GRUPPO SCAI

SCAI LAB

# Gruppo SCAI

System Integration,
Digital Innovation, Tecnologie,
Soluzioni e Servizi Innovativi

Speaker:
**Vincenzo Ferretti**
**Innovation Engineer**

# Fabbisogni e Risk Management

POLOICT

- Esigenze delle PMI
  - Proteggere i propri Asset e l'Infrastruttura informatica
  - Proteggere i Dati, il Codice, il Know How aziendale
  - Predisporre misure adeguate contro danni di Reputazione, Finanziari e rispetto a controversie Legali

- Normativa e best practices
  - Italian Cyber Security Report « Un Framework Nazionale per la Cyber Security», versione 1.0, Febbraio 2016
  - NIST SP-800, ISO/IEC 27xxx, OWASP best practices
  - Codice in materia di protezione dei dati personali D.lgs 30 giugno 2003, n.196

- Ruolo del Risk Management
  - Fornire uno strumento organizzativo integrabile e flessibile
  - Permettere un controllo costante e dettagliato degli Asset e dei Rischi ad essi collegati
  - Proteggere gli interessi aziendali e garantire la compliance normativa

# Caso Applicativo su PMI

Media Impresa operante nel Settore Telecomunicazioni.

Si vuole analizzare un segmento della rete aziendale erogante i servizi primari, così composto:

- **10 Server / Dispositivi interni**
- **1 Server / Dispositivi esterni**

L'infrastruttura oggetto di Vulnerability Assessment include il Sistema Informatico Interno e la struttura esterna di gestione Sito Web e Posta Elettronica.

Soluzione:

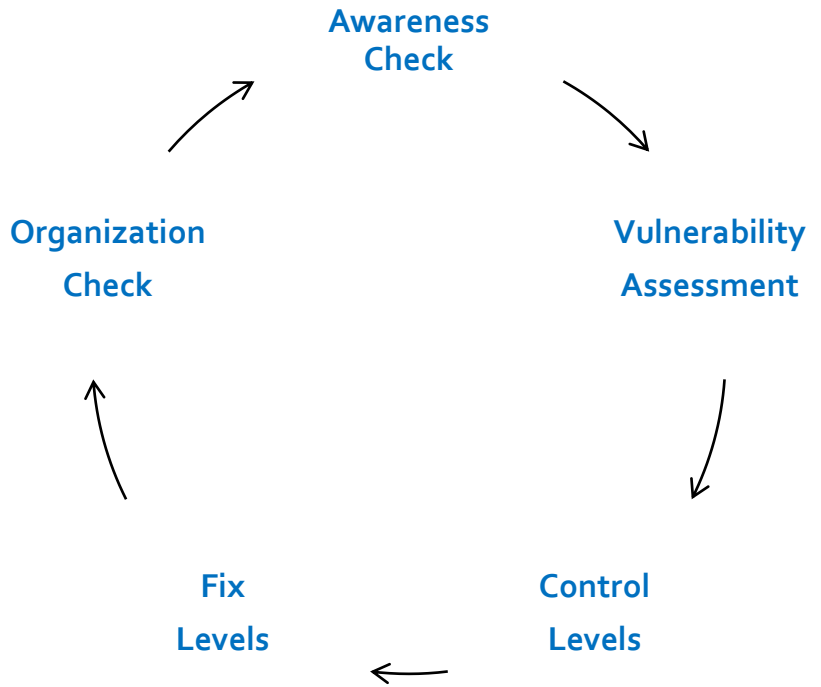
- **Vulnerability Assessment Security Platform**

# Vulnerability Assessment Security Platform

POLOICT

## Obiettivi raggiunti

- Supporto alle attività di **Risk Management**
- Controllo dei **livelli di esposizione** degli Asset
- Controllo dei livelli di organizzazione e consapevolezza in relazione alla **sicurezza dell'infrastruttura**
- Automazione del **Vulnerability Assessment**



# Contatti

Vincenzo Ferretti

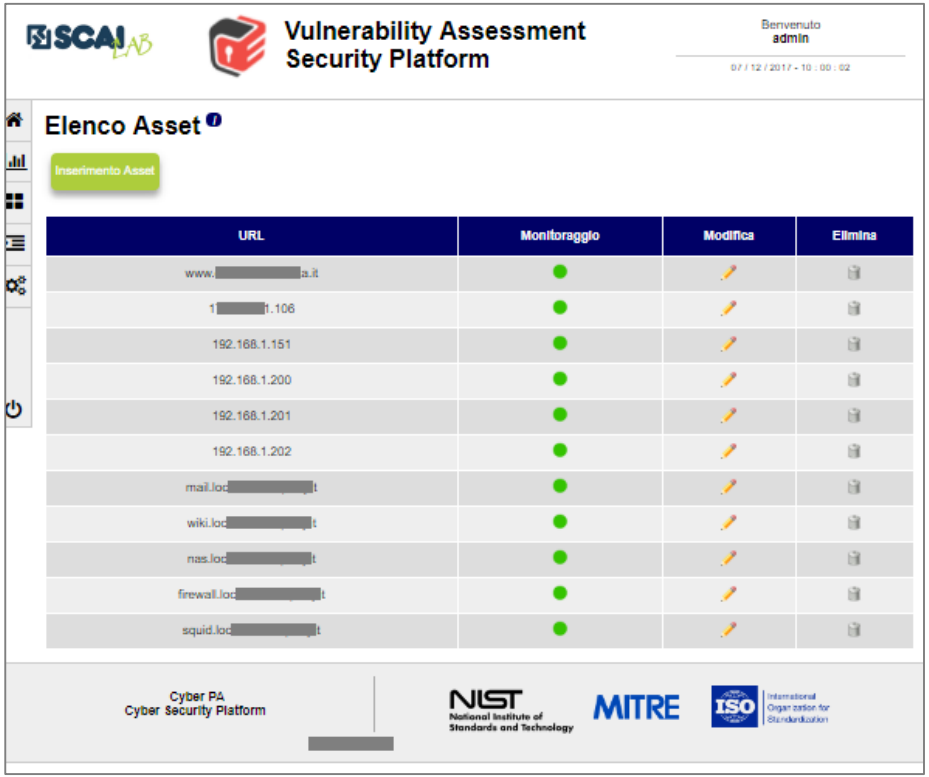
E-mail: vincenzo.ferretti@scai-innovation.grupposcai.it
Tel. +39 011 2273611
www.grupposcai.it

# Allegati

# Vulnerability Assessment Security Platform

POLOICT

## Step 1 «Definizione Asset»




**Raccolta ed Analisi Dati** → *Attribuzione Rating* → *Generazione Report*

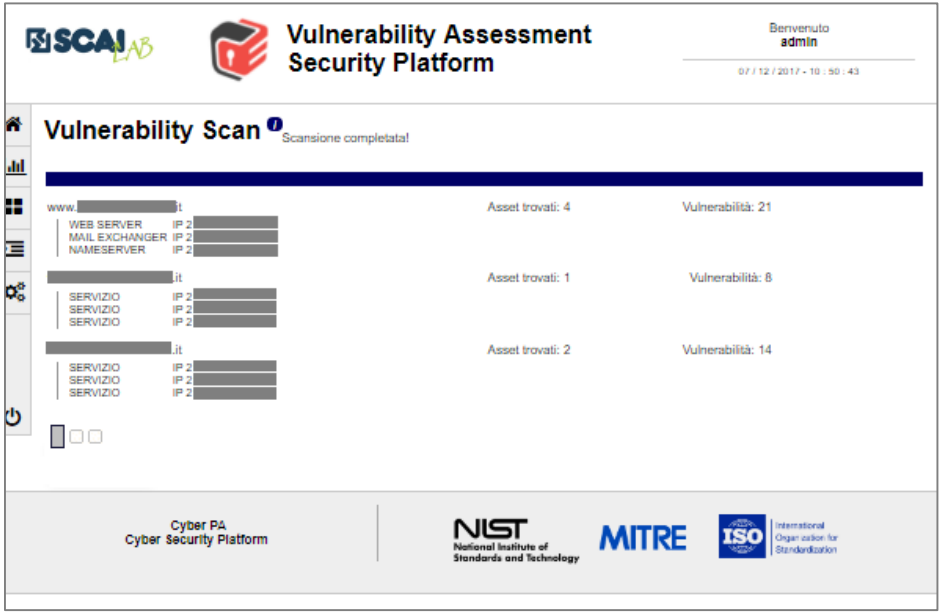
Modello Dati

| Questionario Organization | Questionario Awareness | Elenco Asset |
|---|---|---|

# Vulnerability Assessment Security Platform

POLOICT

## Step 2 «Scansione Asset»




**Raccolta ed Analisi Dati** → *Attribuzione Rating* → *Generazione Report*

Modello Dati

| Questionario Organization | Questionario Awareness | Elenco Asset |
|---|---|---|

# Vulnerability Assessment Security Platform

POLOICT

## Step 3 «Vulnerability Assessment ed attribuzione Rating»

Raccolta ed Analisi Dati | **Attribuzione Rating** | Generazione Report

### Sommario dei servizi rilevati per asset

Segue l'elenco tabellare degli asset oggetto di *vulnerability assessment* ed il dettaglio dei servizi rilevati.

| Dettaglio Servizi per Asset | |
|---|---|
| **Numero Asset scansionati** | **Numero Servizi** |
| 1 | 10 |

| Dettaglio Servizi | |
|---|---|
| **Asset principale** | w[redacted].it |
| Asset Web Server | 217.64.195.69 |

| Tipo Servizio | Product/Vendor |
|---|---|
| - | 21/tcp, ProFTPD 1.3.3e |
| - | 25/tcp, Postfix smtpd |
| - | 53/tcp, ISC BIND 9.7.3 |
| - | 80/tcp, Apache httpd |
| - | 110/tcp, Courier pop3d |
| - | 143/tcp, Plesk Courier imapd |
| - | 443/tcp, Apache httpd |
| - | 587/tcp, Postfix smtpd |
| - | 8443/tcp, sw-cp-server httpd (Parallels Plesk WebAdmin version psa-10.4.4-1013111102.18) |

### Sommario delle Vulnerabilità rilevate

Segue l'elenco dettagliato potenziali vulnerabilità rilevate per servizi ed asset.

| Dettaglio Vulnerabilità | |
|---|---|
| **Asset principale** | w[redacted]t |
| Asset Web Server | 217.64.195.69 |

| | | | Tipo di impatto | | |
|---|---|---|---|---|---|
| **Product/Vendor** | **Vulnerabilità** | **Gravità** | **Confidenzialità** | **Integrità** | **Disponibilità** |
| 21/tcp, ProFTPD 1.3.3e | | | | | |
| 25/tcp, Postfix smtpd | | | | | |
| 53/tcp, ISC BIND 9.7.3 | CVE-2015-1349 | media | none | none | complete |
| | CVE-2015-4620 | alta | none | none | complete |
| | CVE-2015-8000 | media | none | none | partial |
| | CVE-2015-8461 | alta | none | none | complete |
| 80/tcp, Apache httpd | | | | | |
| 110/tcp, Courier pop3d | | | | | |
| 143/tcp, Plesk Courier imapd | | | | | |
| 443/tcp, Apache httpd | | | | | |
| 587/tcp, Postfix smtpd | | | | | |
| 8443/tcp, sw-cp-server httpd (Parallels Plesk WebAdmin version psa-10.4.4-1013111102.18) | | | | | |

# Vulnerability Assessment Security Platform

POLOICT

## Step 4 «Reportistica e storicizzazione»

**Risultato**

A seguire è riportato l'esito del vulnerability assessment rispetto agli Asset rilevati. Sono mostrati gli indici di gravità delle vulnerabilità rilevate ed il tipo di impatto che si avrebbe sfruttando tali vulnerabilità.


Fig. 1 - Indice generale report

L'indice generale riassume lo stato degli Asset rispetto alle vulnerabilità rilevate. Il valore è calcolato in una scala tra 0 e 10, dove 0 rappresenta una situazione di esposizione massima e 10 rappresenta una condizione ideale senza vulnerabilità.

Fig. 2 - Livelli di vulnerabilità

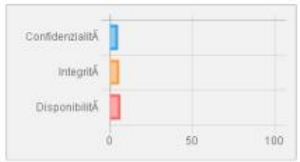



Fig. 3 - Indici CID

| Grave | Medio | Non grave |
|---|---|---|
| 3 | 7 | 4 |

Tab. 1 - Livelli di vulnerabilità

| Confidenzialità | Integrità | Disponibilità |
|---|---|---|
| 5 | 6 | 7 |

Tab. 2 - Risultati tabellari