Cybsec by Deloitte.

Cyber-Resilience in Organizations

Julio Ardita – Cybsec by Deloitte - jardita@deloitte.com

Agenda

1 – Cyber-Resilience

2 – Incident prevention

3 – Incident Management

4 - Conclusions

Cybsec by Deloitte.

Agenda

1 – Cyber-Resilience

2 – Incident prevention

3 – Incident management

4 - Conclusions

Cyber-Resilience in Organizations

Cybsec by Deloitte.

Cyber-resilience is an inherent attribute of an organism, entity, corporation or state that allows facing a cybersecurity crisis without affecting any activity.

It is the management of technological threats so that it is possible to effectively manage cyber attacks using cybersecurity incident prevention and management methodologies.

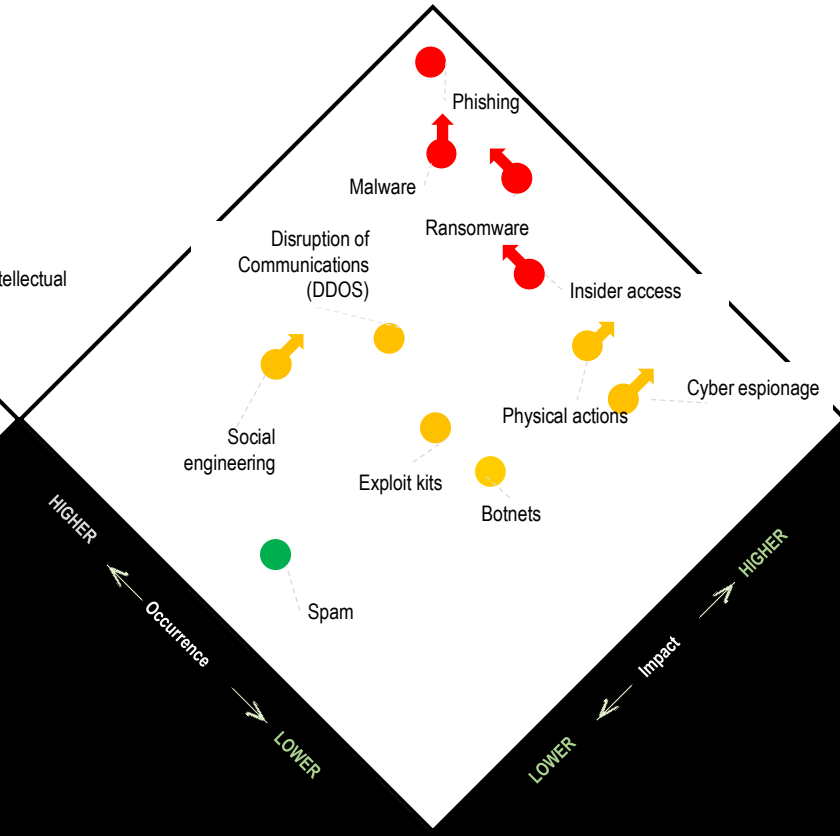
Cyber-Resilience in Organizations

Cybsec by Deloitte.

The oil and gas industry has improved their productivity by digitalization of their operational processes, however this has opened the enterprise to a whole new array of cyber risks

TOP THREAT SCENARIOS

TOP ATTACK VECTORS



TOP ADVERSARY GROUPS

NOTABLE CYBER SECURITY EVENTS

- DragonFly 2.0/Energetic bear targets US power grid
- North Korean threat actor targets US power grid's ICS sys
- Irelands electrical supply board was targeted
- Multiple south east Asian oil companies targeted by Chinese state sponsored threat actor (NAIKON Team)

KEY TAKEAWAYS

Nation state actors appear to be more active in the energy and resources sector compared to other industries. Initial attack vector normally stays consistent with being initiated well crafted phishing campaigns. Energy and resources sector consist of numerous SCADA systems that are associated with subcomponents that are interconnected together and if one is compromised that can lead to disruptions trough out the industry.

Cybsec by Deloitte.

State-of-the-art in industrial cybersecurity

- Few relationships between IS and the engineer and industrial network operations areas.
- There is more interconnection between industrial networks and corporate networks and the Internet.
- System updates: legacy systems that are upgraded to new versions with new embedded technologies (open system, web, java, etc.).
- Lack of knowledge in technical security aspects.

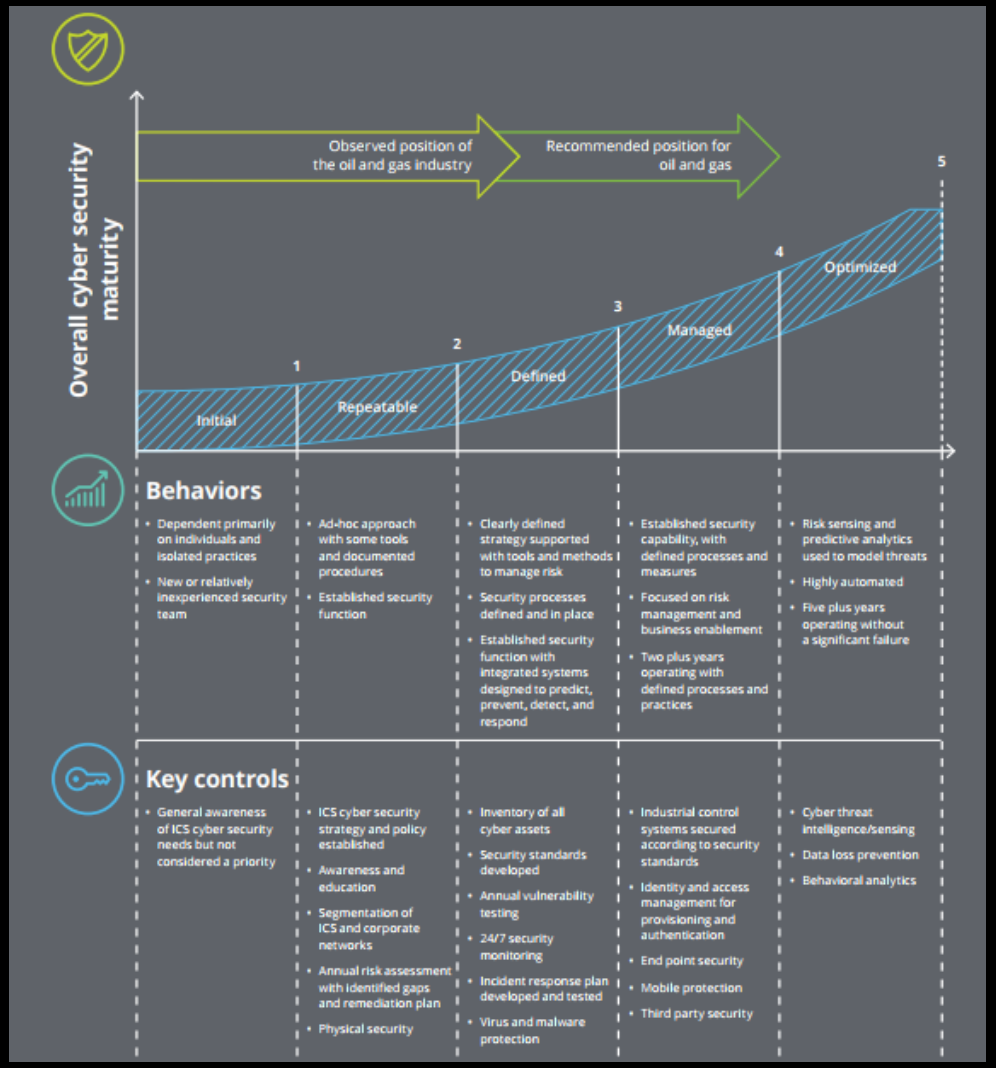
Cybsec by Deloitte.

State-of-the-art in industrial cybersecurity

- Security awareness among local engineers, local representatives and some international providers is far too low.
- Savings in costs and easy operation of security issues.
- Remote accesses for administrative and provider access.

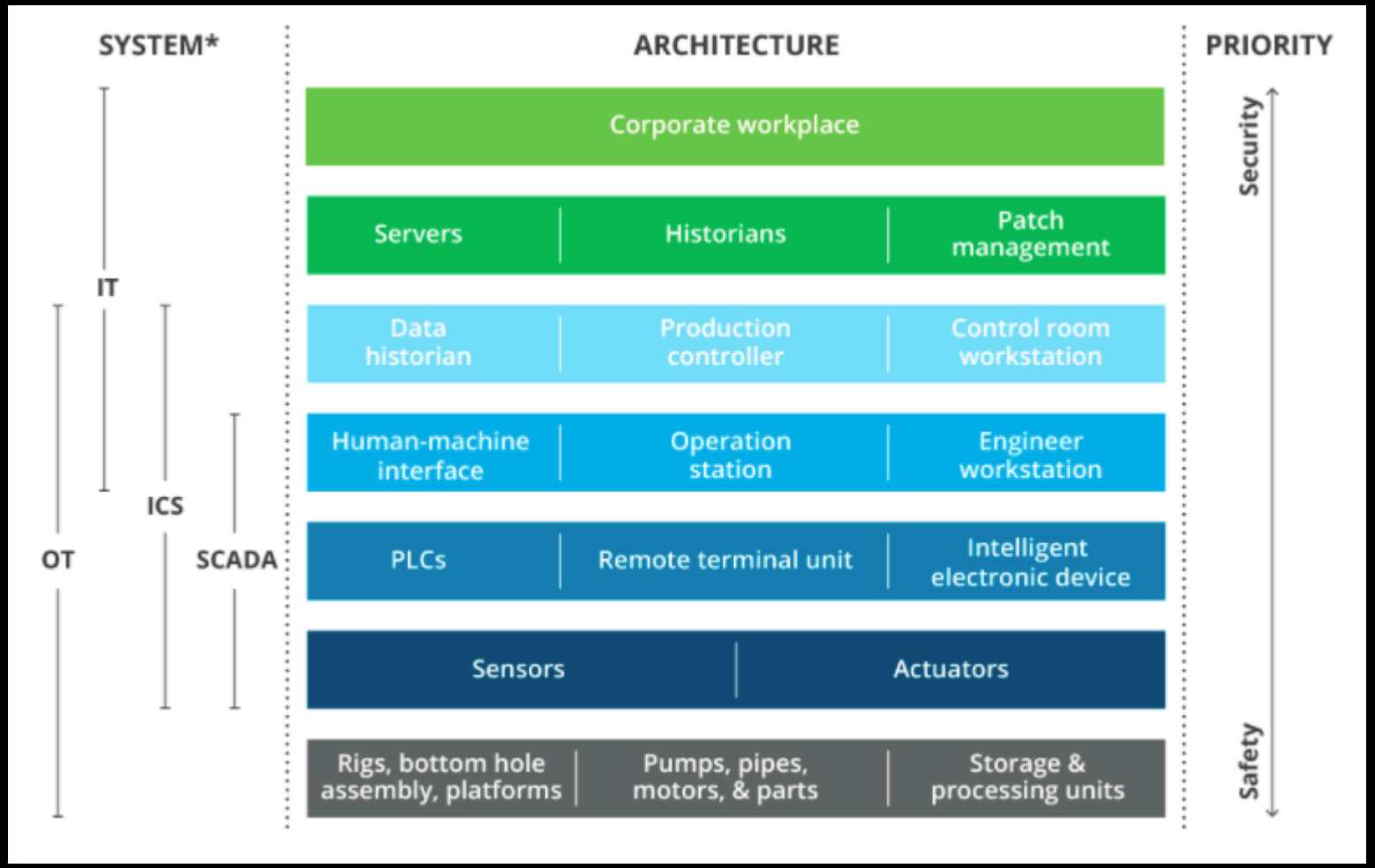
Cybsec by Deloitte.

State-of-the-art in industrial cybersecurity



Cybsec by Deloitte.

State-of-the-art in industrial cybersecurity



Cybsec by Deloitte.

Cyber Threat in the Oli&Gas

Upstream

Exploration

- Geophysical evaluation and design
- Field development
- Drilling operations

Upstream scenario #1:
Misappropriation of commercially sensitive reservoir performance and well data

Risk: Damage to the operator's competitive position in a play or field

Production

- Bringing the oil to the surface

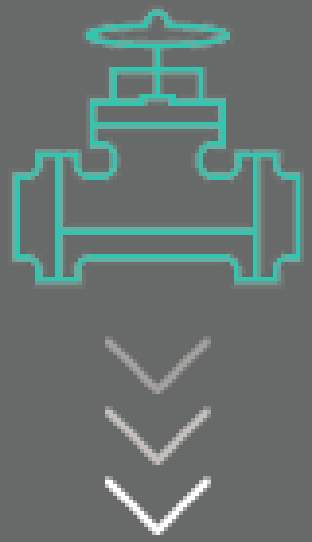
Upstream scenario #2:
Key well-control and safety equipment is pushed outside normal operating parameters or shut down completely

Risk: Operational shutdown and financial loss, as well as field safety incidents, due to equipment malfunction

Cybsec by Deloitte.

Cyber Threat in the Oli&Gas

Midstream



Transportation

- Gathering and transporting—pipelines, tankers, trucks

Midstream scenario #1:
Unauthorized access to and manipulation of pipelines systems

Risk: Explosion, spillage, environmental, damage, and unsafe conditions for personnel and adjacent populations

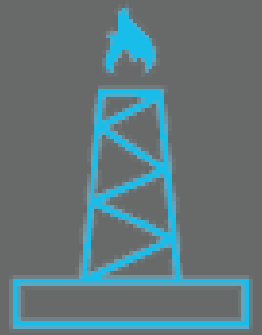
Midstream scenario #2:
Monitoring is distorted or interrupted, thus compromising equipment integrity

Risk: Shutdown of system for investigation, resulting in missed shipments and financial loss

Cybsec by Deloitte.

Cyber Threat in the Oli&Gas

Downstream

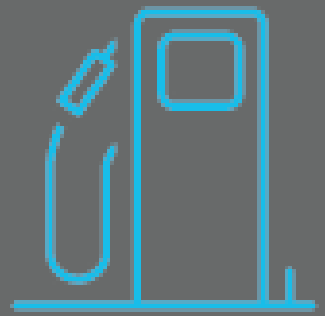


Refining

- Processing of crude oil into petroleum products
- Product blending

Downstream scenario #1:
Theft of inventory data on crude oil and refined products

Risk: Failure to meet business commitments and reputation damage



Marketing

- Retailing
- Trading

Downstream scenario #2:
Interruption or tampering with operational controls

Risk: Unsafe operating conditions and downtime, leading to supply disruption and revenue loss

Cybsec by Deloitte.

Agenda

1 – Cyber-Resilience

2 – Incident prevention

3 – Incident management

4 - Conclusions

Cybsec by Deloitte.

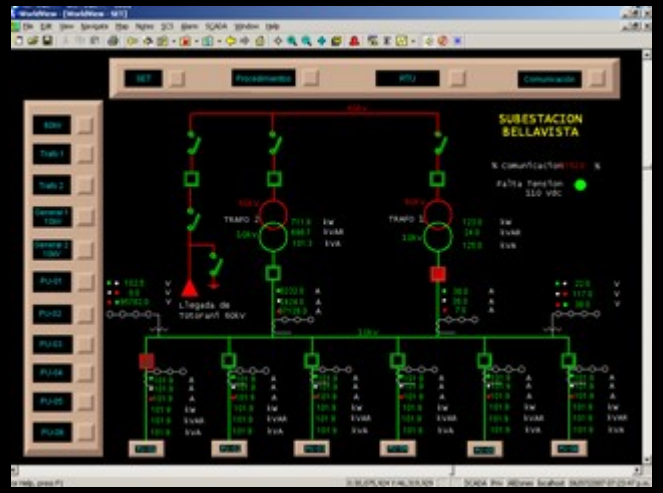
Cyber incident prevention

1. An external intruder sent phishing emails to industrial system administrators (he had gathered the information on the people involved through social networks). Two administrators accessed the email and left their access passwords to the corporate network.
2. The intruder connected remotely through vpn using that user/pass as authentication factor. He achieved remote access to the corporate network.
3. Afterwards the intruder, using the same users and passwords, accessed those administrators' equipment remotely (via RDP), from where he learnt, researched, knew about new users and passwords, read user's guides, etc.
4. He installed a Keylogger on both workstations (which had administrative privileges).

Cybsec by Deloitte.

Cyber incident prevention

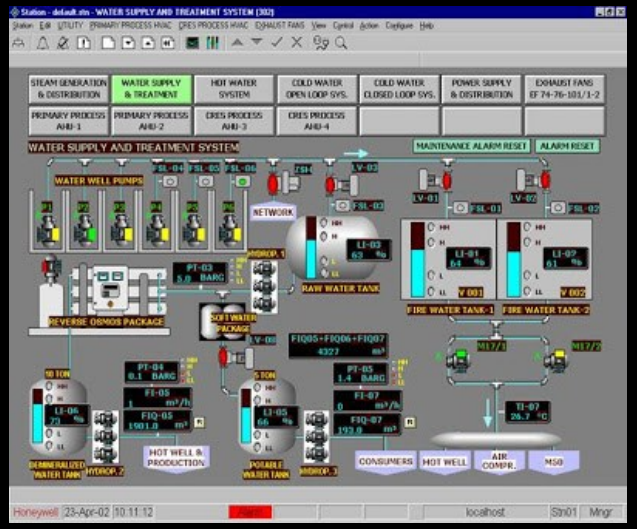
5. He connected to the pivot system to get to the industrial network (he authenticated with a user/pass he had obtained) and with a soft-token installed in the equipment of the mentioned administrators.
6. From the pivot equipment, he accessed the HMI system console for system management (power/gas/water) through the web. He authenticated with another user and password he had obtained with the Keylogger installed in administrators' equipment.
7. The intruder learnt to use the system.



Cybsec by Deloitte.

Cyber incident prevention

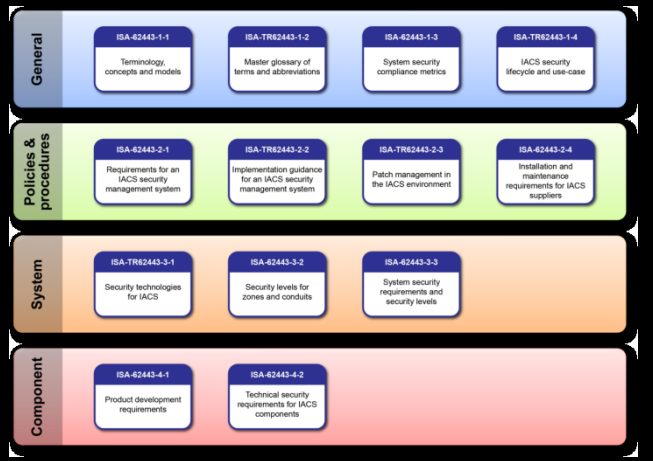
8. During the attack, the intruder accessed the HMI system (he blocked substations / closed pumps / modified gas pressure) causing serious drawbacks.
9. Afterwards, the intruder accessed the ICS system servers at operating system level and deleted the configurations of the core and secondary systems. He then shut down the systems..



Cybsec by Deloitte.

Cyber incident prevention

a. Approach between the IS sector and the engineer and industrial network operations areas.
b. Compile an Inventory, have a clear understanding and determine the systems covered.
c. Technological Risk Analysis on the industrial systems covered by the scope.
d. Assessment against industrial cybersecurity standards: ISA-IEC 62443 (ISA-99) – ICS CERT.
e. Establish attack scenarios.



Cybsec by Deloitte.

Cyber incident scenarios

Internal attack:

- Technical staff in engineering
- Operations staff
- IT / Security staff
- Internal staff (other areas in the Organization)
- External provider staff

External attack :

- Service provider (through previously authorized remote accesses)
- External intruders (remote accesses - Internet)
- Criminal organizations
- Foreign governments

Cybsec by Deloitte.

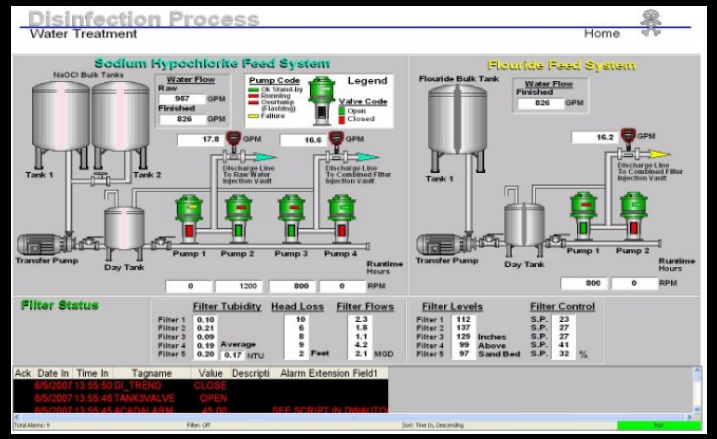
Real-case cyber attack scenarios in Latin America

1. Internal intruder who caused a sabotage using the industrial system in an unauthorized manner.
2. External intruder who accessed the industrial system through the Internet and deleted all the servers of the HMI system.
3. External intruder who accessed the monitoring system through the Internet and exploited vulnerabilities.
4. Provider who accessed with his equipment, connected to the internal network and infected the whole corporate and industrial network with a malware.
5. Internal intruder who accessed the HMI system from the corporate network and caused a shutdown of the industrial network equipment.

Cyber incident prevention

f. Definition of an Action Plan to mitigate risks.

- In-depth defence – secure design - network segmentation.
- Availability, integrity and confidentiality.
- Configuration of security aspects (pass + parameters)
- Application of patches and upgrades
- Limited use of local Anti-Virus.
- Authentication and authorization.
- Auditing and logging level.
- Inappropriate use of ICS.
- Third-party Access.
- Human factor.



Cybsec by Deloitte.

Cyber incident prevention

g. Implement the Action Plan

- Remote industrial network access always based on two-factor authentication.
- Access to the industrial network from the corporate network always based on two-factor authentication.
- Provider remote access control (Company's own links and VPN).
- Generate logs and event logging in equipment and devices.
- Proactive monitoring.
- Raise awareness on cybersecurity aspects.

Cyber incident prevention

h. Continuous improvement

- Continuous and in-depth Assessment.
- Secure by Design – Participate in the new unfolding of industrial systems.

i. Manage cybersecurity incidents

Cybsec by Deloitte.

Agenda

1 – Cyber-Resilience

2 – Incident prevention

3 – Incident Management

4 - Conclusions

Cybsec by Deloitte.

Cyber incident management

Are we ready to react to a security incident?

The answer is NO.

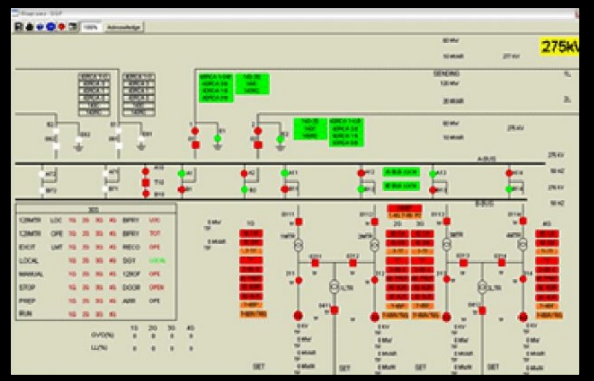
- Little interaction between SI and OT.
- At the most, we have internal CSIRT with a low level of maturity and scope.
- There are few logs with information and they are implemented by default most of the time.
- There is lack of technical knowledge in information security among the IS staff.
- There is lack of technical knowledge in OT systems among the SI staff.

Cybsec by Deloitte.

Cyber attack against an industrial network and a corporate network

In an attack to an industrial network:

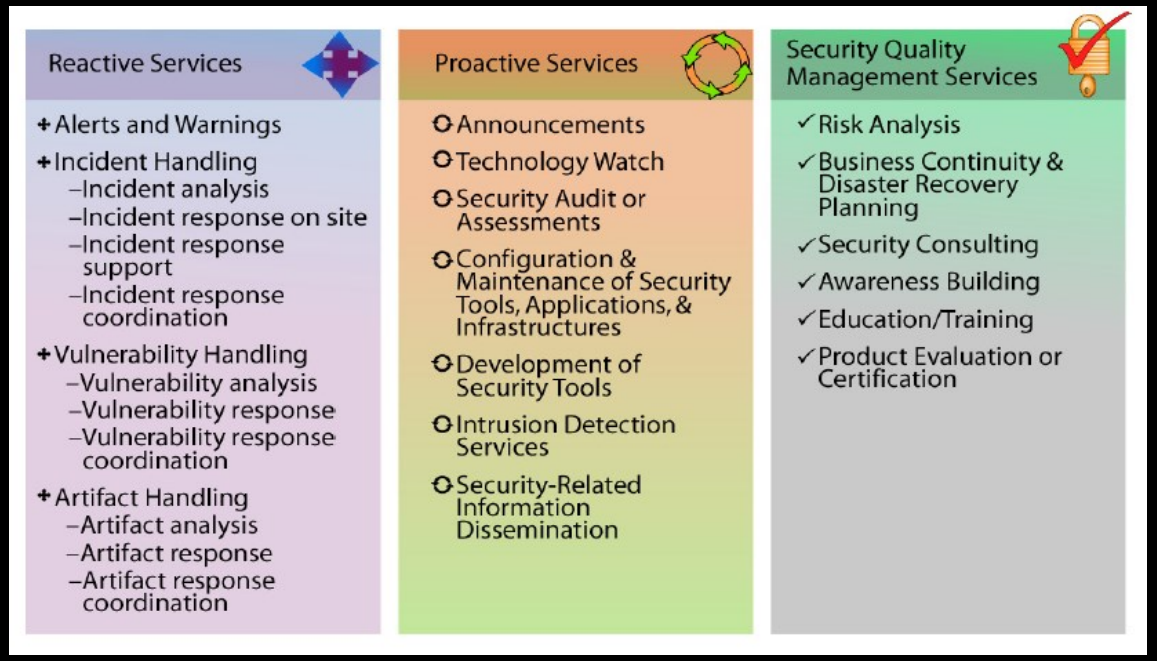
- There has to be knowledge on other technologies and different protocols with their own systems, applications and configurations.
- There should be stronger security measures (two-factor authentication, IDS, IPS, internal firewalls, pivot equipment, etc.).
- You should be knowledgeable on and know how to operate an ICS. (there are thousands of HMI systems and customized settings).
- Much more time is needed.



Cybsec by Deloitte.

Recommendations to establish the internal CSIRT

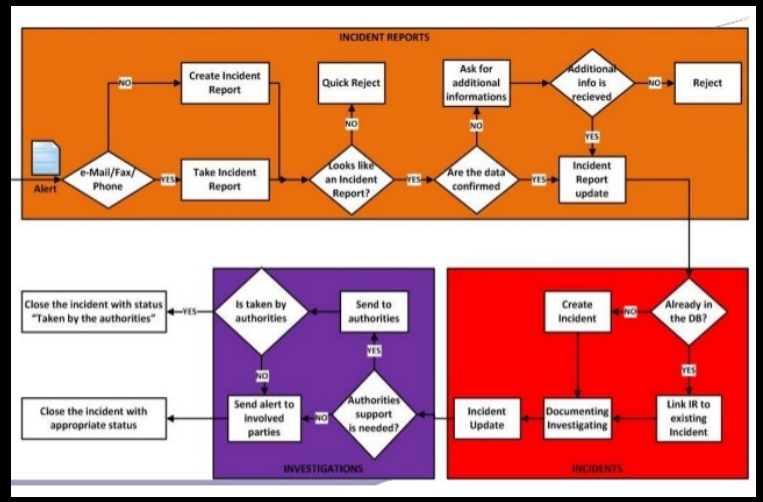
1. Identify project sponsors and participating areas (include the industrial area).
2. Gain support and acceptance from senior management. Define the leadership to implement the CSIRT.
3. Identify and define the internal CSIRT. Determine the range and level of the service to be provided.



Cybsec by Deloitte.

Recommendations to establish the internal CSIRT

3. Identify the resources required (staff, equipment, infrastructure, training, etc.). Draw a budget and have it approved. Have a back-up plan of the CSIRT components.
4. Define roles and responsibilities clearly. Define the CSIRT interactions with the rest of the organization and the exterior.
5. Establish workflows.



Cybsec by Deloitte.

Recommendations to establish the internal CSIRT

6. Implement the CSIRT. Notify internally and externally.
7. Operate the CSIRT. Manage security incidents.
8. Continuous CSIRT upgrading from the lessons learned, the interaction with other CSIRTs, metrics, etc.

Agenda

1 – Cyber-Resilience

2 – Incident prevention

3 – Incident management

4 - Conclusions

Cybsec by Deloitte.

Conclusions

Our organization must be cyber-resilient to survive.

We must build bridges between industrial areas and make them aware of cybersecurity.

We must implement preventive measures to protect ourselves from cyber incidents.

We must be ready to manage future cybersecurity incidents.

Thank you

Julio Ardita – Cybsec by Deloitte - jardita@deloitte.com