	Dispatch New Event	0	0	User
UN[redacted] Local P2P Server Detected	User Tuning	Custom Rule	FLOW	true	Dispatch New Event	46.636.001	151	User
Un[redacted] Remote Intrusion Attempt	User Tuning	Custom Rule	EVENT	true	Dispatch New Eve...	43.957	80	User
Un[redacted] Worm Activity Local	User Tuning	Custom Rule	EVENT	true	Dispatch New Eve...	48	1	User
Un[redacted] Worm Multiple Destinations	User Tuning	Custom Rule	COMMON	true		0	0	User
Un[redacted] DB unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Un[redacted] DHCP unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Un[redacted] DNS unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Un[redacted] FTP unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Un[redacted] LDAP unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Un[redacted] Mail unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Un[redacted] WEB unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User

Rule

Apply Uni[redacted]. Worm Activity Local on events which are detected by the Local system
and when Exploit: Multiple Exploit Types Against Single Destination, Exploit: Exploit/Malware Events Across Multiple Destinations, Recon: Local L2L Windows Server Scanner, Uni[redacted] Worm Multiple Destinations match at least 2 times in 10 minutes
and when the event context is Local to Local, Local to Remote
and NOT when an event matches any of the following Unir[redacted]-BB-HostDefinition: Condono Altro, Unir[redacted]-BB-HostDefinition: Router, Uni[redacted]-BB-HostDefinition: Firewall, BB:HostDefinition: Servers

Altro tipo offesa gestita



Display: Rules | Group: User Tuning | Groups | Actions | Revert Rule | Search Rules...

Rule Name	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count	Origin
Botnet: DNSChanger compromised host	Botnet, User Tuning	Custom Rule	FLOW	true	Dispatch New Event	0	0	User
Phishing Webmail Unimi	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
Policy: Remote: Local P2P Client Connected to more than...	User Tuning	Custom Rule	FLOW	true	Dispatch New Event	9.694.062	137	Modified
Rule for detecting virus in the wireless network of unimi	User Tuning	Custom Rule	EVENT	true	Email, Notification	0	0	User
Super Nodo Skype	User Tuning	Custom Rule	FLOW	false	Dispatch New Event	0	0	User
U [redacted] Local P2P Server Detected	User Tuning	Custom Rule	FLOW	true	Dispatch New Event	46.636.001	151	User
U [redacted] Remote Intrusion Attempt	User Tuning	Custom Rule	EVENT	true	Dispatch New Eve...	43.957	80	User
U [redacted] Worm Activity Local	User Tuning	Custom Rule	EVENT	true	Dispatch New Eve...	48	1	User
U [redacted] Worm Multiple Destinations	User Tuning	Custom Rule	COMMON	true		0	0	User
U [redacted] DB unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
U [redacted] DHCP unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
U [redacted] DNS unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
U [redacted] FTP unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
U [redacted] LDAP unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
U [redacted] Mail unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User
U [redacted] WEB unauthorized	User Tuning	Custom Rule	FLOW	true	Dispatch New Eve...	0	0	User

Rule

Apply Un ' Worm Multiple Destinations on events or flows which are detected by the Local system
and when any of these Unii '-BB:TrafficConverter, Unii '-BB:ConfickerHosts, Uni -BB:DownadupHosts, Uni. '-BB:WebExploit with the same source IP more than 5 times, across more than 10 destination IP within 10 minutes

Riassumendo

- ***SEGNALAZIONE INCIDENTE***
  - Automatizzazione della fase di segnalazione degli incidenti più critici
  - Effetto: aumento della tempestività nell'individuazione dell'incidente
- ***ANALISI DELL'INCIDENTE***
  1. Riduzione automatica dei falsi positivi e delle informazioni non rilevanti:
  - Effetto: semplificazione del lavoro del SOC e risparmio di tempo nell'individuazione delle fonti di incidenti
  2. Individuazione di forme di botnet precedentemente non rilevate
  - Effetto: aumentata proattività del SOC, aumento del numero di incidenti individuati dal SOC, eliminazione dei falsi positivi legati ai DNS istituzionali
  3. Realizzazione di meccanismi per la creazione di offese customizzate contenenti la "diagnosi"
  - Effetto: semplificazione del lavoro dell'operatore, risparmio di tempo e possibilità di fare script per il trattamento automatico.

Riassumendo

- ***ANALISI DELL'INCIDENTE***
  4. Integrazione DSCC e DB-IPMAC
  – Effetto: risparmio temporale per il SOC nell'accesso alle informazioni relative all'IP in analisi
  5. Generazione di offese custom per tipologie di traffico critiche
  – Effetto: risparmio di tempo nell'analisi dell'incidente
- ***AZIONE***
  1. Plugin user friendly che consente al SOC di agire istantaneamente
  – Effetto: intervento immediato di blocco o contenimento, evitando l'accesso diretto ad un appliance critica
  2. Automatizzazione del trattamento automatico delle offese più critiche :
  – Effetto: maggiore proattività SOC, tempestività applicazione azione, minimizzazione tempo esposizione,

Riassumendo

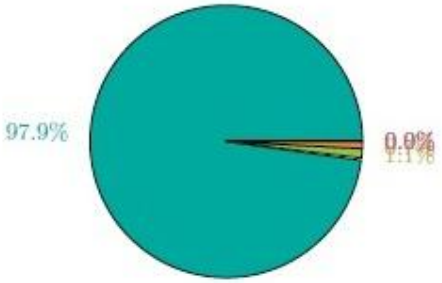
- ***REPORTISTICA***
  1. Crezione Viste ad hoc: es liste Unauthorized Server, Visualizzazione di liste di IP differenziate per traffico applicativo (Es. P2P) con relativi grafici di offese custom per tipologie di traffico critiche
  – Effetto: Migliore fruibilità delle informazioni AZIONE
  2. Inserimento automatico Info su Incidente in DB Incidenti
  – Effetto: ottimizzazione tempo SOC
  3. Automatizzazione generazione dei report su Incidenti Sicurezza
  – Effetto: ottimizzazione tempo SOC

Dati su incidenti primi 5 mesi

TOTALE INCIDENTI: 9894

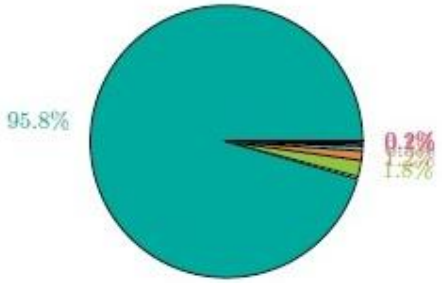
Segnalazione

	#
dscc	9683
analisi soc	113
garr	73
altra fonte interna	18
ids	4
altra fonte esterna	3



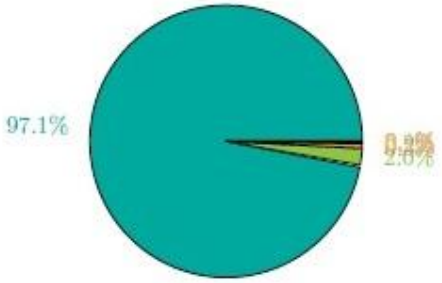
Causa

	#
abuso esterno	9475
traffico anomalo	181
malconfigurazione	120
presunta pirateria	45
server non registrato	43
compromesso	19
spam	11



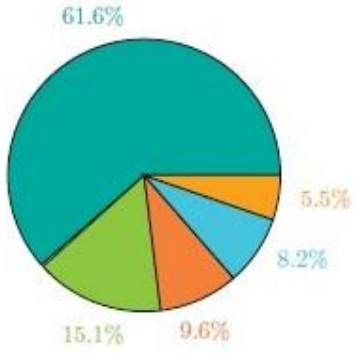
Interventi non normalizzati

	#
blocco automatico DSCC	9630
intervento referente	203
blocco IP	28
falso positivo	24
blocco porta	14
analisi	7
intervento utente	5
non rintracciabile	5



Tipologia segnalazioni

	#
presunta pirateria	45
malconfigurazione	11
traffico anomalo	7
compromesso	6
spam	4

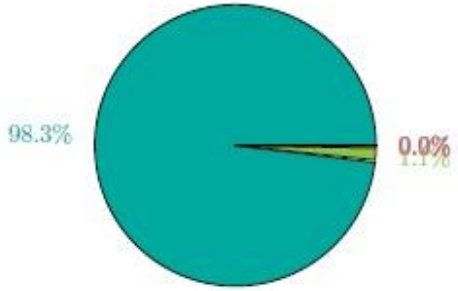


Dati su incidenti primi 5 mesi

TOTALE INCIDENTI SICUREZZA: 9849

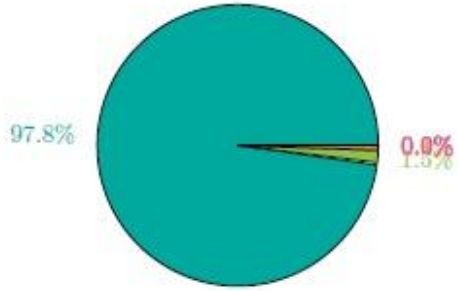
Segnalazione

	#
dscc	9683
analisi soc	113
garr	28
altra fonte interna	18
ids	4
altra fonte esterna	3



Interventi

	#
contenimento automatico	9630
intervento referente	144
contenimento manuale	42
falso positivo	16
analisi	6
intervento utente	3
non rintracciabile	2



Riassumendo

- ***REPORTISTICA***
  1. Crezione Viste ad hoc: es liste Unauthorized Server, Visualizzazione di liste di IP differenziate per traffico applicativo (Es. P2P) con relativi grafici di offese custom per tipologie di traffico critiche
  – Effetto: Migliore fruibilità delle informazioni AZIONE
  2. Inserimento automatico Info su Incidente in DB Incidenti
  – Effetto: ottimizzazione tempo SOC
  3. Automatizzazione generazione dei report su Incidenti Sicurezza
  – Effetto: ottimizzazione tempo SOC

Alcuni incidenti molto gravi: DRDoS

- ULTIMO ANNO **176 attacchi DRDoS**
- Picco giugno 2013: attacchi DDRoS basati su DNS
  - L'attacco si basa sul protocollo DNS: l'aggressore invia pacchetti con IP sorgente falso che interrogano il. Server DNS, il traffico risultante viene ricevuto dalla vittima;
  - non si tratta quindi di una compromissione ma di una configurazione troppo aperta (open recusive DNS server).
  - Chi lancia l'attacco ottiene un effetto di amplificazione: le interrogazioni della dimensione di qualche byte generano risposte di vari Kbyte.
  - Alcune possibili soluzioni:
    . disabilitare il servizio dns se non utilizzato
    . configurare il dns perche' risponda solo ai client del proprio dominio
    . autorizzare il protocollo DNS a livello di border router solo per i server ufficiali

Alcuni incidenti molto gravi: DRDOS

- gennaio 2014- maggio 2014: attacchi DRDoS causati da NTP reflection
  - Sfrutta vulnerabilita' di configurazione del protocollo NTP che consente la riflessione moltiplicata dei pacchetti causando DoS e DDoS sulla rete.
  - l'aggressore invia pacchetti con IP sorgente falso che interrogano (comando monlist) i server sulla porta 123.
    Il traffico di risposta e' molto maggiore dell'interrogazione (amplificazione fino a 200 volte) e viene inviato alla vittima anche su porte diverse dalla 123.

Q & A

Grazie per l'attenzione