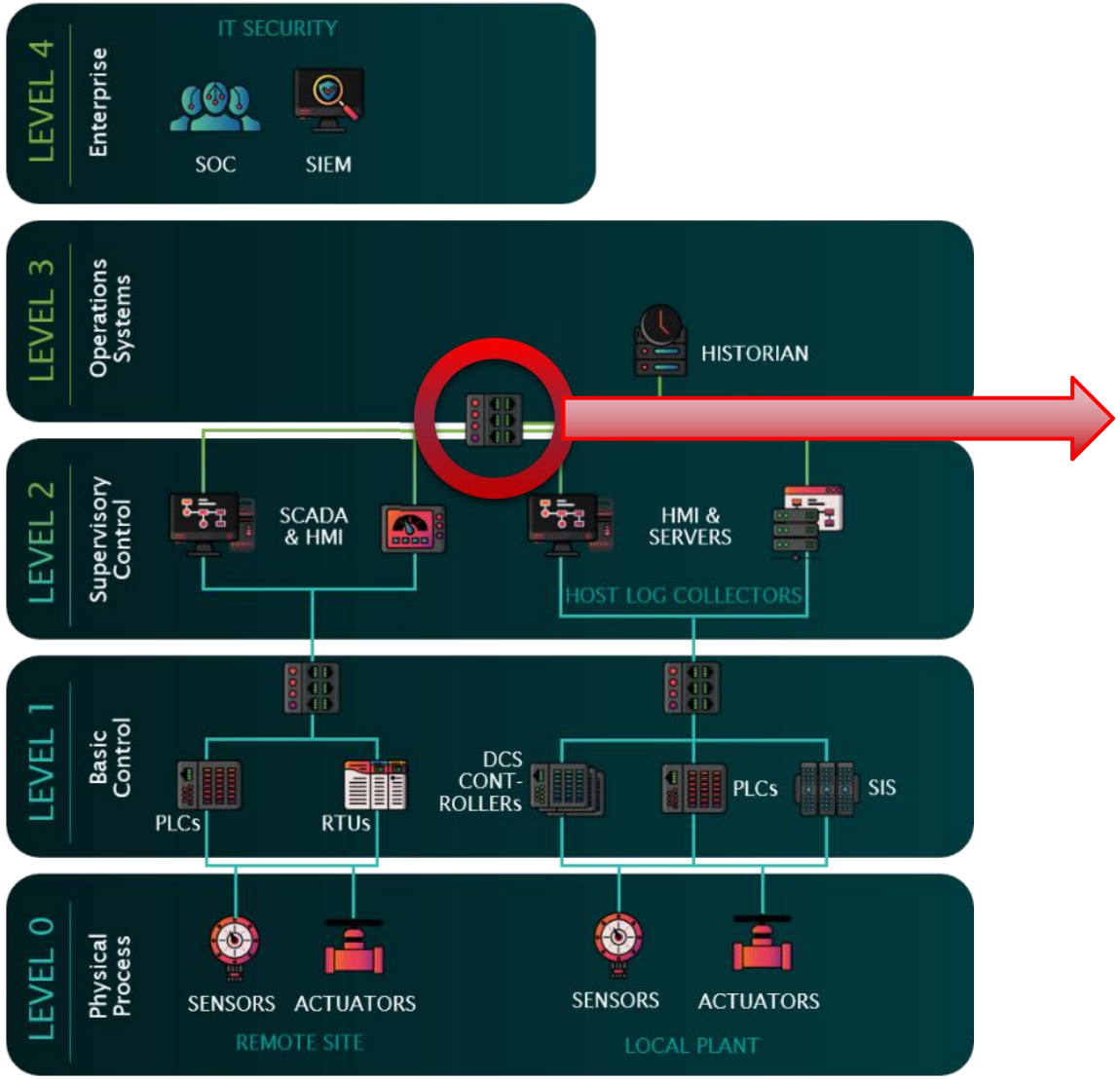
Arquitecturas Defendibles en ICS/OT

Diego Espitia

Ingeniero Electrónico de Profesión.
Hacker por Pasión

@ dsespitia

Estructuras de Red en ICS

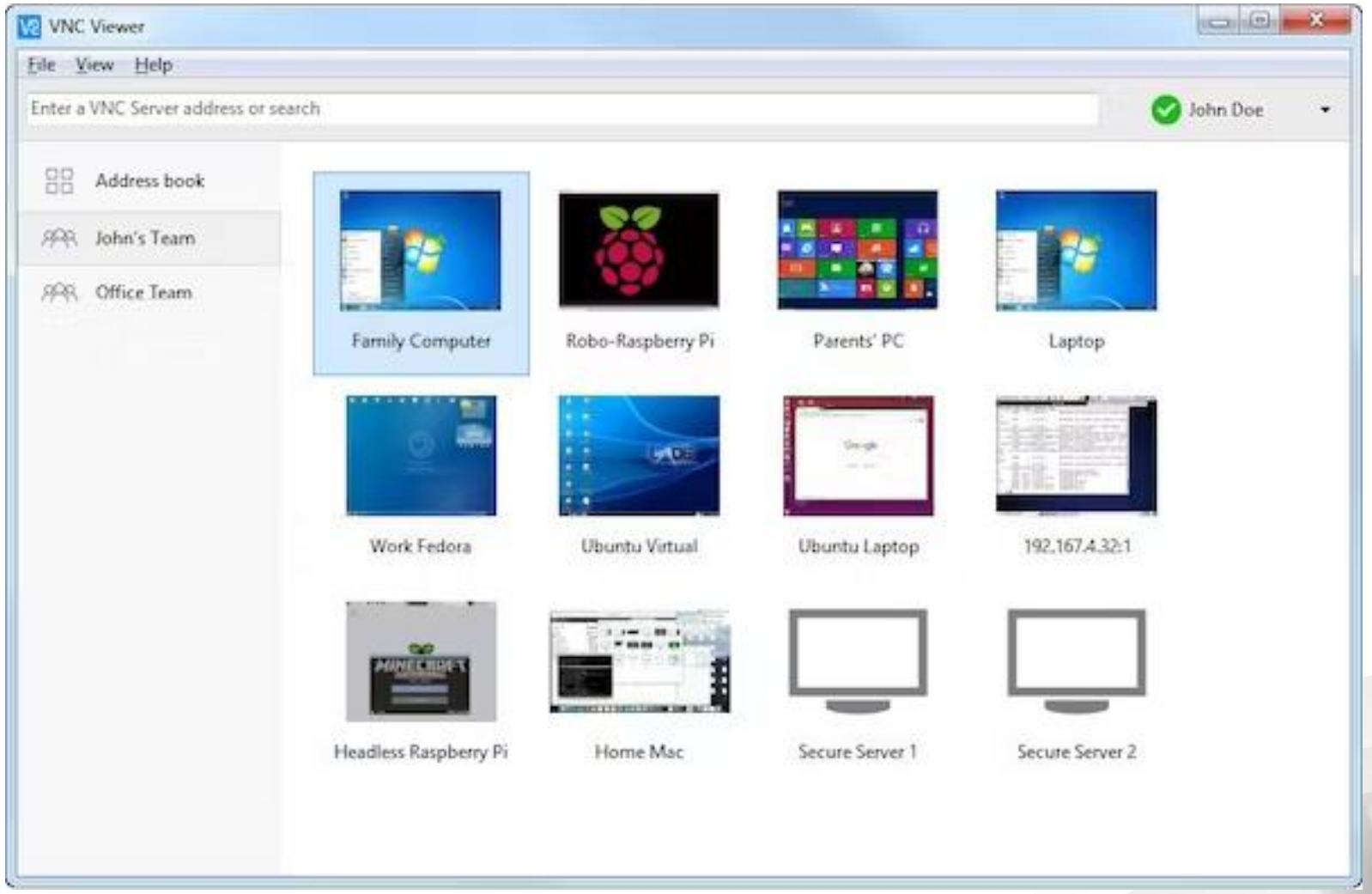


¿Lo pueden conectar desde cualquier segmento de la red corporativa?

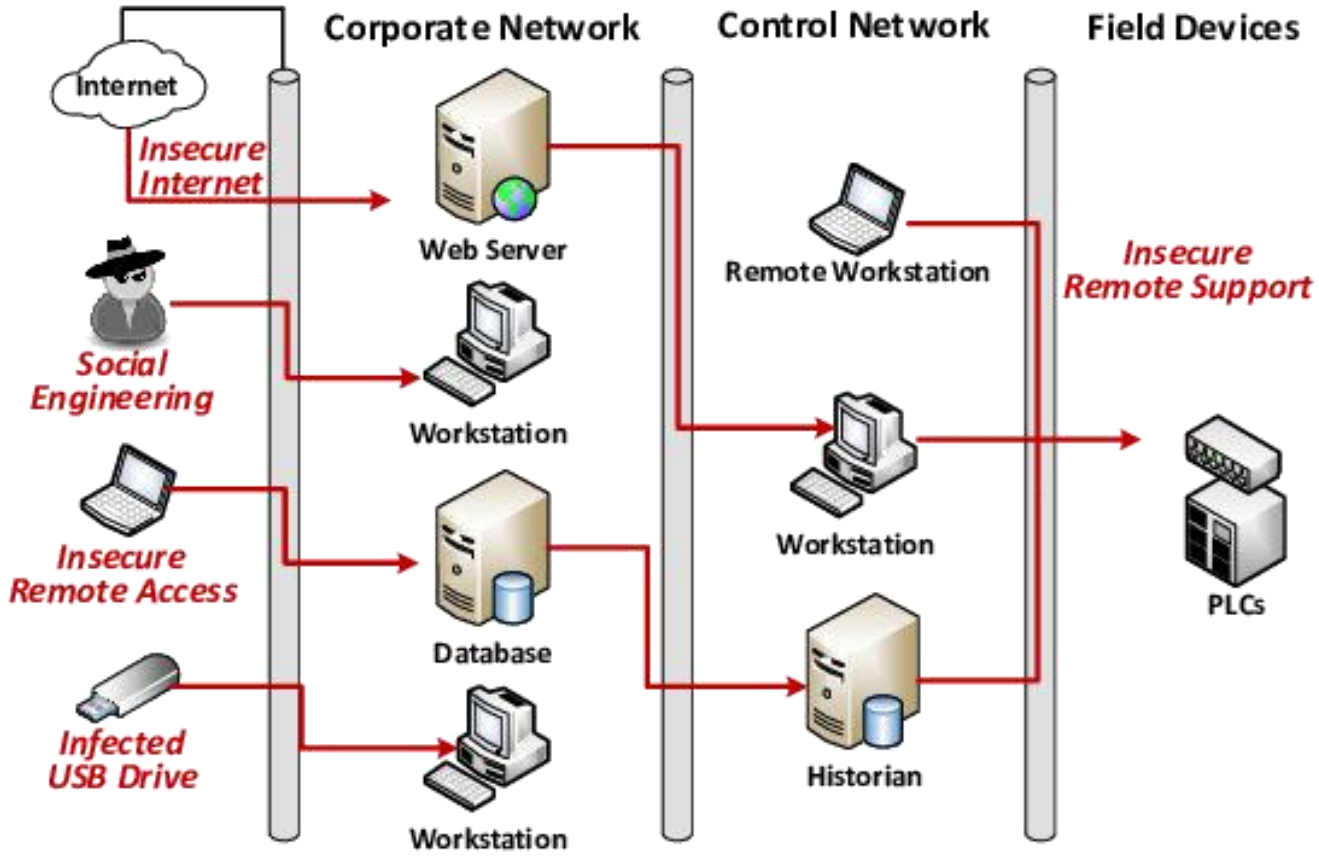
¿Tiene controles de acceso seguros?

¿Cómo accede a los servidores de las redes industriales?

Desde el Pivote



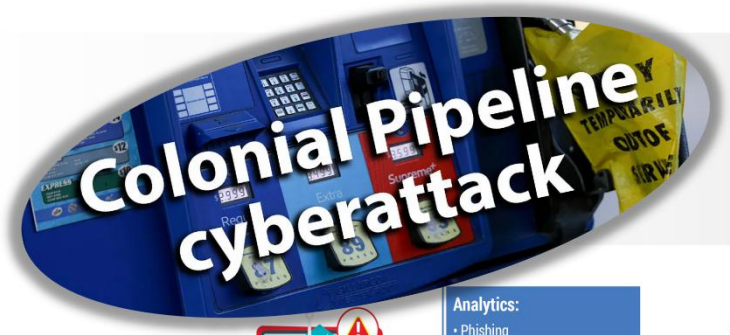
Consecuencias

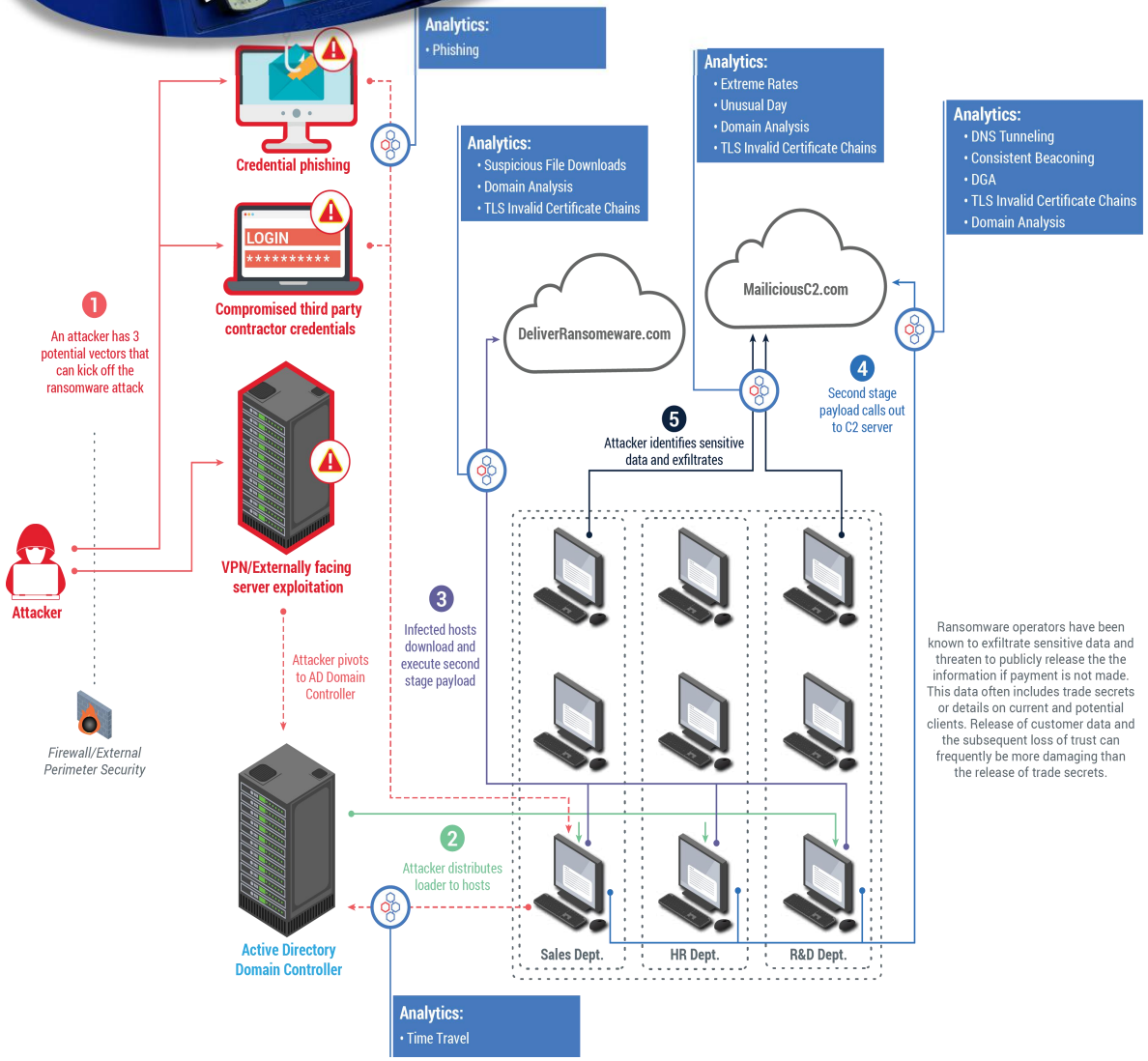


Incidentes internos que se propagan rapidamente.

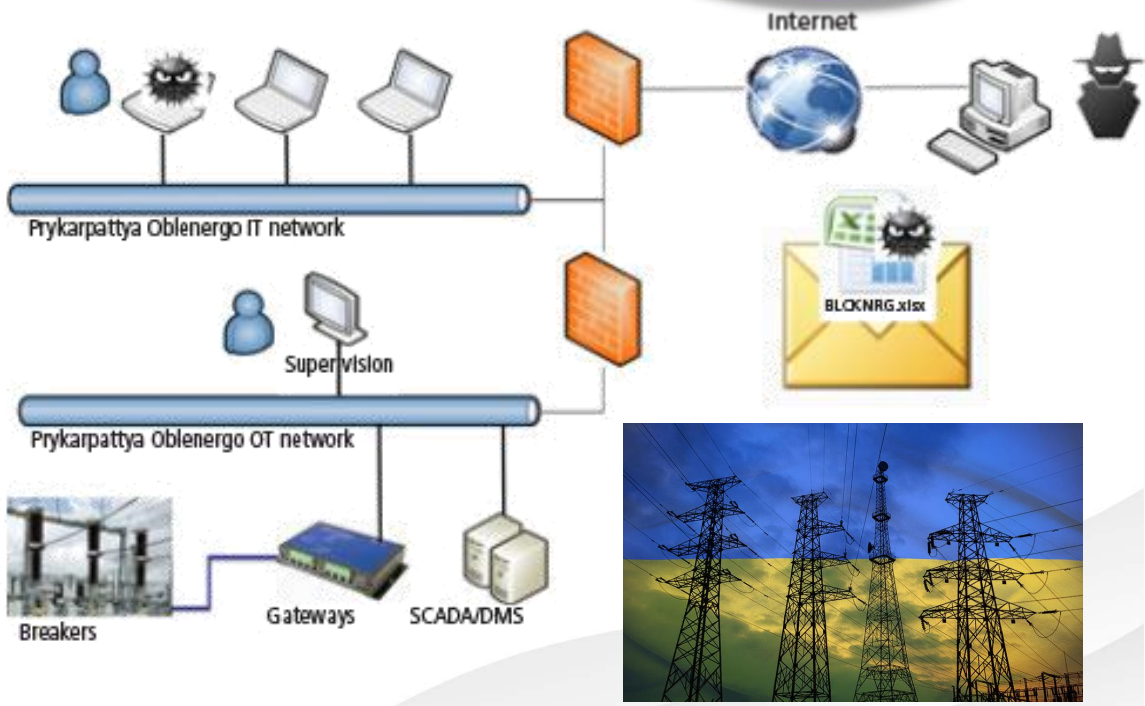
Ataques tienen varios mecanismos para afectar OT.

La recuperación de un incidente es muy complejo.

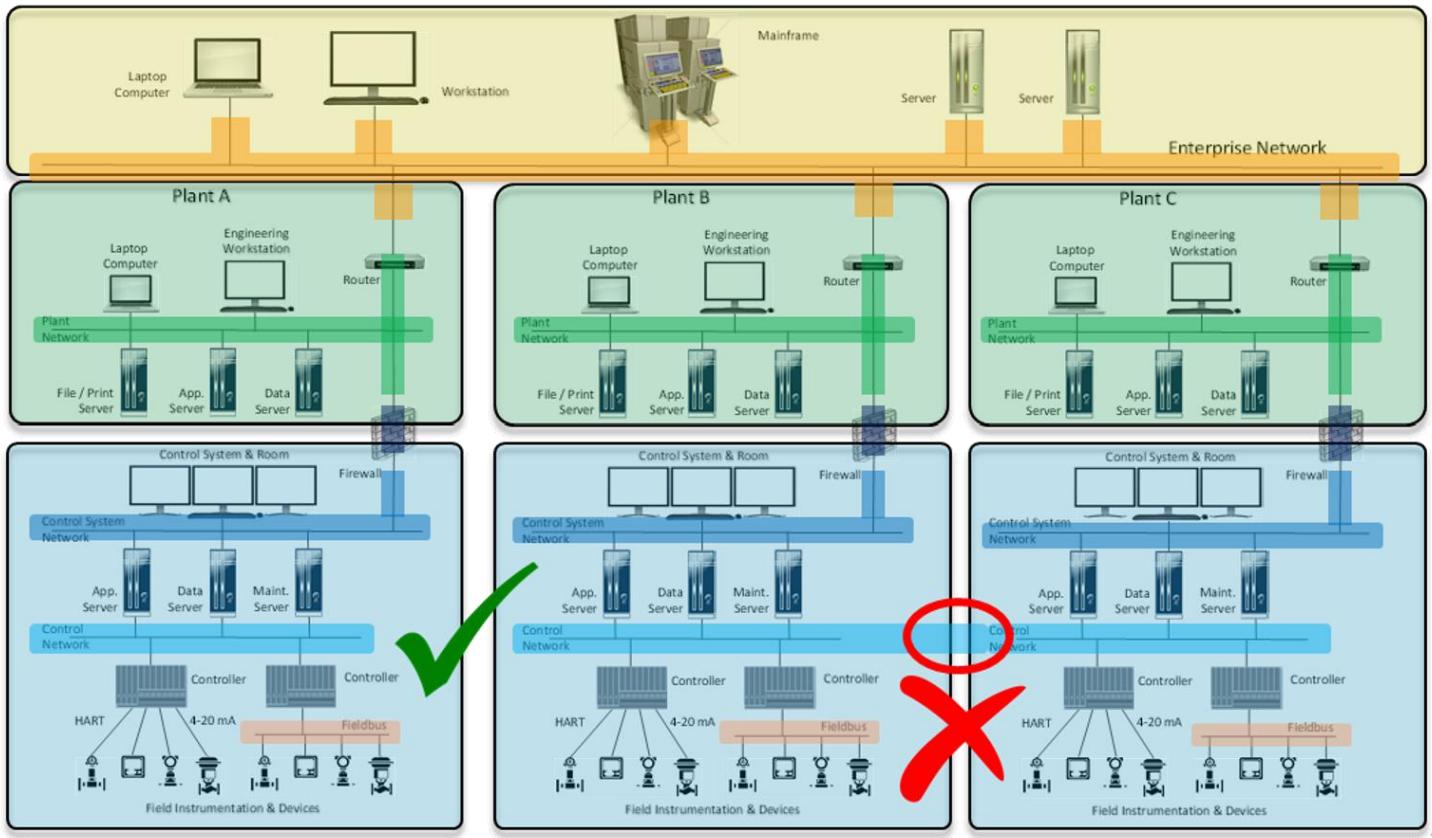

Colonial Pipeline
cyberattack


Analytics:
• Phishing
Credential phishing
LOGIN
****
Compromised third party contractor credentials
1
An attacker has 3 potential vectors that can kick off the ransomware attack
VPN/Externally facing server exploitation
Attacker
Firewall/External Perimeter Security
Attacker pivots to AD Domain Controller
Active Directory Domain Controller
Analytics:
• Suspicious File Downloads
• Domain Analysis
• TLS Invalid Certificate Chains
DeliverRansomeware.com
Analytics:
• Extreme Rates
• Unusual Day
• Domain Analysis
• TLS Invalid Certificate Chains
MailiciousC2.com
Analytics:
• DNS Tunneling
• Consistent Beaconing
• DGA
• TLS Invalid Certificate Chains
• Domain Analysis
4
Second stage payload calls out to C2 server
5
Attacker identifies sensitive data and exfiltrates
3
Infected hosts download and execute second stage payload
2
Attacker distributes loader to hosts
Sales Dept.
HR Dept.
R&D Dept.
Analytics:
• Time Travel
Ransomware operators have been known to exfiltrate sensitive data and threaten to publicly release the the information if payment is not made. This data often includes trade secrets or details on current and potential clients. Release of customer data and the subsequent loss of trust can frequently be more damaging than the release of trade secrets.

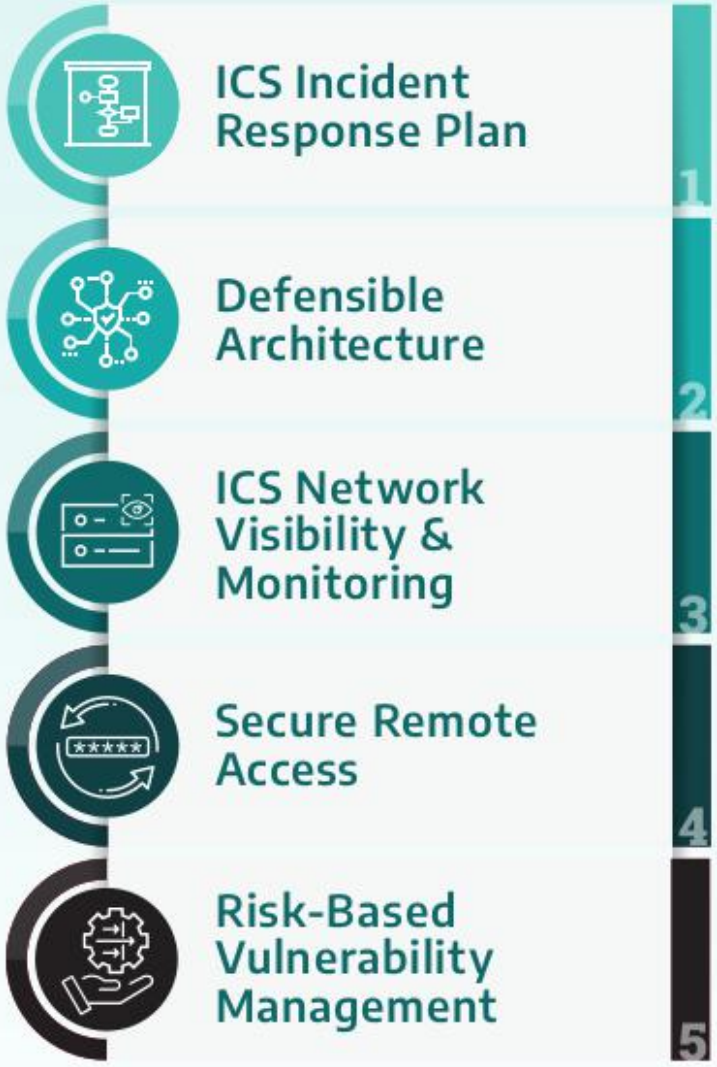

UKRAINIAN
POWER GRID
HACKED

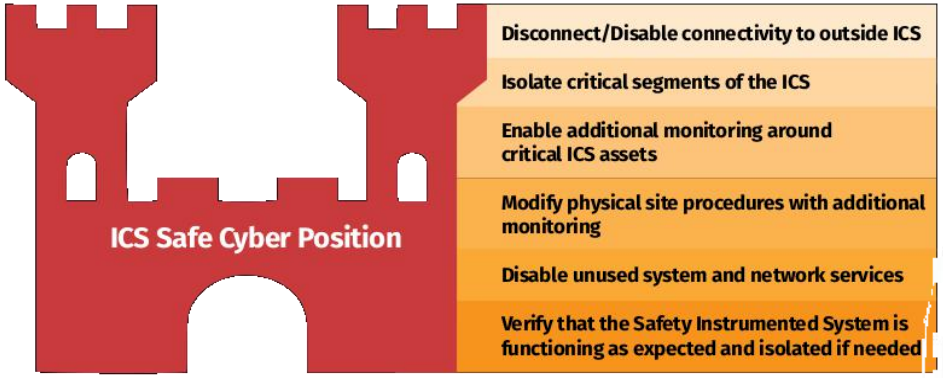

Internet
Prykarpattya Oblenergo IT network
Supervision
Prykarpattya Oblenergo OT network
BLCKNRG.xlsx
Breakers
Gateways
SCADA/DMS

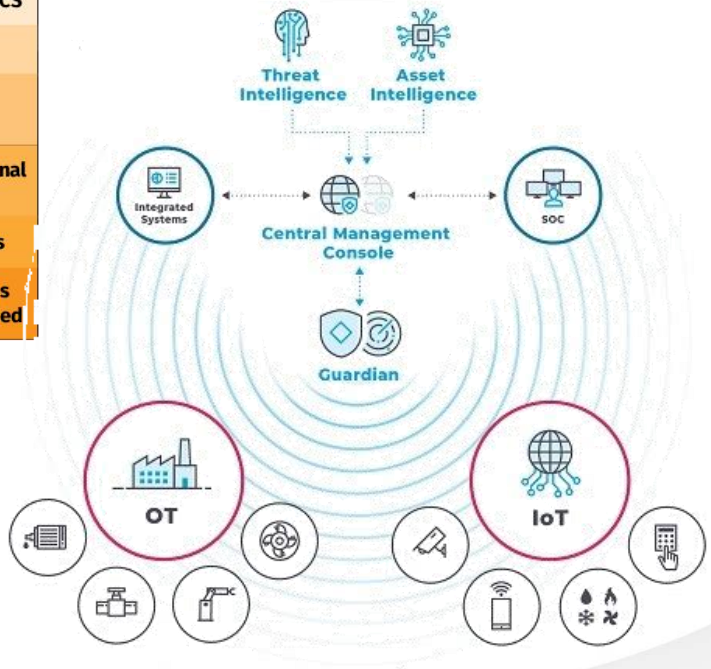
¿Qué dicen los estandares?

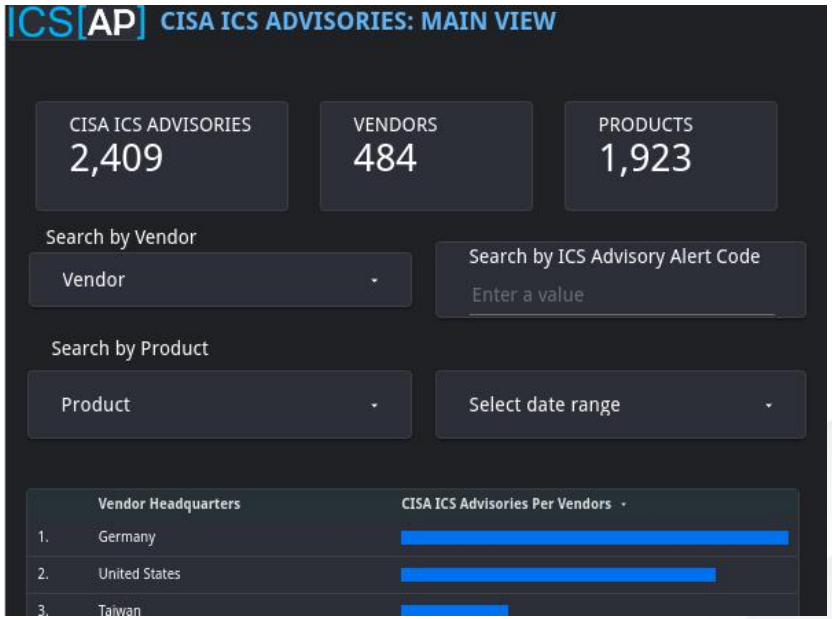


Controles Críticos

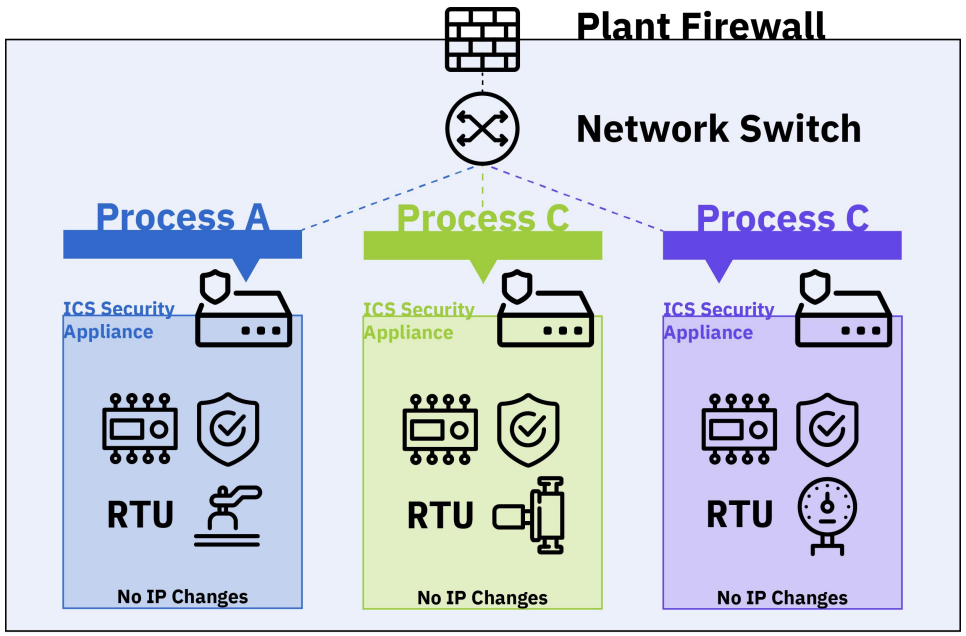








Aplicando Controles

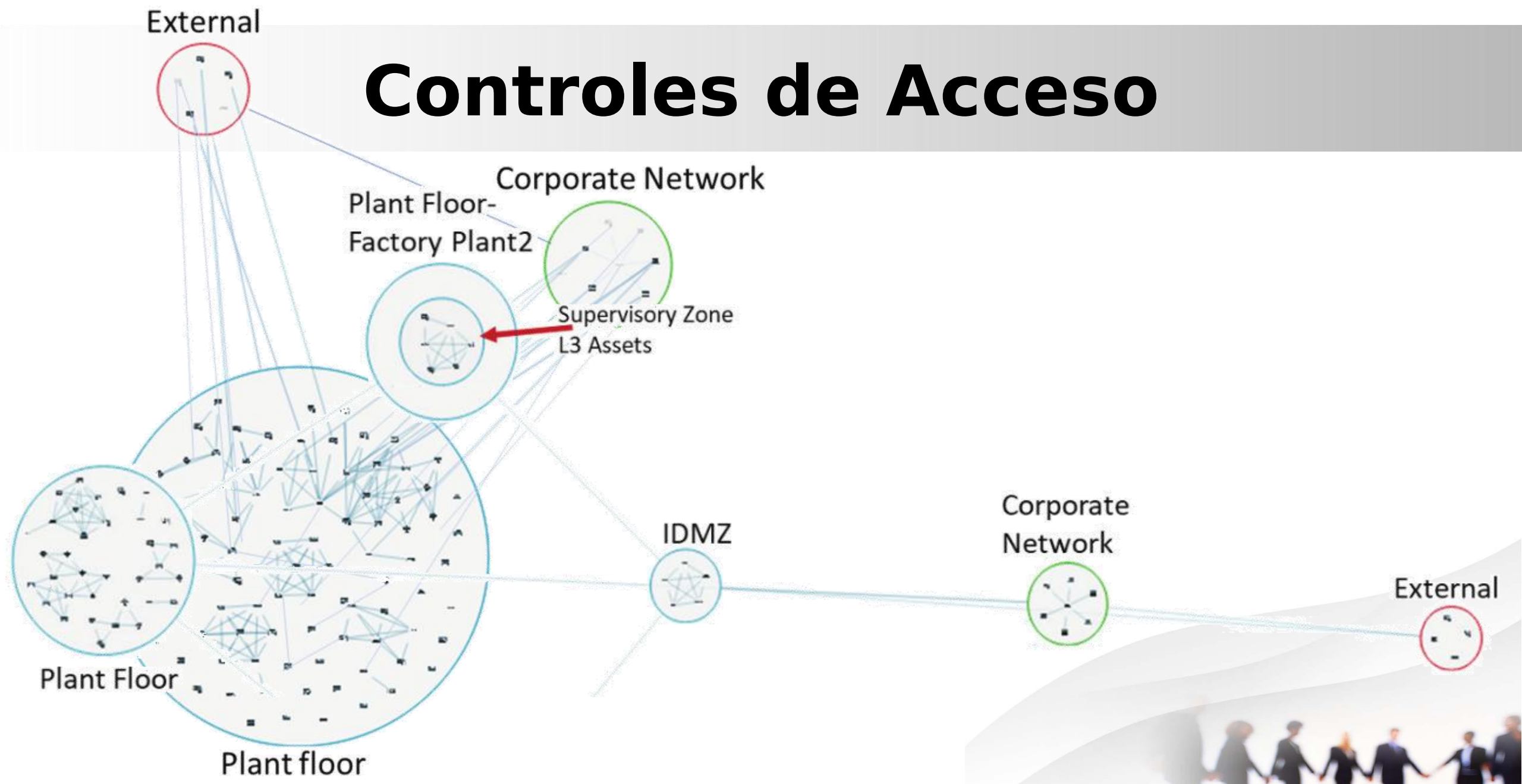


identification

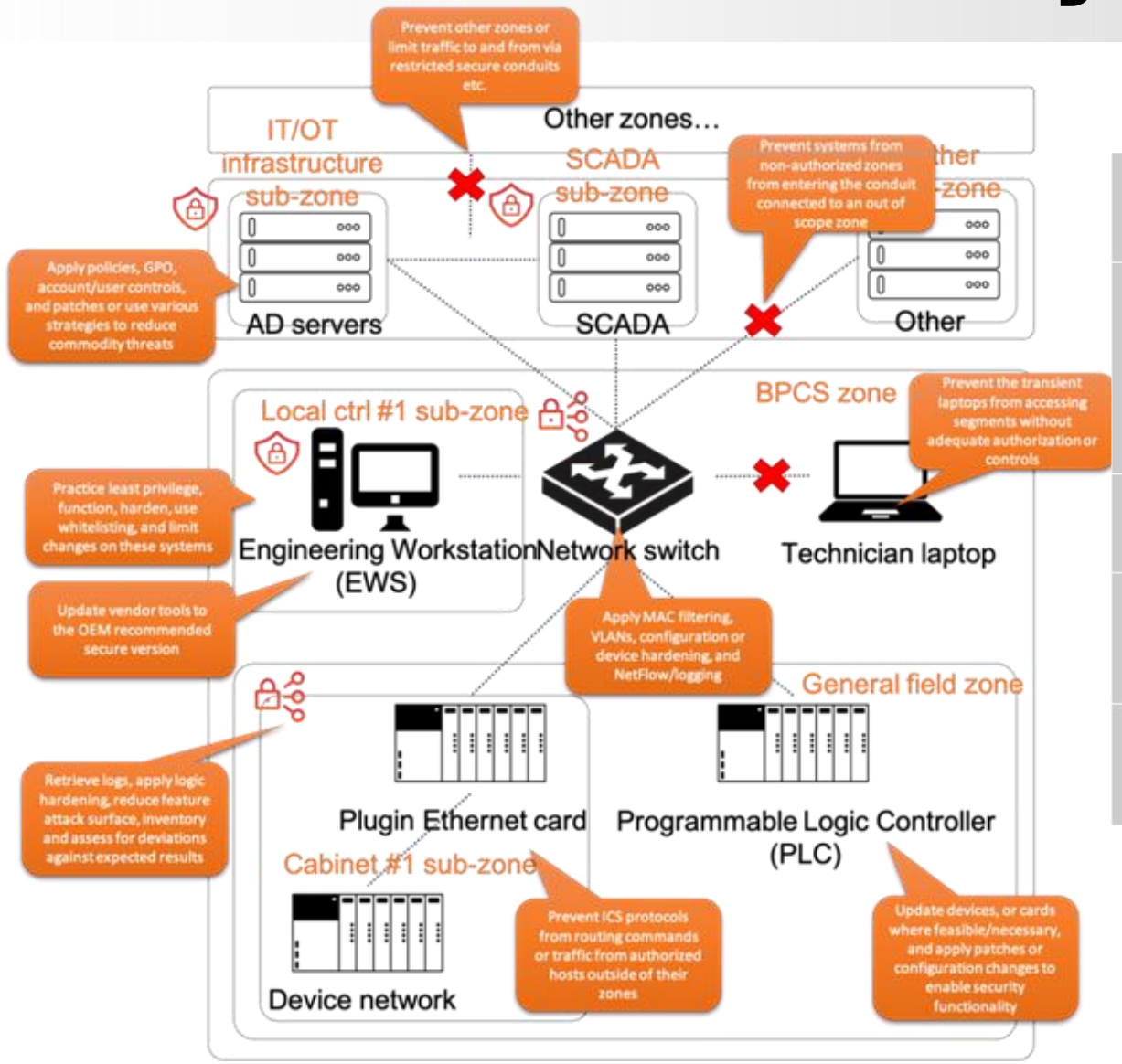
authentication

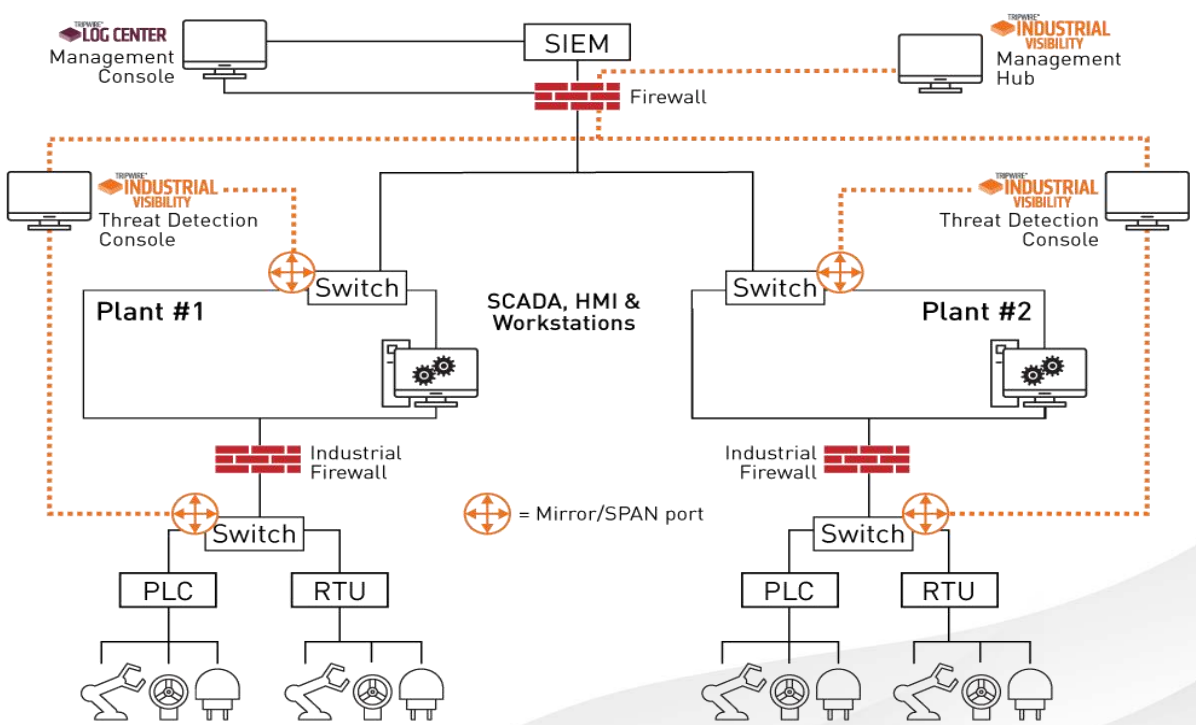
authorization

Controles de Acceso

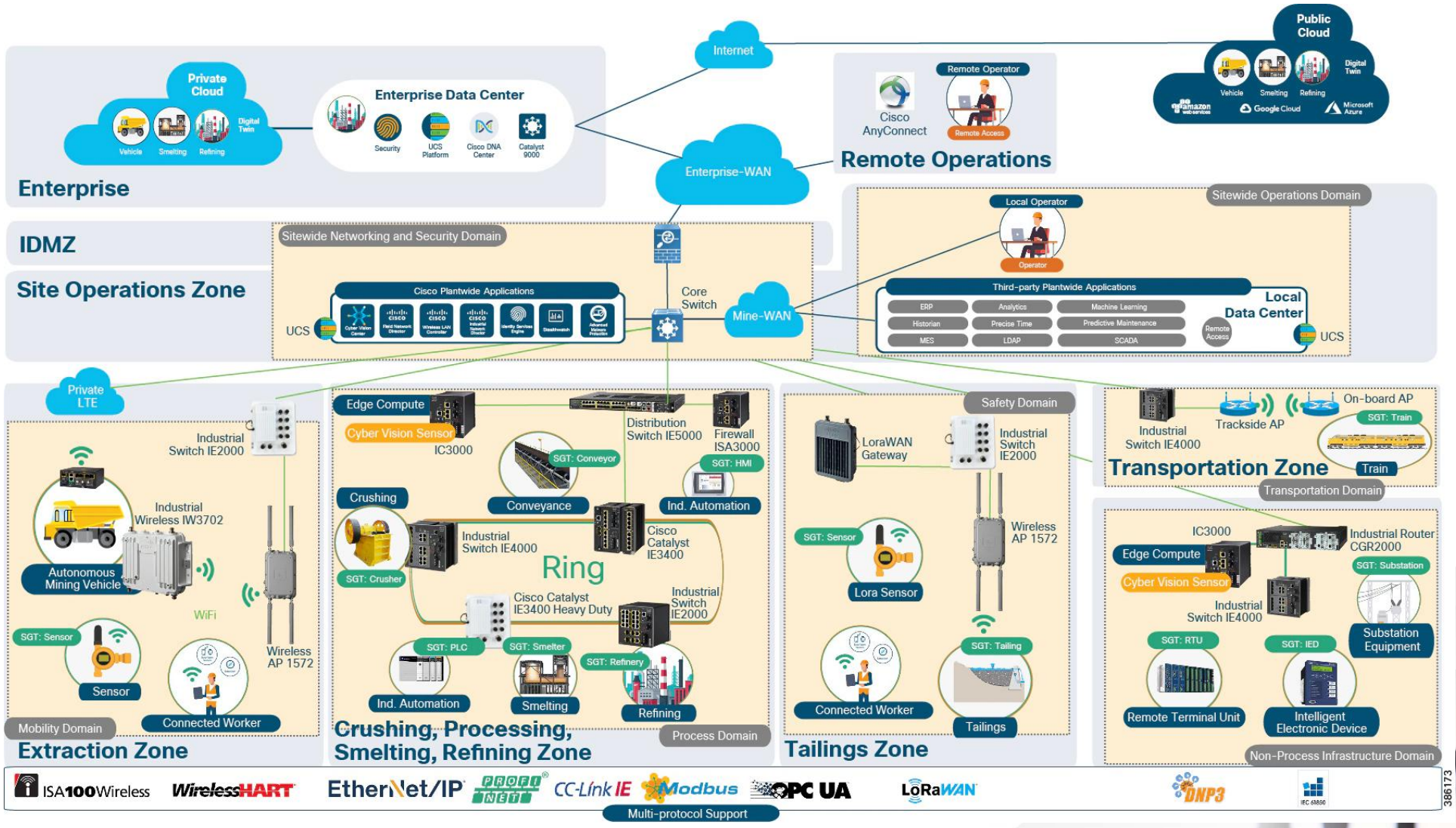


Monitoreo y Visualización

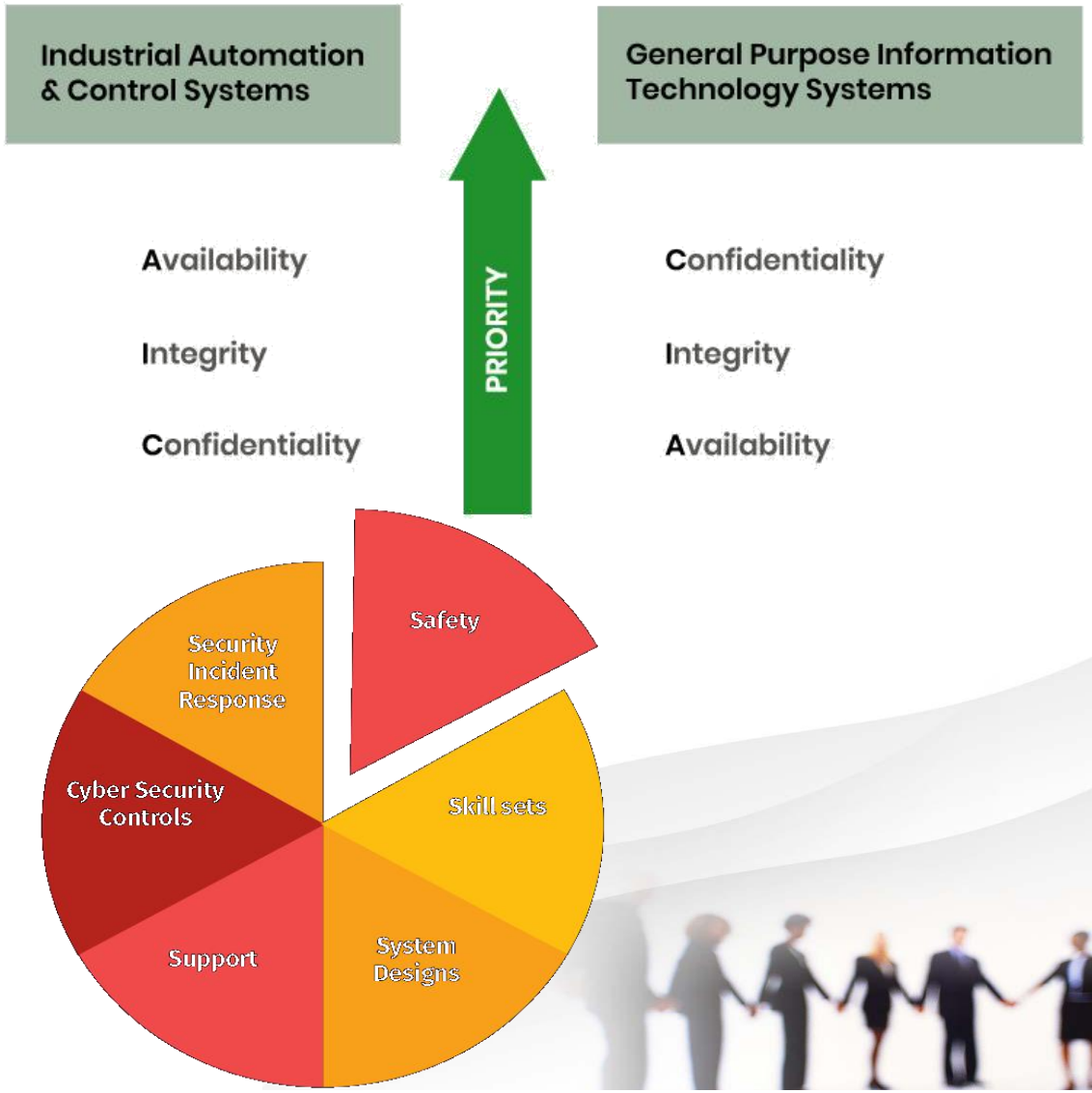




Conexiones y Protocolos



Respuesta de Incidentes



GRACIAS

¿Preguntas?