Continuous monitoring

efficace degli eventi di sicurezza:

un caso concreto di successo

Digital Forensics Alumni

OPEN DAY 2016

Milano, 28/6/2016

Roberto Obialero

Presentazione dei relatori

Fabio Bucciarelli

Regione Emilia-Romagna

Roberto Obialero

Descrizione contesto operativo del case study

Regione Emilia-Romagna

Il Servizio Sistema Informativo Informatico Regionale

- Gestione dell'informatica “all'interno” dell'Ente Regione Emilia-Romagna
- Comprende la gestione della sicurezza informatica
- Alcuni numeri

Approccio alla sicurezza in Regione Emilia-Romagna

- Una certa sensibilità ai temi della sicurezza informatica, fin dai tempi del decreto privacy
- Lo stimolo viene soprattutto dalle normative, purtroppo la sicurezza viene percepita di solito come un problema dell'IT

MA ...

- Si è cercato di "usare" le normative per allargare la visuale e intervenire con misure che migliorino la sicurezza informatica
- Questo si è tradotto in investimenti rivolti al miglioramento della sicurezza informatica

Il punto di partenza per il processo di countinuos monitoring

- Ai tempi del provvedimento del Garante sugli amministratori di sistema ci siamo dotati di un SIEM e abbiamo iniziato a raccogliere i log di tutti i nostri sistemi
- Chiaramente era esagerato rispetto a quanto richiesto dal provvedimento …

Il punto di partenza per il processo di countinuos monitoring

- Perché non utilizzare tutti questi dati per monitorare in maniera continua la sicurezza?
- Come estrarre le “informazioni dal rumore di fondo”?
- Il tutto a fronte di un numero di risorse molto limitato

Best practices applicabili al processo di continuous monitoring degli eventi di sicurezza

CSC6: Maintenance, Monitoring and Analysis of Audit Logs

CSC19: Incident Response and Management

Il problema (ovvero la gestione di un numero infinito di eventi con risorse finite)

Key figures

- Sistema Informativo eterogeneo (circa 700 server)
- > 1500 EPS (events per second)
- > 135.000.000 EPD
- 32 connettori (raccolta log da OS e middleware)
- Budget & Response Team limitato

Specifiche progettuali

Approccio seguito:

- progetto pilota
- verifica dei risultati
- standardizzazione delle procedure

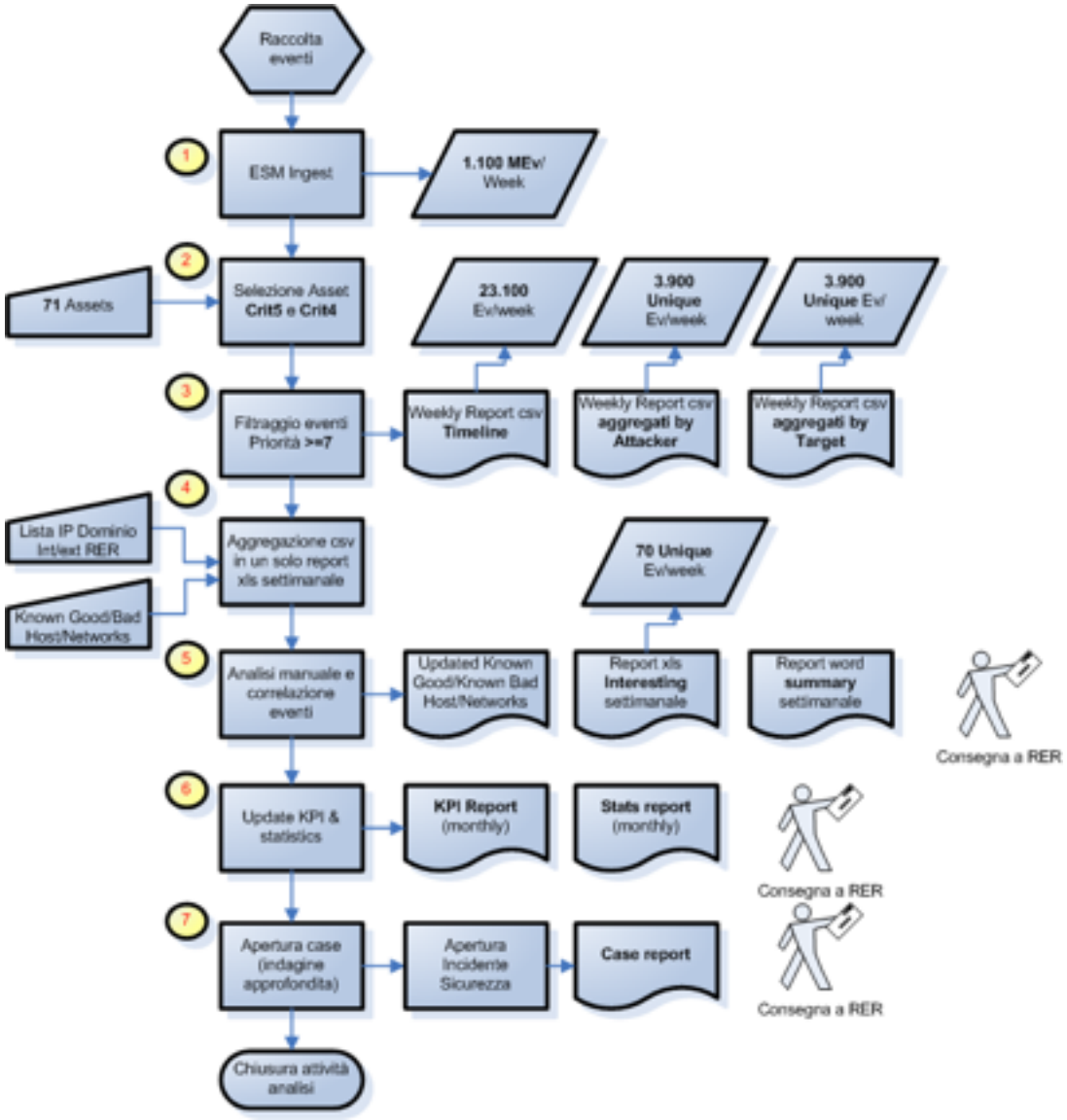
Parametri di classificazione

degli oggetti e degli eventi:

Criticità > business role & privacy

Priorità > confidence, relevance, severity

L'attività di analisi e la formalizzazione del processo



Output delle attività di analisi

Attacker Address	Hostname	Name	Priority	Target Address	Hostname	Target Port	Device Product	Count	Date Time	Comments
23.239.69.179	NODESDIRECT	_Customer High Number of Denied Connections	8				VPN-1 & FireWall-1	1	Oct 26 2015 05:38:26	Anche da altri IP netblock
61.147.103.70	CHINANET-JS	_Customer High Number of Denied Connections	7				VPN-1 & FireWall-1	11	Oct 26 2015 01:24:11	Anche da altri IP netblock
85.25.218.117	malta1013.startdedicated.com	_Customer High Number of Denied Connections	8				VPN-1 & FireWall-1	2	Oct 26 2015 12:00:32	Anche da altri IP netblock
89.248.174.117	hosted-by.ecatel.net	_Customer High Number of Denied Connections	7				VPN-1 & FireWall-1	1	Oct 30 2015 17:42:26	Anche da altri IP netblock
123.151.149.222	TIANJIN-HAOWEIGAOKE-LTD	_Customer High Number of Denied Connections	7				VPN-1 & FireWall-1	6	Oct 26 2015 03:23:13	
113.108.21.16	CHINANET-GD	_Customer High Number of Denied Connections	7				VPN-1 & FireWall-1	7	Oct 26 2015 01:28:58	
146.0.226.251	VELIANET-DE-HTEC	_Customer High Number of Denied Connections	8				VPN-1 & FireWall-1	5	Oct 26 2015 01:27:17	Anche da altri IP stesso net
169.45.161.189	vw.bd.a1.2da9.ip4.static.sl-reverse.com/	_Customer High Number of Denied Connections	7				VPN-1 & FireWall-1	4	Oct 26 2015 06:34:03	Anche da altri IP stesso net
222.186.61.8	CHINANET-JS	_Customer High Number of Denied Connections	7				VPN-1 & FireWall-1	12	Oct 26 2015 00:15:54	Anche da altri IP stesso net
223.4.244.13	ALISOFT	_Customer High Number of Denied Connections	7				VPN-1 & FireWall-1	1	Oct 26 2015 07:26:26	Anche da altri IP stesso net
XXX.YYY.200.1	Customer Ext ?	0051: IP: Source IP Address Spoofed (Impossible Packet)	10	XXX.YYY.200.1	Customer Ext ?	36640	UnityOne	1	Oct 26 2015 10:24:28	
208.109.255.51	pdns04.domaincontrol.com	20875: DNS: Kaspersky Sinkhole DNS Reply	7	XXX.YYY.192.81	ArcelO	60487	UnityOne	1	Oct 26 2015 00:44:01	Anche verso altre porte tar
216.69.185.51	pdns03.domaincontrol.com	20875: DNS: Kaspersky Sinkhole DNS Reply	7	XXX.YYY.192.81	ArcelO	37175	UnityOne	1	Oct 26 2015 00:44:01	Anche verso altre porte tar
192.168.141.12	Customer Int ?	12563: SMB: Samba SVCCTL StartServiceW Buffer Overflo	8	192.168.41.46	Customer Int ?	445	UnityOne	16	Oct 26 2015 02:53:03	Anche da altri IP Int verso a
23.239.69.131	SC7067-23-239-69-128-29	13012: SIP: SipVicious Brute Force SIP Tool	8	XXX.YYY.200.206	videodg.arpa.nnn.its	5060	UnityOne	35	Oct 27 2015 22:51:59	Anche da diversi altri IP Ext
37.113.7.13	cip-37-113-7-13.pppoe.ufa.ertelecom.ru.	13814: TLS: OpenSSL Suspicious Heartbeat Packet	7	XXX.YYY.197.97	Customer Ext ?	8443	UnityOne	6	Oct 29 2015 09:58:56	Anche verso altri IP Custom
37.187.129.166	ns316491.ip-37-187-129.eu	13817: TLS: OpenSSL Heartbleed Vulnerability	9	XXX.YYY.197.127	sanita.provider.Customer.it	443	UnityOne	1	Oct 28 2015 00:48:35	Anche verso altri IP Custom
64.247.172.12	12-172-247-64-static.centennialpr.net	13817: TLS: OpenSSL Heartbleed Vulnerability	8	XXX.YYY.197.35		443	UnityOne	4	Oct 29 2015 06:34:55	Anche verso altri IP Custom
77.247.181.165	politkovskaja.torservers.net	13817: TLS: OpenSSL Heartbleed Vulnerability	9	XXX.YYY.200.211	www.smr.arpa.nnn.its	443	UnityOne	1	Oct 26 2015 16:14:33	Anche verso altri IP Custom
85.143.95.50	VLSU-NET	13817: TLS: OpenSSL Heartbleed Vulnerability	8	XXX.YYY.197.142	Customer Ext ?	8443	UnityOne	1		Anche verso altri IP Custom
94.23.248.36	ns305334.ip-94-23-217.eu	13817: TLS: OpenSSL Heartbleed Vulnerability	8	XXX.YYY.193.55		443	UnityOne	1	Oct 26 2015 16:14:32	Anche verso altri IP Custom
94.103.176.86	tor-exit.squirrel.theremailer.net	13817: TLS: OpenSSL Heartbleed Vulnerability	8	XXX.YYY.197.91	servizimoka.provider.Customer.it	443	UnityOne	2	Oct 29 2015 09:58:55	Anche verso altri IP Custom
104.232.3.33	tor-exit.manzres.org	13817: TLS: OpenSSL Heartbleed Vulnerability	8	XXX.YYY.197.142	Customer Ext ?	443	UnityOne	2	Oct 30 2015 18:59:53	Anche verso altri IP Custom
149.202.98.161	2.tor.exit.babylon.network	13817: TLS: OpenSSL Heartbleed Vulnerability	8	XXX.YYY.200.252	ippc-elatest.arpa.nnn.its	443	UnityOne	2	Oct 28 2015 00:48:25	Anche verso altri IP Custom
171.25.193.235	tor-exit3-readme.dfri.se	13817: TLS: OpenSSL Heartbleed Vulnerability	8	XXX.YYY.197.130	webmail.provider.Customer.it	443	UnityOne	2		Anche verso altri IP Custom
176.126.252.12	aurora.enn.lu	13817: TLS: OpenSSL Heartbleed Vulnerability	9	XXX.YYY.197.86	iass.provider.Customer.it	443	UnityOne	1	Oct 29 2015 09:59:05	Anche verso altri IP Custom
185.36.100.145	tor-proxy-readme.cloudexit.eu	13817: TLS: OpenSSL Heartbleed Vulnerability	8	XXX.YYY.193.54	FPDELNX	443	UnityOne	1	Oct 26 2015 16:14:31	Anche verso altri IP Custom
185.62.189.216	hosted-by.blazingfast.io	13817: TLS: OpenSSL Heartbleed Vulnerability	8	XXX.YYY.197.190		443	UnityOne	1	Oct 26 2015 16:14:31	Anche verso altri IP Custom
185.82.201.17	poolsrv202.maxided.com	13817: TLS: OpenSSL Heartbleed Vulnerability	8	XXX.YYY.197.143	www.assemblea.nnn.its	443	UnityOne	4	Oct 29 2015 04:51:06	Anche verso altri IP Custom
198.27.85.134	g00.int.nandex.org	13817: TLS: OpenSSL Heartbleed Vulnerability	9	XXX.YYY.200.196	srvmaster.arpa.nnn.its	443	UnityOne	4	Oct 28 2015 00:48:26	Anche verso altri IP Custom
212.47.238.193	193-238-47-212.rev.cloud.scaleway.com	13817: TLS: OpenSSL Heartbleed Vulnerability	9	XXX.YYY.197.93	testsanita.provider.Customer.it	443	UnityOne	3	Oct 26 2015 16:14:32	Anche da altri IP netblock
162.218.67.34	mistihead.com	12348: HTTP: PHP-CGI Query String Parameter Comman	8	XXX.YYY.200.212	Customer Ext ?	80	UnityOne	2		Anche verso altri IP Custom
192.169.71.34	fiberaned.com	12348: HTTP: PHP-CGI Query String Parameter Comman	9	XXX.YYY.200.145	fe.arpa.nnn.its	80	UnityOne	6	Oct 28 2015 04:00:23	Anche verso altri IP Custom

Statistiche e KPI

Month	# Total	Average Total/ Day	# Unique EV	Average Unique/Day	# Interesting	Average interesting	#Categorized Cases
1501	9.305	775	996	83	20	2	
1502	20.677	738	2.165	77	61	2	
1503	20.506	661	1.976	64	98	3	
1504	224.468	7.482	48.915	1.631	188	6	16
150							
15							
15							
15							
15							
15							
15							
Tot							

Area	KPI #	Nome	Misurazione	Fonte e modalità Misura	Frequenza	05-lug	12-lug	19-lug	26-lug	02-ago
Ambiente	1	NAMO	# Asset Monitorati	Asset ESM Manuale	M			647		
	2	NACR	# Asset Critici	Asset associati a Criticità > =4 Manuale	M			71		
	3	NEVG	# Eventi giornalieri	Eventi ESM Manuale	M/W	129.600.000	140.400.000	140.400.000	281.000.000	192.200.000
Criticità	4	NEPA	# Eventi rilevanti associati ad alta priorità	Eventi associati a Priorità >=7 ESM	M/W	58.418	27.014	3.809	100.000	97.639
	5	NLFA	# Episodi login falliti > 3	Analisi report Manuale	M/W	12	11	15	6	7
	6	INTE	# Categorie eventi interesting	Analisi report Manuale	M/W	19	31	27	24	19
	7	HNDC	# Episodi "High number of denied connections" > 4	(# e lista) Subquery da Report Manuale	M			59		
	8	IEPF	# Incidenti di sicurezza gestiti al di fuori della piattaforma SIEM	Valutazione Manuale	M					

Key findings

Date Time	Attacker Address	Attacker Hostname
Jan 24 2016 23:58:03	X.243.204.79	X.-243-204-79.foo.
Jan 29 2016 23:10:34	X.243204103	X.-243-204-103.foo.
Jan 26 2016 03:15:22	X.243.205.90	X.-243-205-90.foo.
Jan 28 2016 12:27:28	X.243205203	
Jan 28 2016 12:27:34	X.243205203	
Jan 28 2016 12:27:36	X.243205203	
Jan 29 2016 01:03:48	X.243254234	X.-243-254-234.foo.
Jan 26 2016 10:49:19	X.248.57.18	
Jan 26 2016 10:49:12	X.248.57.18	
Jan 26 2016 01:04:03	X.248.57.125	X.-248-57-125.foo.
Jan 26 2016 01:03:57	X.248.57.125	X.-248-57-125.foo.
Jan 27 2016 00:48:07	X.248.57.176	
Jan 27 2016 00:48:26	X.248.57.176	X.-248-57-176.foo.
Jan 27 2016 00:48:19	X.248.57.176	X.-248-57-176.foo.
Jan 25 2016 11:28:25	X.248.58.35	
Jan 25 2016 11:28:12	X.248.58.35	
Jan 25 2016 06:36:18	X.248.58.175	
Jan 26 2016 06:59:51	X.248.58.213	X.-248-58-213.foo.
Jan 26 2016 06:59:48	X.248.58.213	X.-248-58-213.foo.
Jan 26 2016 07:00:05	X.248.58.213	X.-248-58-213.foo.
Jan 26 2016 06:59:50	X.248.58.213	X.-248-58-213.foo.
Jan 26 2016 07:00:01	X.248.58.213	X.-248-58-213.foo.
Jan 26 2016 06:59:48	X.248.58.213	X.-248-58-213.foo.
Jan 29 2016 05:35:45	X.248.58.249	X.-248-58-249.foo.
Jan 29 2016 05:35:47	X.248.58.249	X.-248-58-249.foo.
Jan 30 2016 18:36:39	X.248.58.253	X.-248-58-253.foo.
Jan 25 2016 12:32:52	X.248.59.126	
Jan 28 2016 03:03:32	X.248.59.232	
Jan 28 2016 03:03:33	X.248.59.232	
Jan 26 2016 03:49:48	X.248.60.158	
Jan 26 2016 03:49:47	X.248.60.158	
Jan 30 2016 14:17:28	X.248.61.39	
Jan 30 2016 14:17:29	X.248.61.39	X.-248-61-39.foo.

End Time	Attacker Address	Name	Priority	Target Address	Target Port	Device Product
Aug 23 2015 01:17:36	192.99.154.24	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.200.211	443	UnityOne
Aug 23 2015 01:17:36	192.99.154.24	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.200.199	443	UnityOne
Aug 23 2015 01:17:36	107.181.174.84	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.193.54	443	UnityOne
Aug 23 2015 01:17:36	69.42.58.204	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.200.252	443	UnityOne
Aug 23 2015 01:17:36	107.181.174.84	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.200.251	443	UnityOne
Aug 23 2015 01:17:36	5.9.36.66	13817: TLS: OpenSSL Heartbleed Vulnerability	9	68.71.200.97	443	UnityOne
Aug 23 2015 01:17:36	5.9.36.66	13817: TLS: OpenSSL Heartbleed Vulnerability	9	68.71.200.202	443	UnityOne
Aug 23 2015 01:17:37	69.42.58.204	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.200.105	443	UnityOne
Aug 23 2015 01:17:37	192.99.154.24	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.200.247	443	UnityOne
Aug 23 2015 01:17:37	107.181.174.84	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.200.196	443	UnityOne
Aug 23 2015 01:17:37	107.181.174.84	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.200.195	443	UnityOne
Aug 23 2015 01:17:37	104.232.3.33	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.200.169	443	UnityOne
Aug 23 2015 01:17:37	107.181.174.84	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.200.121	443	UnityOne
Aug 23 2015 01:17:38	192.99.154.24	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.200.252	443	UnityOne
Aug 23 2015 01:17:38	195.154.56.44	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.200.251	443	UnityOne
Aug 23 2015 01:17:40	5.79.68.161	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.197.32	443	UnityOne
Aug 23 2015 01:17:40	5.79.68.161	13817: TLS: OpenSSL Heartbleed Vulnerability	9	68.71.197.86	443	UnityOne
Aug 23 2015 01:17:40	5.79.68.161	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.197.52	443	UnityOne
Aug 23 2015 01:17:40	195.154.56.44	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.197.31	443	UnityOne
Aug 23 2015 01:17:40	195.154.56.44	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.197.49	443	UnityOne
Aug 23 2015 01:17:40	37.187.129.166	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.197.93	443	UnityOne
Aug 23 2015 01:17:40	37.187.129.166	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.197.35	443	UnityOne
Aug 23 2015 01:17:40	37.187.129.166	13817: TLS: OpenSSL Heartbleed Vulnerability	8	68.71.197.91	443	UnityOne

Known Bad List

IP Address	Host/Net Name	Organization	GEO	Net Range	Since	
1.164.37.106	1-164-37-106.dynamic.hinet.net	Chunghwa Telecom Co	TW	1.160.0.0 - 1.175.255.255	26/04/2015	2556: HTTP: HTTP CONNECT TCP Tunnel to SMTP port
5.9.36.66	r3.apx.pub	Hetzner Online AG	DE	5.9.36.64 - 5.9.36.95	23/08/2015	13817: TLS: OpenSSL Heartbleed Vulnerability
5.196.66.162	ns330209.ip-5-196-66.eu	OVH SAS	FR	5.196.0.0 - 5.196.255.255	06/09/2015	13817: TLS: OpenSSL Heartbleed Vulnerability, 13248: HT
23.91.70.237	23.91.70.237.ipdns.io	A Small Orange LLC	USA	23.91.64.0 - 23.91.79.255	22/11/2015	12348: HTTP: PHP-CGI Query String Parameter Command I
23.91.122.62	windflower.arvixe.com	Arvixe, LLC	USA	23.91.112.0 - 23.91.127.255	02/08/2015	3808: HTTP: SQL Injection Variable Declaration Evasion, T
31.172.30.2	tor19.anonymizer.ccc.de	Chaos Computer Club e.V.	DE	31.172.30.0 - 31.172.30.7	23/08/2015	13817: TLS: OpenSSL Heartbleed Vulnerability
36.226.115.222	36-226-115-222.dynamic-ip.hinet.net	Chunghwa Telecom Co.,Ltd.	TW	36.224.0.0 - 36.239.255.255	03/05/2015	2556: HTTP: HTTP CONNECT TCP Tunnel to SMTP port
37.59.9.143	ns3262471.ip-37-59-9.eu	OVH SAS	FR	37.59.0.0 - 37.59.63.255	03/05/2015	16798: HTTP: GNU Bash HTTP Header Remote Code Execut
37.205.0.65	sweb16.ecozum.dc	E-Cozum Elektronik Ticaret Hizmetleri	TR	37.205.0.0 - 37.205.0.255	13/09/2015	3808: HTTP: SQL Injection Variable Declaration Evasion
38.102.150.27	COGENT-A	PSINet, Inc.	USA	38.0.0.0 - 38.255.255.255	21/06/2015	14266: HTTP: Downadup/Conficker A or B Worm reporting
46.165.210.84	NETDIRECT-NET	Leaseweb Germany GmbH	DE	46.165.208.0 - 46.165.215.255	07/06/2015	_RER High Number of Denied Connections
46.234.105.231	prague-5.cdn77.com	SuperNetwork s.r.o	CZ	46.234.96.0 - 46.234.127.255	10/05/2015	_RER High Number of Denied Connections
52.17.80.106	ec2-52-17-80-106.eu-west-1.compute.ama	Amazon Technologies Inc.	USA	52.0.0.0 - 52.31.255.255	11/10/2015	13817: TLS: OpenSSL Heartbleed Vulnerability, GNU Bash
61.147.103.171	CHINANET-JS	CHINANET jiangsu province network	CN	61.147.0.0 - 61.147.255.255	10/05/2015	_RER High Number of Denied Connections

Adozione di contromisure & next steps progetto

- Blocco netblock ostili a livello di border router
- Verifica delle vulnerabilità e loro rimozione
- Tuning apparati di sicurezza (IPS, Firewall, SIEM)
- Estensione a sistemi a criticità inferiore
- Alerting tempestivo
- Integrazione e correlazione con informazioni fornite da CERT e da piattaforme OSINT
- Adozione tecniche di Active Defense

Il disciplinare RER sulla «Gestione degli incidenti di sicurezza»

- Prima versione del 2007
- Basato su “Computer Security Incident Handling Guide” del NIST (SP 800-61 rev1)
- Coinvolgimento del management e delle altre strutture organizzative
- Creazione di una apposita unità di gestione degli incidenti
- Definizione di un workflow per la gestione degli incidenti di sicurezza

Il disciplinare RER sulla «Gestione degli incidenti di sicurezza»

- Gestione complessa e poco efficace
- Venivano tracciati come incidenti di sicurezza SOLO i casi veramente gravi, quelli con impatto su tutti gli utenti

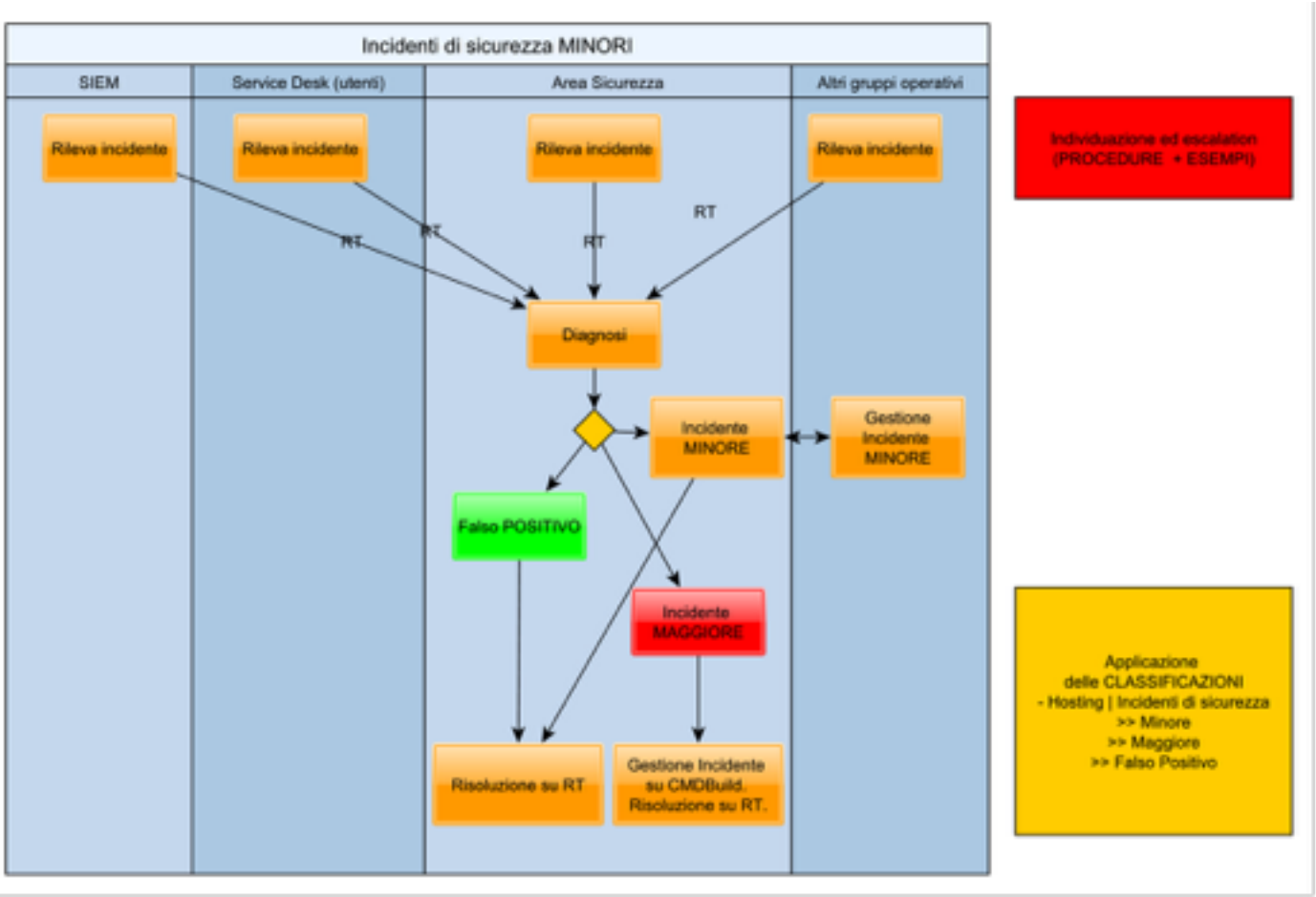
Il collegamento dell'attività di analisi degli eventi al processo di gestione degli incidenti di sicurezza informatica (disciplinato nella nuova versione del DT)

- I dati del monitoraggio entrano nel processo di gestione degli incidenti di sicurezza informatica
- Modalità reattiva (attuabile a seguito risultati analisi)
- Modalità preventiva (azione automatica a seguito alerting)
- Integrazione con lo strumento di ticketing
- Gestione degli incidenti "minori" e dei "near miss", con conseguente arricchimento della kb

Il collegamento dell'attività di analisi degli eventi al processo di gestione degli incidenti di sicurezza informatica (disciplinato nella nuova versione del DT)

- Come avvenuto per il documento del NIST, sono state cancellate le parti specifiche sulle varie tipologie di incidenti, concentrandoci sulla definizione di ruoli e responsabilità
- La figura dell'**Incident Handling Leader**

Il collegamento dell'attività al processo di gestione degli incidenti di sicurezza informatica (disciplinato nella nuova versione del DT)



Prospettiva percorso di certificazione ISO 27001

Integrazioni con il sistema di gestione della sicurezza informatica nella prospettiva della certificazione ISO27001

Impatto sui seguenti obiettivi di controllo (annex A)

Controllo A.12.4: **Raccolta di log e monitoraggio**

Obiettivo: registrare eventi e generare evidenze

Prospettiva percorso di certificazione ISO 27001

Controllo A.16.1 - **Gestione degli incidenti relativi alla sicurezza delle informazioni e miglioramento del processo**

Obiettivo: assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, incluse le comunicazioni relative agli eventi di sicurezza ed ai punti di debolezza.

Conclusioni

- Esigenza di attività Incident Response strutturata
- Applicazione del modello di traffico di rete e comportamento standard (baseline)
- Difficoltà nella separazione attività ostili da rumore
- Eliminazione degli eventi falsi positivi
- Processo iterativo volto al miglioramento continuo
- Necessità di integrazione con gli altri processi di gestione delle sicurezza (incident management e risk treatment)

Open discussion …

Grazie per l'attenzione …

fbucciarelli@regione.emilia-romagna.it

roberto.obialero@gmail.com