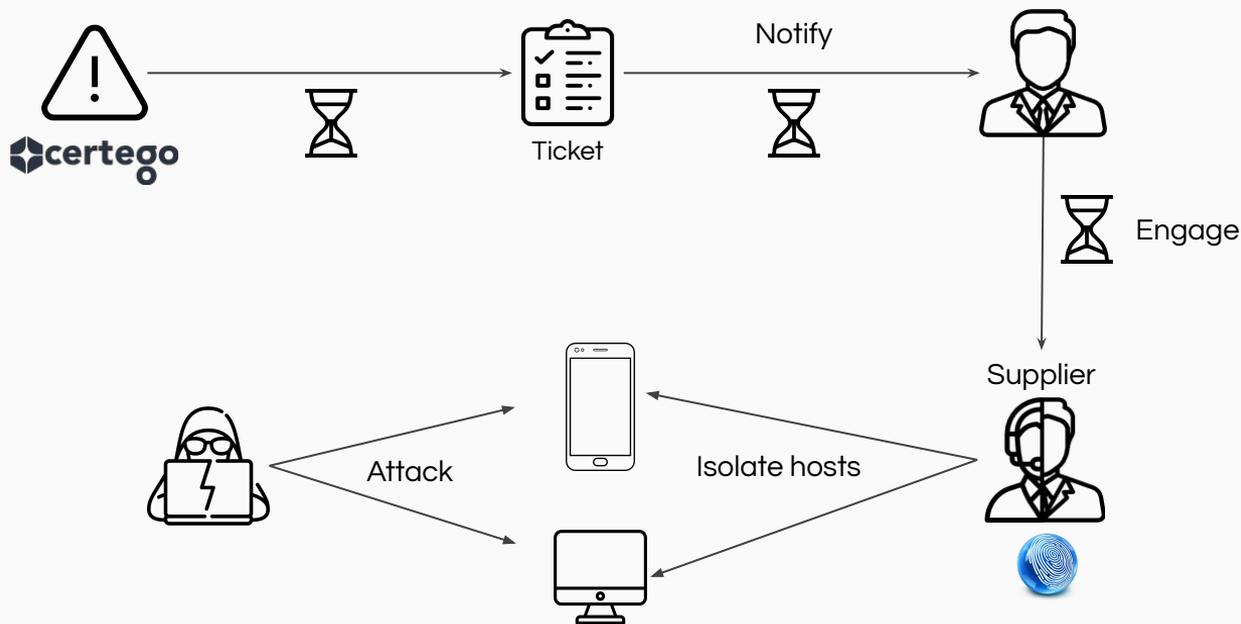


# Tactical Response

# Cisco ISE pxGrid Integration

Tactical Response

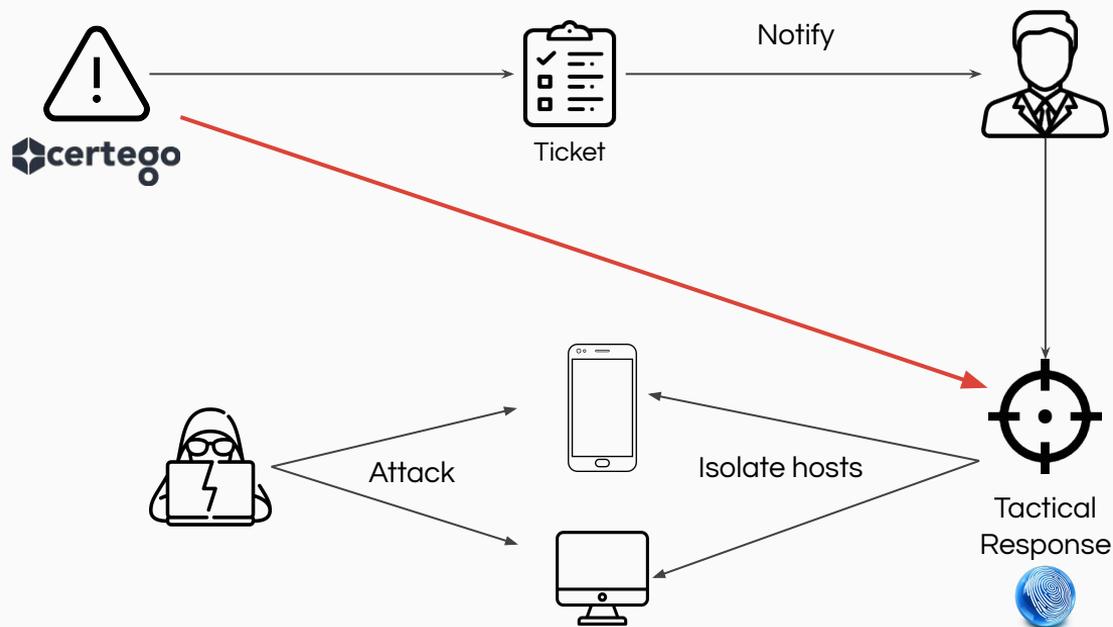
External managing of Cisco ISE could lead to a high MTTR (Mean Time To Respond). Even if the network is managed internally, there could be problems performing some actions (internal escalation, high workload, etc.)



- Reduce the time needed to contain a Cyber Security Incident
- Prevent additional attacks or infections
- Lower the risk associated to ongoing incidents (e.g. by blocking resources related to further infection steps)
- Reduce workload of the Customer



Tactical Response enables Certego IRT to contain attacks in less time, by isolating infected hosts via pxGrid API



Certego s.r.l.  
Opened by Alice Gilli 26 novembre 2020 18:23

## 3 Presence of malware XXX on internal host HOSTNAME

Incident Response Procedure 0%

- Detection
- Analysis
- Info Gathering
- Containment** 1
- Eradiation
- Post Incident

**1** Isolate the reported host CERTEGO

We suggest you to isolate the internal host with the following MAC address from the network to avoid the propagation of infection on other internal hosts:

AA:AA:AA:AA:AA:01

**Acknowledge**

**Tactical Response** Isolate host

Target(s) List

AA:AA:AA:AA:AA:01

Appliances

ISE pxGrid

Expiration date

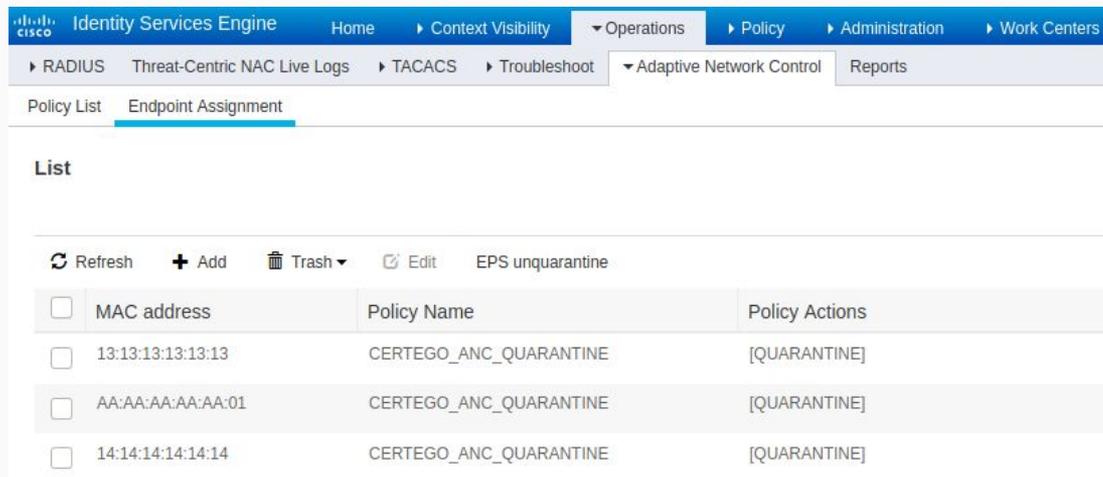
03/06/2021 12:01

Default expiration date is a month from today

Targets blocked on .

**Chiudi**

The MAC address AA:AA:AA:AA:AA:01 is now blocked on ISE, using pxGrid API.



The screenshot shows the Cisco ISE Identity Services Engine interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The active menu is Adaptive Network Control > Reports. The sub-menu is Endpoint Assignment. The main content area is titled 'List' and contains a table of endpoint assignments.

Refresh + Add Trash Edit EPS unquarantine

<input type="checkbox"/>	MAC address	Policy Name	Policy Actions
<input type="checkbox"/>	13:13:13:13:13:13	CERTEGO_ANC_QUARANTINE	[QUARANTINE]
<input type="checkbox"/>	AA:AA:AA:AA:AA:01	CERTEGO_ANC_QUARANTINE	[QUARANTINE]
<input type="checkbox"/>	14:14:14:14:14:14	CERTEGO_ANC_QUARANTINE	[QUARANTINE]