]HackingTeam[

Incident handling

Milano

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
1.0	Gennaio 2012	Prima emissione

INFORMAZIONI		
Data di Emissione	Gennaio 2012	
Versione	1.0	
Tipologia Documento	Documento tecnico	
Numero di Protocollo		
Numero Pagine	8	
Numero Allegati		
Descrizione Allegati	1	
	2	
Redatto da	Costantino Imbrauglio	
Approvato da		

INDICE

1 Introduzione

Obbiettivo del presente documento è illustrare le contromisure adottate internamente da HT srl per la gestione degli incidenti informatici.

HT srl offre ai propri clienti un servizio di supporto tecnico a pagamento. Le richieste di supporto vengono inoltrate dai clienti utilizzando un apposito strumento di trouble ticketing (trattasi di uno strumento web based).

Quella di HT srl è una clientela internazionale e la disponibilità dello strumento di trouble ticketing deve essere garantito su base 24x7. Non così la gestione delle richieste di supporto (ticket) aperte dai clienti che vengono invece gestite nel normale orario lavorativo (da lunedì a venerdì e in un orario compreso fra le 9 e le 18).

Le contromisure adottate da HT srl in tema di gestione degli incidenti informatici sono dunque mirate esclusivamente ad aumentare il livello di disponibilità dell'infrastruttura tecnologica di supporto ai clienti.

2 Infrastruttura tecnologica di supporto ai clienti

L'infrastruttura tecnologica di supporto ai clienti prevede un'istanza dedicata di trouble ticketing per ciascuno di essi. Tutte le istanze di trouble ticketing system sono implementate come macchine virtuali VMware basate su sistema operativo Linux Ubuntu Server rel. 8.04.

L'accesso alle istanze di trouble ticketing da parte dei clienti è garantita per mezzo di un concentratore VPN-SSL.

Le componenti tecnologiche che garantiscono la disponibilità e il corretto funzionamento del servizio di supporto ai clienti sono dunque:

- Istanze di trouble ticketing
- Concentratore VPN-SSL
- Server DNS
- Firewall
- Altri apparati di rete (router-gateway, switch, ecc.)

3 Contromisure in tema di gestione degli incidenti informatici

Le contromisure in tema di gestione degli incidenti informatici e volte ad aumentare il livello di disponibilità del servizio di supporto ai clienti sono di due tipi:

- Contromisure tecnologiche
- Contromisure organizzative

3.1 Contromisure tecnologiche

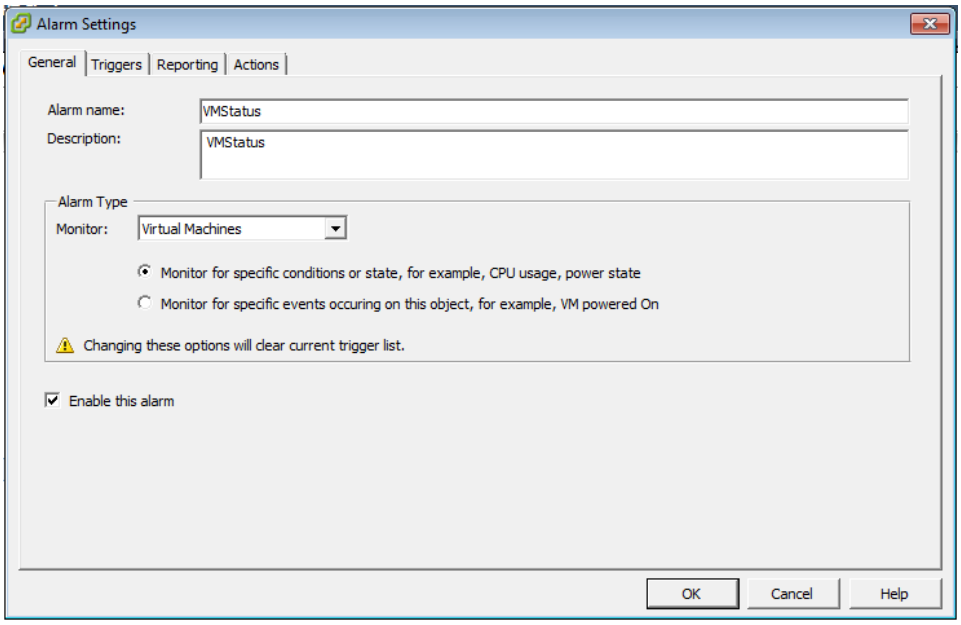
Le contromisure tecnologiche in tema di gestione degli incidenti informatici sono rappresentate da un insieme di strumenti di monitoraggio e generazione allarmi (*monitoring & alerting*). Le componenti tecnologiche oggetto di monitoraggio sono quelle elencate nel paragrafo 2.

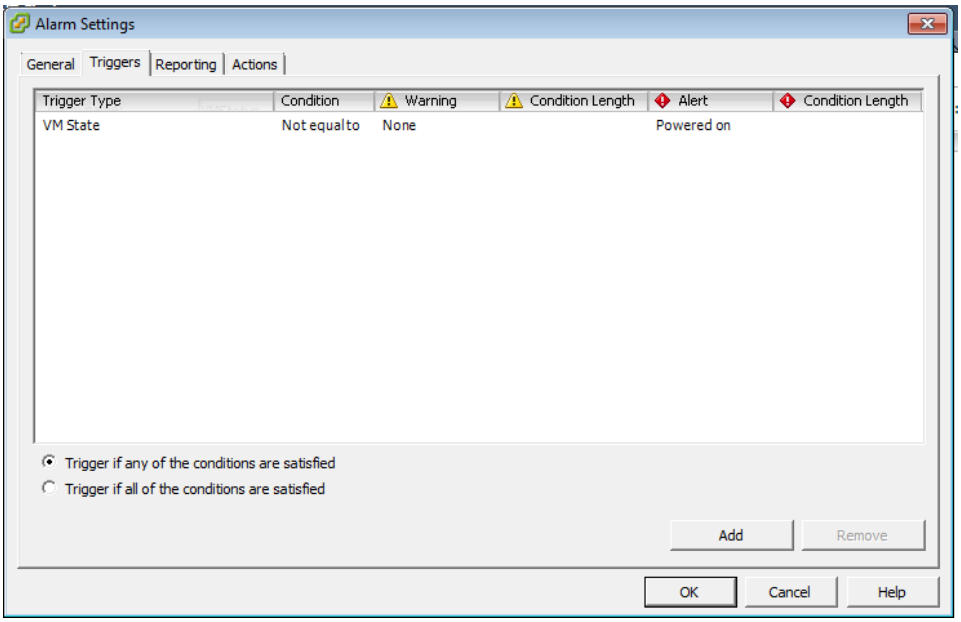
Obbiettivo degli strumenti di monitoraggio è quello di verificare la disponibilità e, ove possibile, il corretto funzionamento delle varie componenti tecnologiche.

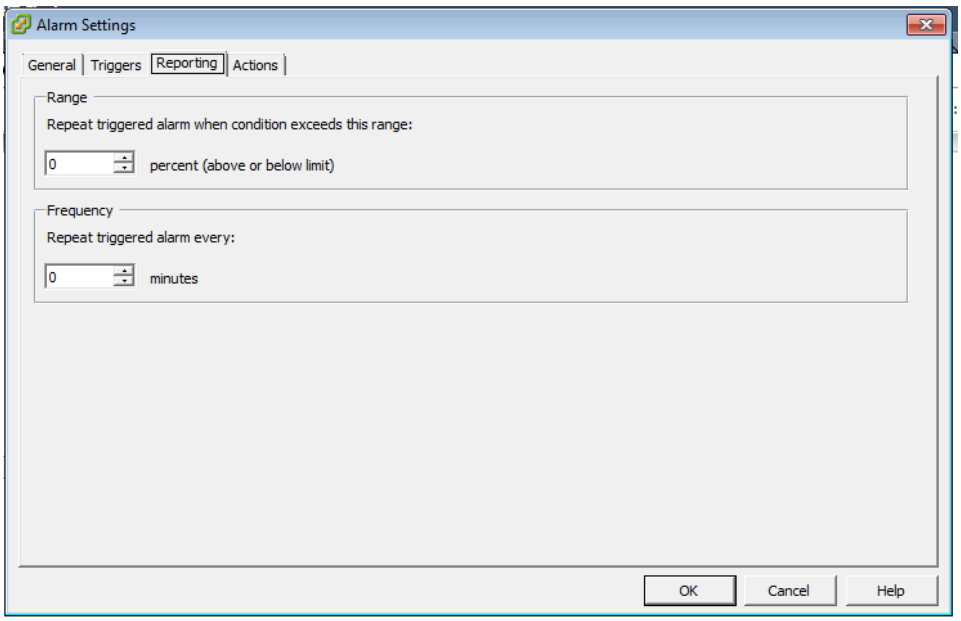
3.1.1 Istanze di trouble ticketing e server DNS

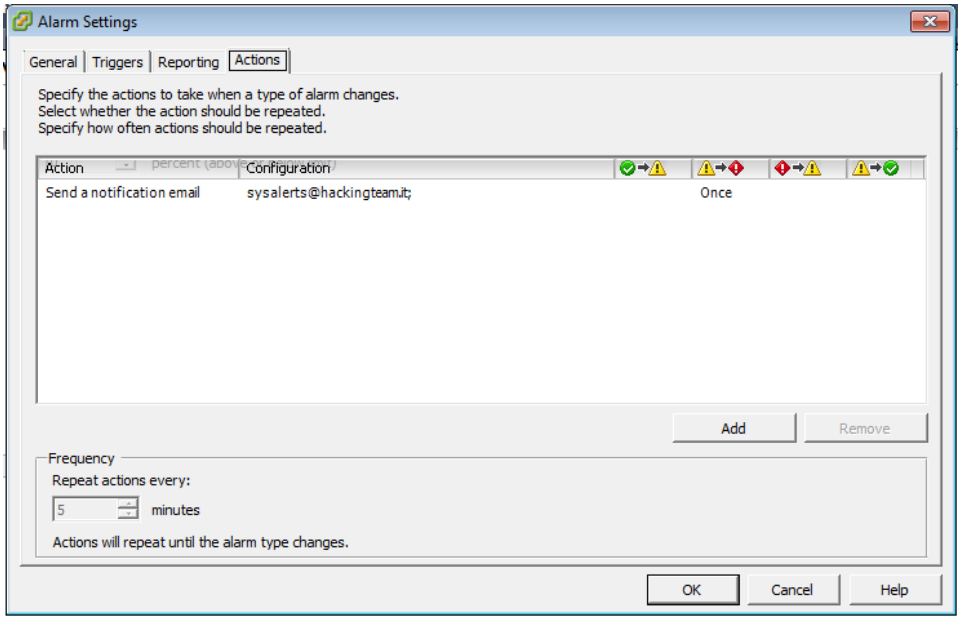
La disponibilità delle istanze di trouble ticketing viene verificata utilizzando il servizio di monitoraggio e generazione allarmi offerto nativamente dalla suite Vmware vCenter. Ove una qualsiasi macchina virtuale di produzione non risulti disponibile (accesa), viene inviata una notifica via e-mail a sysalerts@hackingteam.it.

A questo scopo è stato definito un allarme ad hoc (VMStatus). Le immagini seguenti ne illustrano la definizione.









N.B. L'allarme è associato direttamente ai folder di produzione. Conseguentemente è sufficiente mettere una macchina in produzione (inserirla in uno dei due folder di produzione) affinchè essa venga immediatamente sottoposta a monitoraggio.

N.B. La verifica di disponibilità riguarda esclusivamente lo stato della macchina virtuale (accesa o spenta). Al momento dunque non viene verificata la disponibilità del servizio di trouble ticketing. Ove però si ritenesse opportuno, sarà possibile aggiungere anche questa verifica modificando opportunamente il controllo implementato per verificare la disponibilità del concentratore VPN-SSL.

3.1.2 Concentratore VPN-SSL

La disponibilità del concentratore VPN-SSL viene verificata utilizzando utilizzando uno script di shell opportunamente inserito nel crontab dell'utente nobody sul server mail.hackingteam.it. Lo script viene eseguito ogni 10 minuti. Ne riportiamo qui di seguito il sorgente.

```
#!/bin/sh
URL=https://192.168.100.21/
/usr/bin/curl --connect-timeout 20 -k -I -s $URL > /dev/null 2>&1
if [ $? -ne 0 ]; then
echo "Subject: ALLARME SUPPORTO RCS" | cat -
/usr/local/bin/check_rcs_support.msg | /usr/sbin/sendmail -F
rcs_support_check@hackingteam.it -t rcs-support@hackingteam.it
fi
```

L'eventuale indisponibilità del concentratore VPN-SSL viene segnalata con una mail a rcs-support@hackingteam.it.

3.1.3 Firewall e altri apparati di rete

Al momento non sono stati implementati meccanismi di *monitoring & alerting* né per il firewall né per gli altri apparati di rete.

N.B. L'implementazione di opportuni meccanismi di *monitoring & alerting* per il firewall e gli altri apparati di rete è assolutamente necessaria e auspicabile in tempi brevi.

3.2 Contromisure organizzative

Un sistema di monitoraggio e generazione allarmi al quale non sia associata una policy di gestione degli incidenti è soltanto un sistema ansiogeno.

Una policy di gestione degli incidenti permette di affrontare gli stessi in maniera efficace e razionale in quanto stabilisce chi deve fare cosa allorquando, ad esempio, viene generato un allarme.

La forma più semplice di policy di gestione degli incidenti informatici si limita a definire *l'ownership* degli allarmi generati dalle componenti di *monitoring & alerting*. HT srl si è al momento dotata di una policy di questo tipo.

L'ownership per gli allarmi generati dalle componenti di *monitoring & alerting* è definita nella seguente tabella.

Policy di gestione degli incidenti informatici	
Allarme	**Owner**
Istanze di trouble ticketing	Costantino Imbrauglio
Server DNS	Costantino Imbrauglio
Concentratore VPN-SSL	?
Firewall	N.A.
Altri apparati di rete	N.A.