

ANIE
AUTOMAZIONE

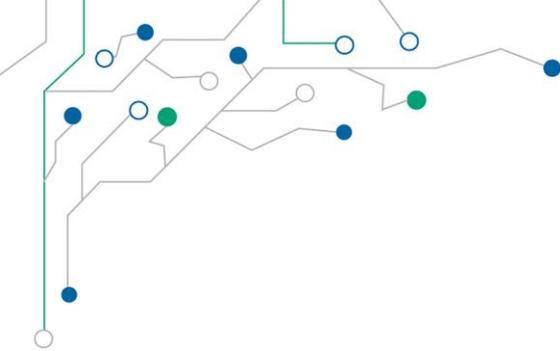


I 4 pilastri del telecontrollo sostenibile

Nicola Zanella

Monitoring & Cloud Services Manager - Elettronica Santerno Spa





1. Sicurezza

Vettori di attacco

- Analisi binari
- Analisi codice sorgente
- Propagazione via mail di codice malevolo
- Tool di intrusione
- Sniffer di rete
- Session hijacking
- Botnet
- Trojan
- Backdoors
- Denial-of-service attack
- Direct-access attacks
- Eavesdropping
- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Privilege escalation
- Exploits
- Social engineering
- Attacchi indiretti
- Spionaggio industriale
- ...

E' difficile trovare un target vulnerabile ?

Shodan Scanhub Developers View All...

SHODAN [Explore](#) [Contact Us](#) [Blog](#) [Enterprise Access](#) [New to Shodan?](#)

[Exploits](#) [Maps](#)

TOP COUNTRIES



Canada	101
United States	69
Spain	18
Serbia	8
Portugal	6

TOP SERVICES

NetBIOS	68
FTP	51
SNMP	42
HTTP	34
Modbus	10

TOP ORGANIZATIONS

Telus Communications	57
Telus Mobility	25
Verizon Wireless	16
Vodafone Spain	7
Telefonica de Espana	4

Showing results 1 - 10 of 292

96.1.64.209
Telus Communications
 Added on 2015-07-24 02:36:32 GMT
 🇨🇦 Canada
[Details](#)

Linux 174 **SCADA** 2.6.27 #1 Thu Jun 13 09:26:49 MDT 2013 armv5tej1 IPn3G.00:0F:92:00:C3:29

46.26.212.35
Vodafone Spain
 Added on 2015-07-23 07:26:02 GMT
 🇪🇸 Spain, Terrassa
[Details](#)

NetBIOS Response
 Servername: PC-**SCADA**
 MAC: a4:1f:72:54:72:af

Names:
 PC-**SCADA** <0x0>
 GRUPO_TRABAJO <0x0>
 PC-**SCADA** <0x20>
 GRUPO_TRABAJO <0x1e>
 GRUPO_TRABAJO <0x1d>
 __MSBROWSE__ <0x1>

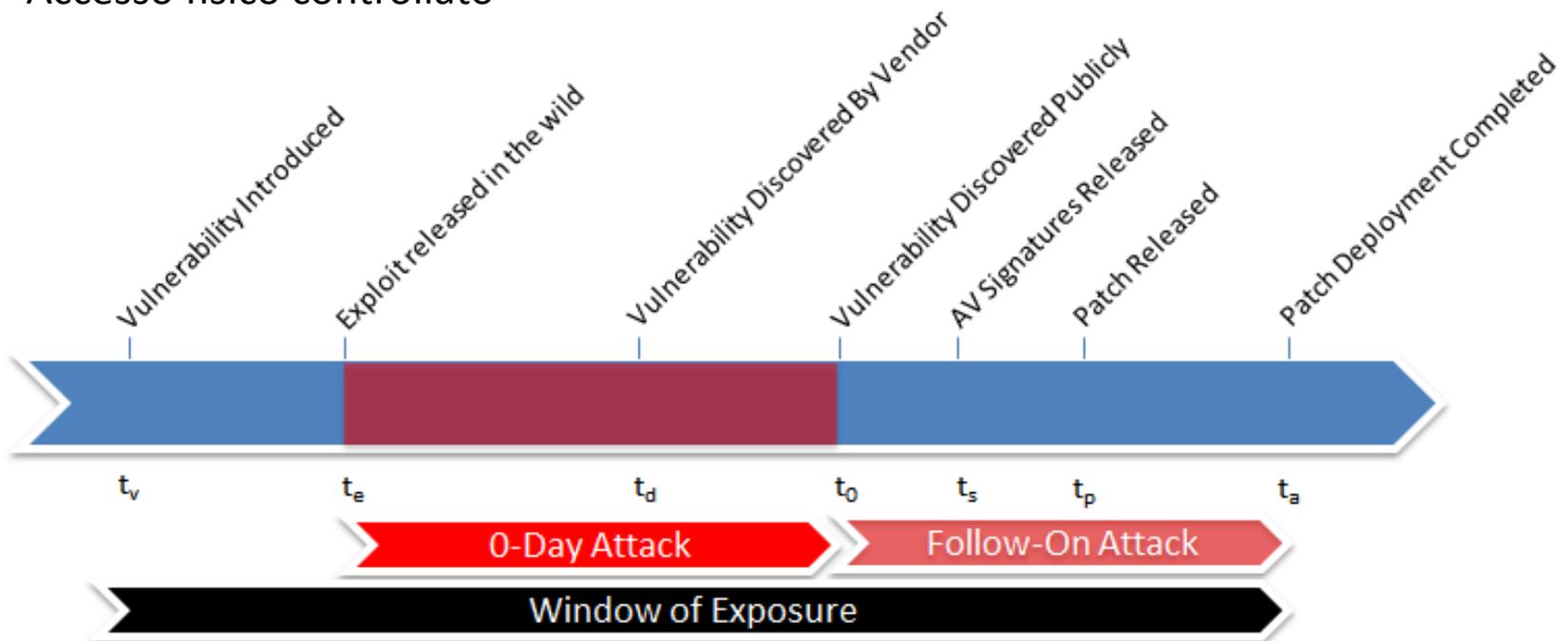
Web Scada
 212.69.20.109
Društvo za telekomunikacije Orion telekom doo Beog
 Added on 2015-07-22 16:17:11 GMT
 🇷🇸 Serbia, Beograd
[Details](#)

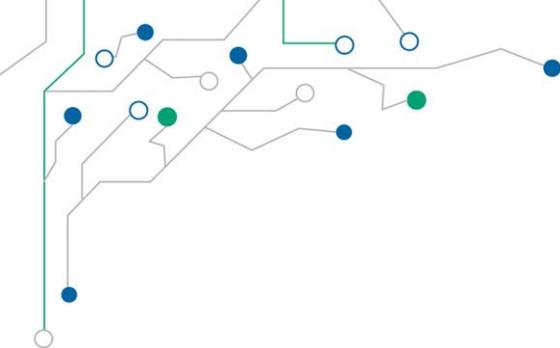
HTTP/1.0 200 OK
 Server: INDAS WEB **SCADA**
 Content-Type: text/html
 Accept-Ranges: bytes
 Content-Length: 4673

Prodotto o processo?

- Sistemi aggiornati all'ultima release
- Firewall attivi
- Password non indovinabili
- Accesso fisico controllato

0-day attack



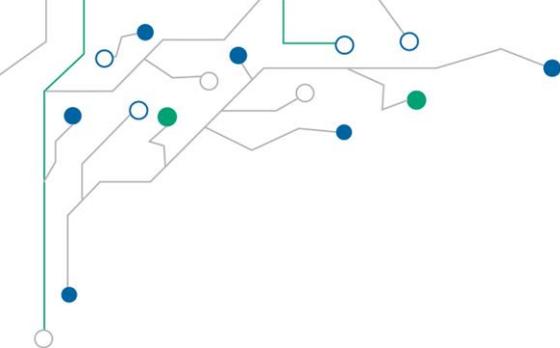


Finalità del processo

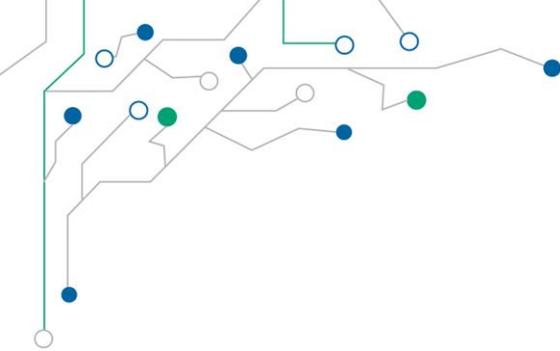
Obiettivo: creare una
cultura condivisa della
sicurezza

Accessi, networking,
storage, applicazioni





2. Operatività remota

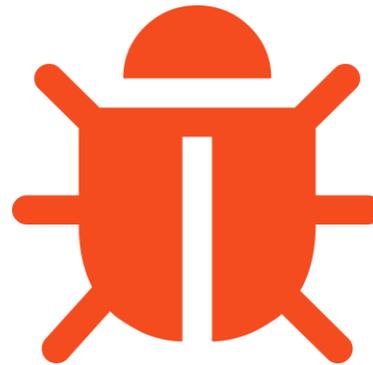


Controllo totale



Update

Sell & Forget non esiste più
Un mondo sempre più
connesso richiede la
capacità di evolvere nel
tempo, soprattutto in
contesti IoT



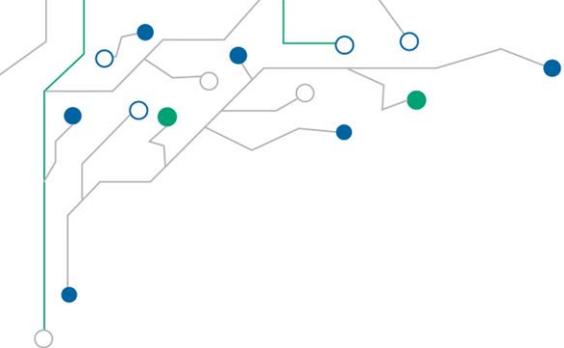
Debug

Individuazione rapida dei
problemi, per avere massima
velocità nei tempi di
intervento e quindi minimo
down time



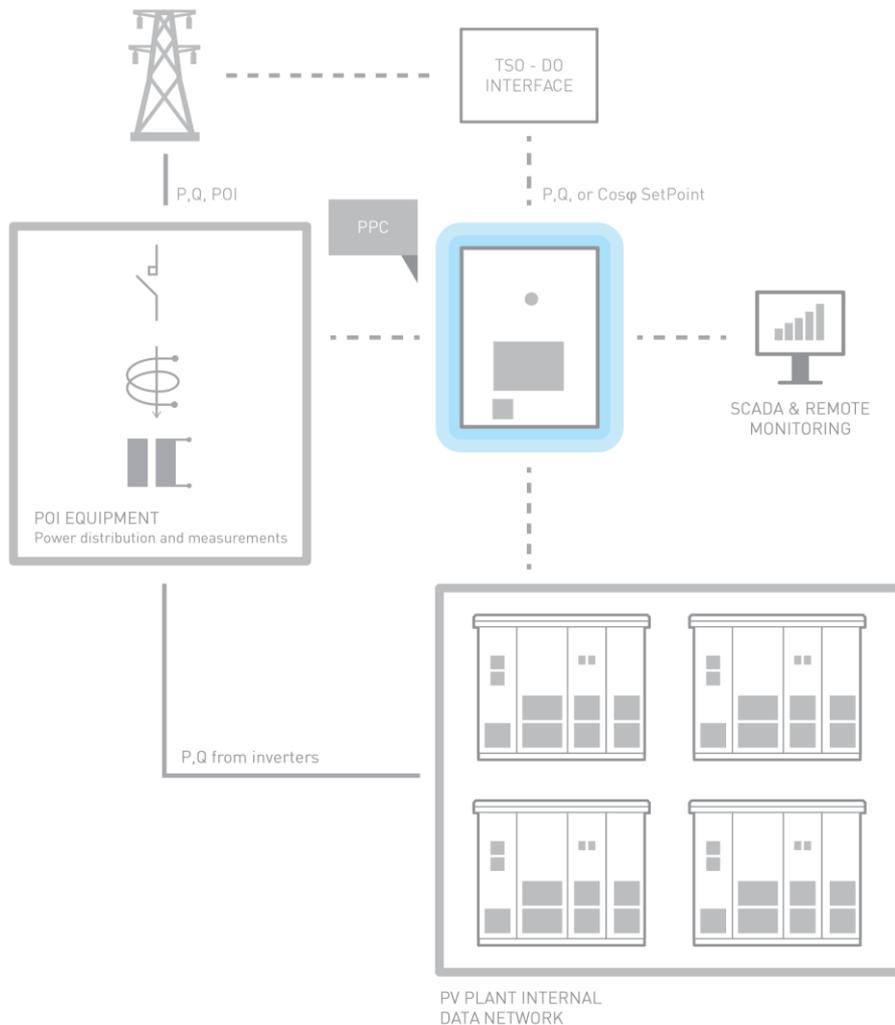
Deploy

Sempre più automatizzato
e parallelo, per assicurare
aggiornamenti distribuiti
e tempestivi



3. Controllo della generazione dell'energia

Power Plant Controller

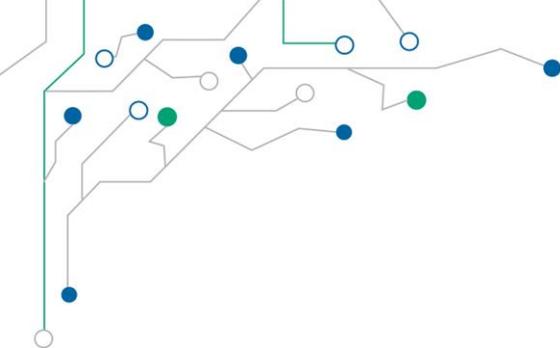


Controllo al POI

Setpoint locale o remoto

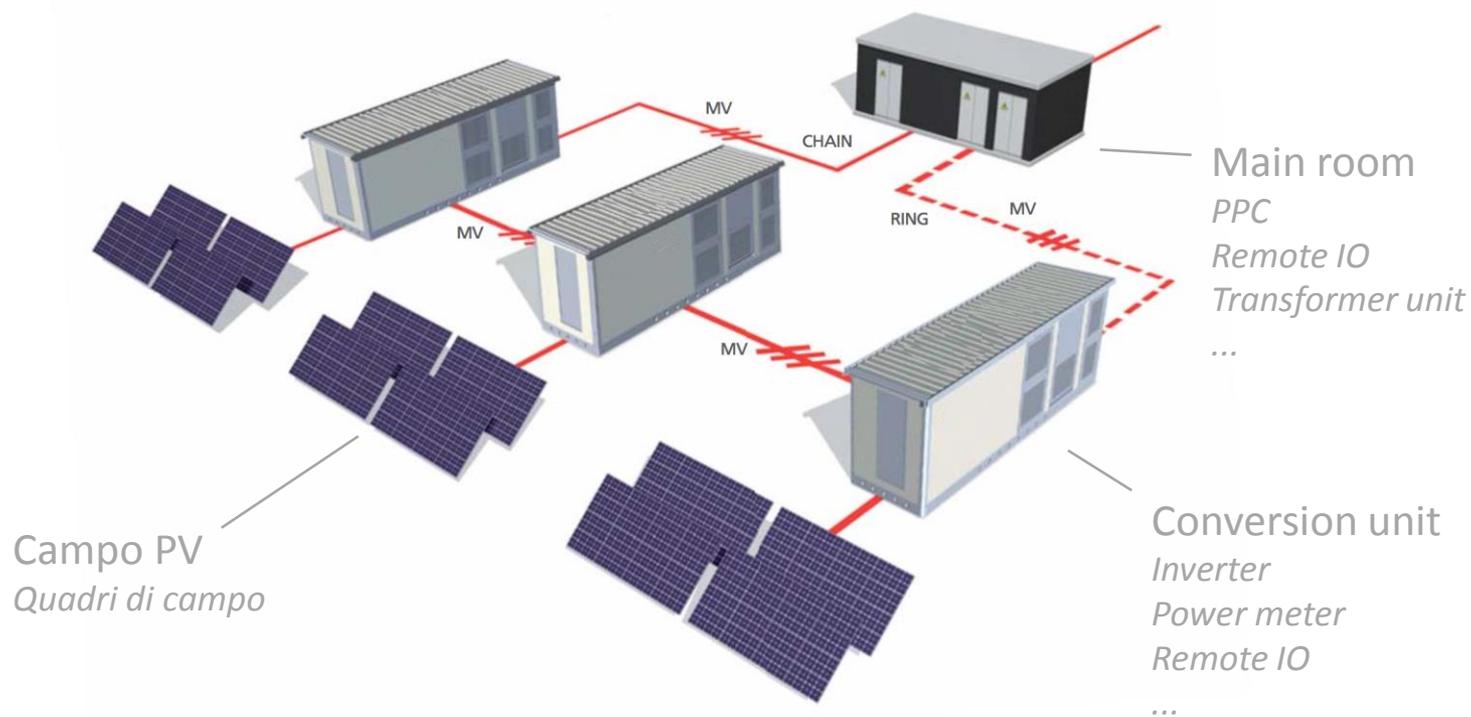
Modalità di controllo:

- Potenza attiva
- Potenza reattiva
- Fattore di potenza ($\cos \phi$)
- Tensione



4. Analisi dei dati

PV Utility scale



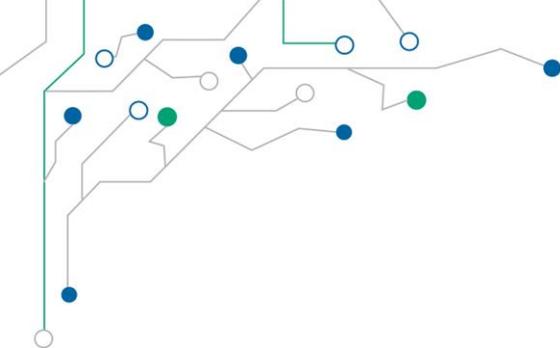
Un impianto da 80MW produce circa 10 milioni di dati al giorno

Metodi ed obiettivi

- Estrarre e graficare i dati chiave
- Cercare relazioni tra i dati di device dello stesso tipo nello stesso impianto
- Confrontare device di tipo simile in impianti diversi
- Applicare i punti 1-2-3 su tutto l'arco temporale di vita monitorato dell'impianto



- Visione sinottica
- Performance e uptime
- Affidabilità dei componenti
- Manutenzione predittiva



Grazie

nicola.zanella@santerno.com

www.santerno.com

www.sunwayportal.it