# Convergência Segura: Boas Práticas de Cibersegurança para Máquinas e Sistemas Industriais

# AVISO IMPORTANTE

**O conteúdo técnico da palestra é de responsabilidade da empresa palestrante.**

**Fique à vontade para baixar o arquivo em PDF e se atualizar com as novas tecnologias apresentadas nesta edição.**



**Qualquer dúvida em relação ao conteúdo apresentado, você pode entrar em contato direto com o palestrante.**

# Cibersegurança na Indústria: muito além de um assunto técnico


Relatório da Dragos de 2025 baseado em modelagens estatísticas, abrange uma década de análise de dados sobre violações e sinistros de seguro, e oferece um panorama realista sobre o impacto financeiro das falhas de segurança em ambientes OT.

Fonte: Dragos (2025)

# Histórico de Ataques na Indústria

**Ataques direcionados OT/ICS**

- 2010 — Stuxnet
- 2013 — DragonFly, Havez
- 2015 — Black Energy
- 2016 — Industroyer
- 2017 — Triton Trisis

**Merck**
Pharmaceuticals
**$310 M**

**TSMC**
Electronics
**$250 M**

**Mondelez**
Food & Beverage
**$150 M**

**Reckitt Benckiser**
Consumer Goods
**$150 M**

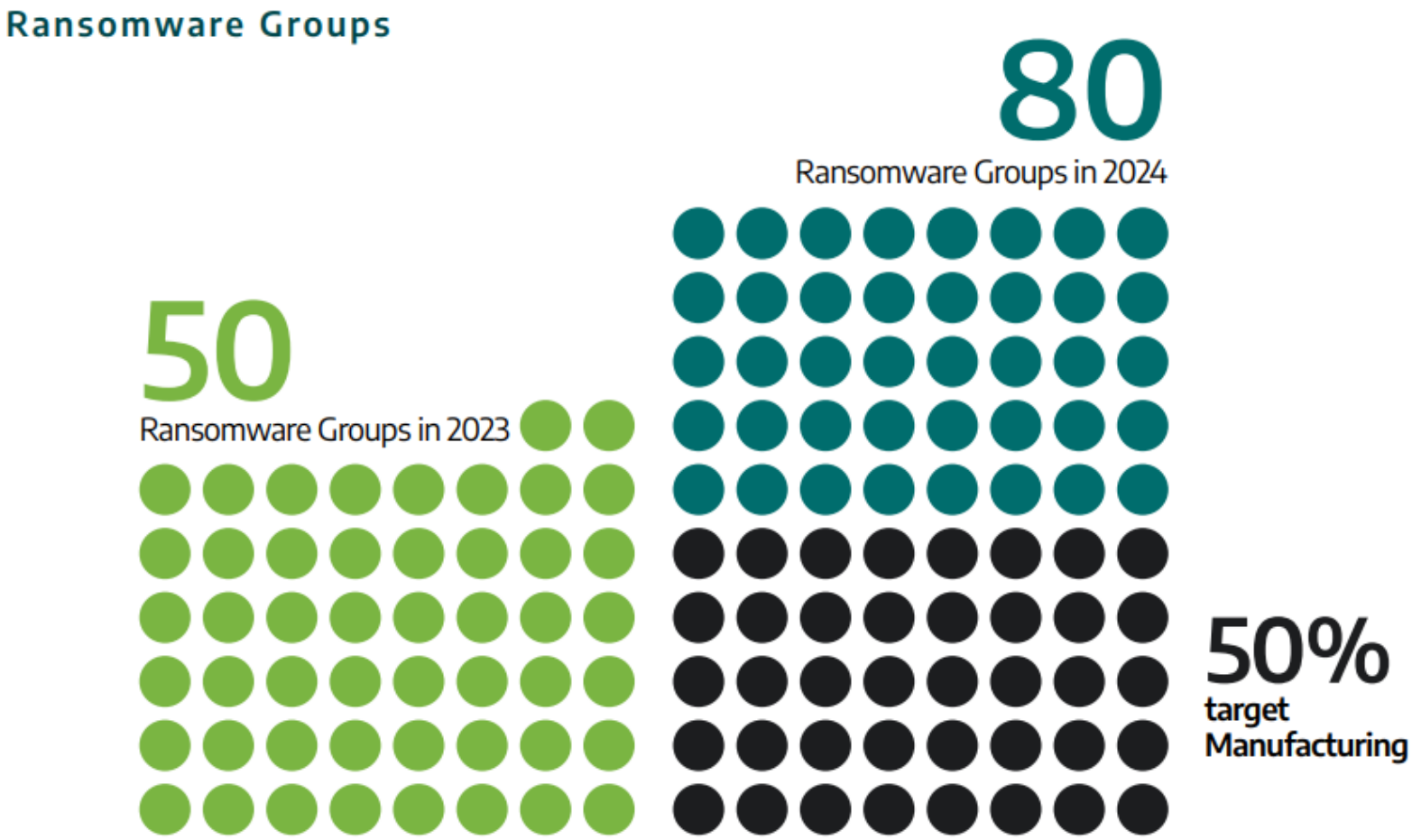
**Worms**

- 2017 — WannaCry, Bad Rabbit
- 2019 — LockerGoga
- 2020 — Wasted Locker
- 2021 — DarkSide, Revil

**Ransomware Direcionado**

Fonte: TXOne Networks

# Crescimento de Ataques na Indústria




Fonte: Dragos (2025)

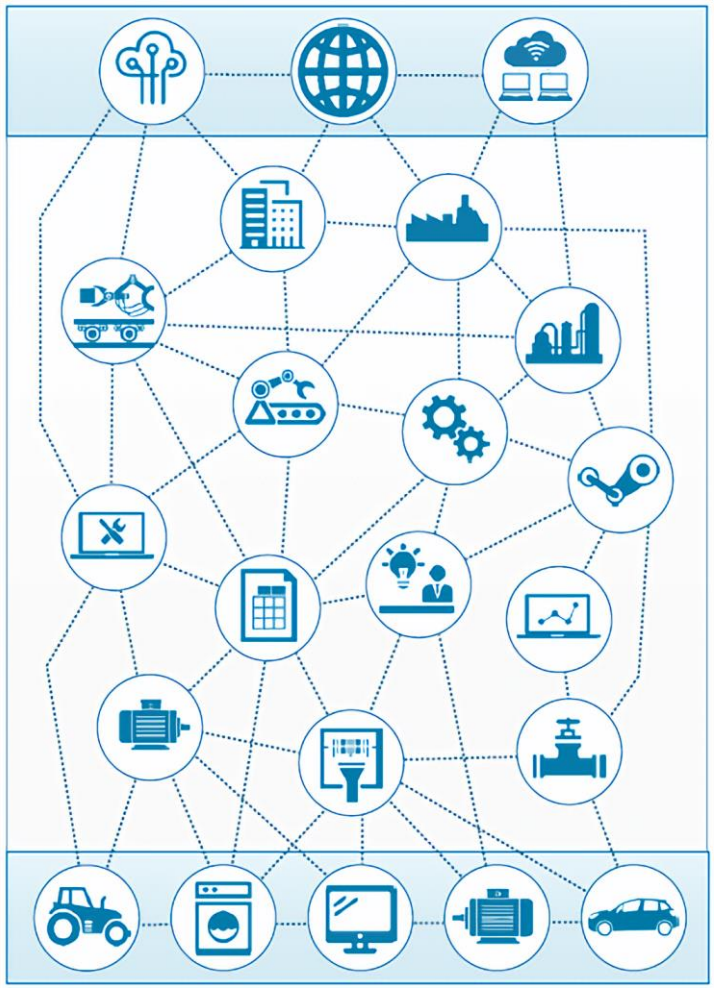
# A Importância dos sistemas industriais

**Segurança cibernética em ambientes industriais não é mais opcional.**

**É um investimento estratégico para garantir continuidade, produtividade e crescimento.**

# Quando os riscos cibernéticos se tornaram maiores na Indústria?

**Smart Factory**

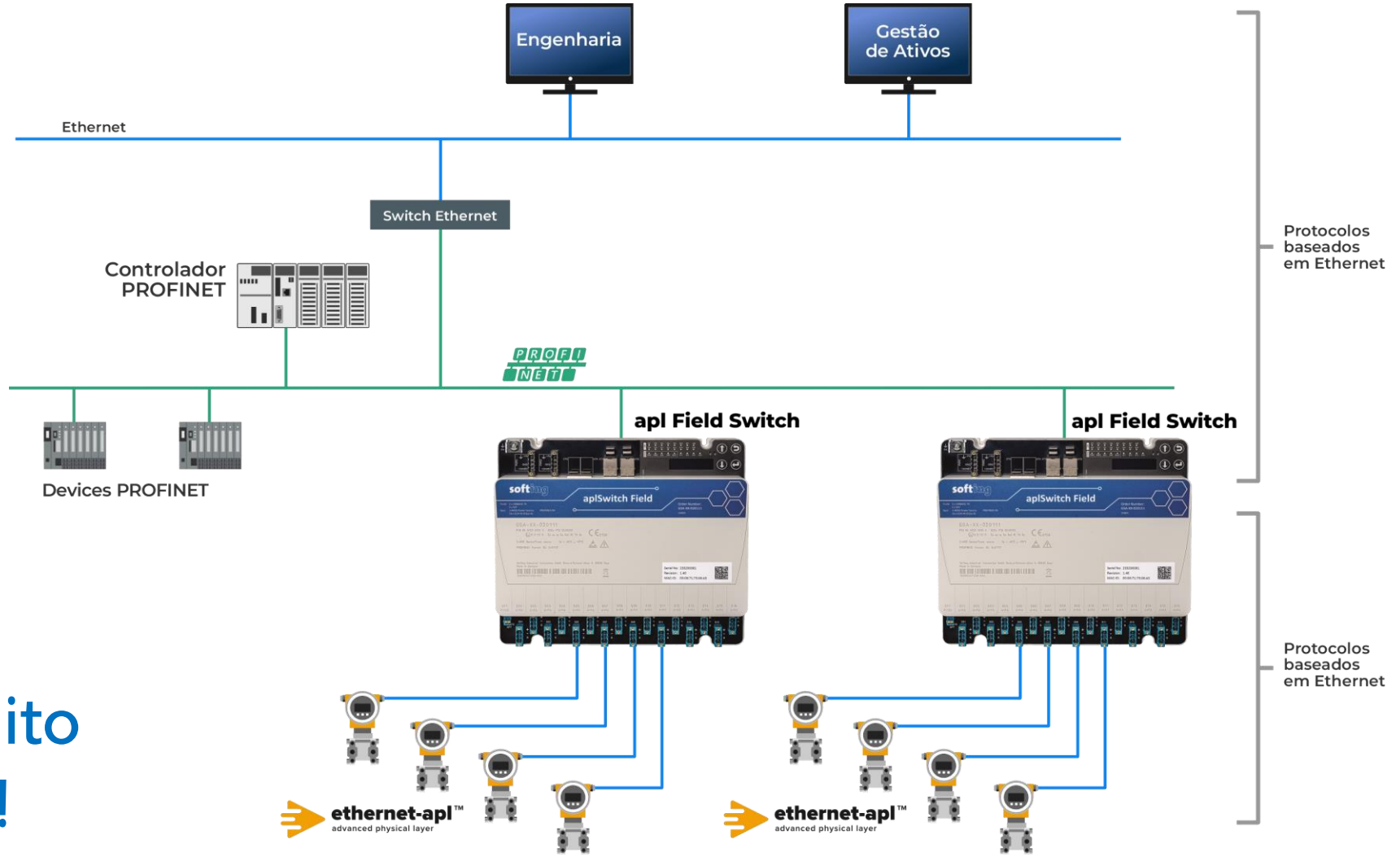


**Smart Products**

## Indústria 4.0

- Sistemas e máquinas flexíveis;
- Funções distribuídas em rede;
- Cooperação entre todos os níveis;
- Comunicação entre todos os participantes;
- Produto integrado à rede.

# Quando os riscos cibernéticos se tornaram maiores na Indústria?




## Arquiteturas muito mais integradas!

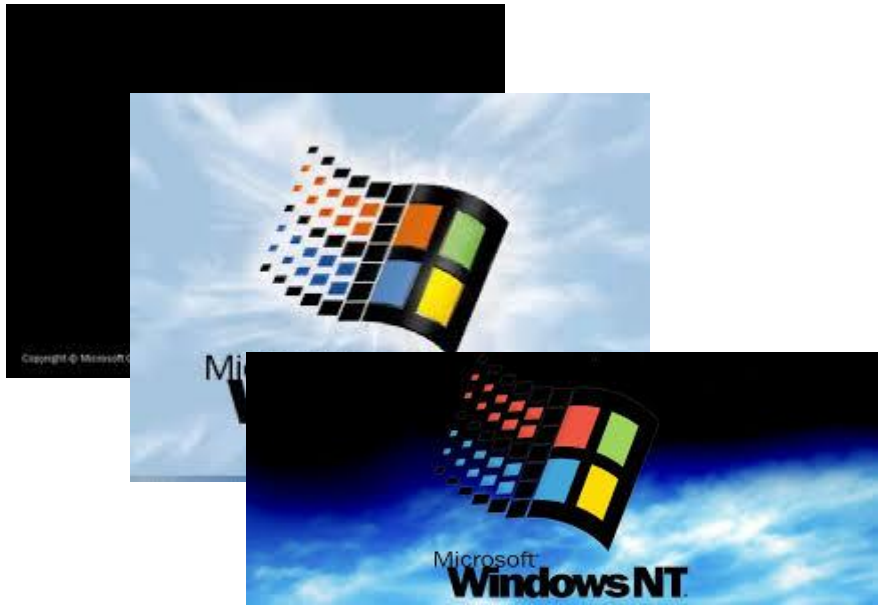
# Qual é a motivação dos atacantes?

Devido a gravidade e os impactos que podem causar em ambientes OT, torna-se muito mais fácil receber o pagamento das vítimas, pois este incidente, além de parar totalmente o negócio, também pode gerar risco à segurança física dos equipamentos e das pessoas.


**Negócio rentável!**

# Qual é a motivação dos atacantes?

Os criminosos entenderam que existem muitas falhas de segurança no ambiente OT, tornando o trabalho deles muito mais fácil;




Microsoft » Windows Xp : Security Vulnerabilities, CVEs CVSS score >= 9

Published in: 2025 January February March April May June July

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

Page: 1 Copy

| | | | |
|---|---|---|---|
| CVE-2017-8487 | Potential exploit | Max CVSS | 9.3 |
| Windows OLE in Windows XP and Windows Server 2003 allows an attacker to execute code when a victim opens a specially crafted file or program aka "Windows olecnv32.dll Remote Code Execution Vulnerability." | | EPSS Score | 74.40% |
| Source: Microsoft Corporation | | Published | 2017-06-15 |
| | | Updated | 2019-10-03 |
| CVE-2017-0176 | Potential exploit | Max CVSS | 9.3 |
| A buffer overflow in Smart Card authentication code in gpkcsp.dll in Microsoft Windows XP through SP3 and Server 2003 through SP2 allows a remote attacker to execute arbitrary code on the target computer, provided that the computer is joined in a Windows domain and has Remote Desktop Protocol connectivity (or Terminal Services) enabled. | | EPSS Score | 62.56% |
| Source: Microsoft Corporation | | Published | 2017-06-22 |
| | | Updated | 2019-10-24 |
| CVE-2014-0301 | | Max CVSS | 9.3 |
| Double free vulnerability in qedit.dll in DirectShow in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via a crafted JPEG image, aka "DirectShow Memory Corruption Vulnerability." | | EPSS Score | 17.27% |
| Source: Microsoft Corporation | | Published | 2014-03-12 |
| | | Updated | 2025-04-12 |

# Diferenças entre o IT e OT

| TI/IT | OT/TA |
|---|---|
| Possui computadores. | = Possui computadores. |
| Possui redes de comunicação. | = Possui redes de comunicação. |
| Possui aplicações Web. | = Possui aplicações Web. |
| Possui redes Wireless. | = Possui redes Wireless. |
| Possui softwares diversos. | = Possui softwares diversos. |
| Possui software antivírus. | ≠ Nem sempre possui software antivírus. |
| É possível realizar atualização de software e sistemas operacionais. | ≠ Dificilmente é possível realizar atualização de software e sistemas operacionais. |
| Paradas para manutenção e implementações podem ser realizadas sem grandes impactos. | ≠ Paradas de qualquer natureza (para manutenção ou por falhas), na maioria dos casos causam grandes impactos. |
| É possível realizar testes e auditorias a qualquer momento e em muitos casos, esses procedimentos são contínuos (Ex.: Pentest). | ≠ Todos os procedimentos de teste precisam ser programados e, na maioria dos casos, com prazos/tempo curtos de duração. |
| As equipes possuem conhecimento em relação às boas práticas de segurança cibernética. Na maioria dos casos, possuem equipes específicas para essa questão. Inclusive, certificações são exigidas desses profissionais (ISFS, CompTIA Security+, CEH, Exin Secure Programing etc.). Por ser considerado um assunto de extrema importância, as próprias empresas investem na formação e certificação desses profissionais. | ≠ As equipes possuem muito conhecimento em relação aos sistemas de automação, porém, em relação às questões de segurança cibernética, ainda não é um assunto de domínio dessas equipes e, muitas vezes, o conhecimento nesse sentido é quase nulo. Poucas empresas investem na formação dessas equipes. Poucas empresas possuem equipes específicas para questões de segurança cibernética em OT/TA e as que possuem, ainda estão em processo para obter de fato maturidade no assunto. |

# Mitos: No ambiente OT não há conexão com a Internet

shodan.io/search?query=S7

Reiniciar para atualizar

Todos os marcadores

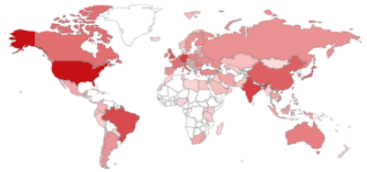
Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | S7 | Account

TOTAL RESULTS

19,784

TOP COUNTRIES



| | |
|---|---|
| United States | 5,156 |
| Germany | 1,821 |
| India | 1,795 |
| Brazil | 1,403 |
| United Kingdom | 1,003 |

More...

TOP PORTS

| | |
|---|---|
| 443 | 6,252 |

View Report | Browse Images | View on Map | Advanced Search

**Product Spotlight:** Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

**177.75.6.124**

Networld Provedor e Servicos de Internet Ltda

Brazil, Brasília

2024-10-28T04:26:15.240900

```
SNMP:
  Uptime: 1
  Description: Siemens, SIMATIC, S7-300
  Service: 72
  Versions:
    1
    3
  Engineid Format: octets
  Contact: Corporate IT
  Engine Boots: 2
  Engineid Data: 80004fb805666262393633363636613561000011500
  Enterprise: 20408
  Objectid: 0.0
  Engine Time: 3:13:08
  Location: BE...
```

**88.26.199.53**

53.red-88-26-199.staticip.rima-tde.net

Telefonica de Espana SAU
Red de servicios IP Spain

2024-10-28T04:26:04.757786

```
SSH-2.0-OpenSSH_5.3
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAABIwAAAQEAxjMRmRBLqM9X/farUDNE8zy+G8f63x66uycu1e10eba564WH
```

# Mitos: Hackers não conhecem redes industriais

```
root@KaliICS:~/git/smod# /usr/bin/python2.7 smod.py
 _______
< SMOD >
 -------
        \   ^__^
         \  (xx)\_______
            (__)\       )\/\
             U  ||----w |
                ||     ||
          --=[MODBUS Penetration Test FrameWork
       --+--=[Version : 1.0.4
       --+--=[Modules : 23
       --+--=[Coder   : Farzin Enddo
          --=[github  : www.github.com/enddo

SMOD > use modbus/s
modbus/scanner  modbus/sniff
SMOD > use modbus/scanner/uid
SMOD modbus(uid) > set RHOSTS 192.168.100.100
SMOD modbus(uid) > exploit
[+] Module Brute Force UID Start
[+] Start Brute Force UID on : 192.168.100.100
Connection unsuccessful due to the following error :

SMOD modbus(uid) > set RHOSTS 192.168.100.1
SMOD modbus(uid) > exploit
[+] Module Brute Force UID Start
[+] Start Brute Force UID on : 192.168.100.1
[+] UID on 192.168.100.1 is : 1
[+] UID on 192.168.100.1 is : 2
```

```
SMOD > use modbus/scanner/getfunc
SMOD modbus(getfunc) > set RHOSTS 192.168.100.1
SMOD modbus(getfunc) > set UID 10
SMOD modbus(getfunc) > exploit
[+] Module Get Function Start
[+] Looking for supported function codes on 192.168.100.1
[+] Function Code 0 is supported.
[+] Function Code 1(Read Coils) is supported.
[+] Function Code 2(Read Discrete Inputs) is supported.
[+] Function Code 3(Read Multiple Holding Registers) is supported.
[+] Function Code 4(Read Input Registers) is supported.
[+] Function Code 5(Write Single Coil) is supported.
[+] Function Code 6(Write Single Holding Register) is supported.
[+] Function Code 7(Read Exception Status) is supported.
[+] Function Code 8(Diagnostic) is supported.
[+] Function Code 9 is supported.
[+] Function Code 10 is supported.
[+] Function Code 11(Get Com Event Counter) is supported.
[+] Function Code 12(Get Com Event Log) is supported.
[+] Function Code 13 is supported.
[+] Function Code 14 is supported.
[+] Function Code 15(Write Multiple Coils) is supported.
[+] Function Code 16(Write Multiple Holding Registers) is supported.
[+] Function Code 17(Report Slave ID) is supported.
[+] Function Code 18 is supported.
[+] Function Code 19 is supported.
[+] Function Code 20(Read File Record) is supported.
[+] Function Code 21(Write File Record) is supported.
[+] Function Code 22(Mask Write Register) is supported.
[+] Function Code 23(Read/Write Multiple Registers) is supported.
```

```
SMOD > use modbus/function/readCoils
SMOD modbus(readCoils) > set RHOSTS 192.168.100.1
SMOD modbus(readCoils) > set UID 10
SMOD modbus(readCoils) > exploit
[+] Module Read Coils Function Start
[+] Connecting to 192.168.100.1
[+] Response is :
###[ ModbusADU ]###
  transId   = 0x300
  protoId   = 0x0
  len       = 0x5
  unitId    = 0xa
###[ Read Coils Answer ]###
     funcCode  = 0x1
     byteCount = 2L
     coilStatus= [0, 3]
```

## Script para ataque em redes Modbus

# Mitos: Hackers não conhecem redes industriais

XII Simpósio Brasileiro de Automação Inteligente (SBAI)
Natal – RN, 25 a 28 de outubro de 2015

**ATAQUE *DENIAL OF SERVICE* EM REDES PROFINET: ESTUDO DE CASO**

AFONSO CELSO TURCATO[1] / ROGÉRIO ANDRADE FLAUZINO[1]
GUILHERME SERPA SESTITO[2] / ANDRÉ LUIS DIAS[2] / DENNIS BRANDÃO[2]

1. *Laboratório de Automação Inteligente de Processos e Sistemas, Departamento de Engenharia Elétrica, USP*
*Avenida Trabalhador São-carlense, 400, 13566-590 - São Carlos - SP*
afonso.turcato@usp.br, raflauzino@sc.usp.br

2. *Laboratório de Automação Industrial, Departamento de Engenharia Elétrica, USP*
*Avenida Trabalhador São-carlense, 400, 13566-590 - São Carlos - SP*
guilherme.sestito@usp.br, andreldias@usp.br, dennis@sc.usp.br

**Abstract**— Profinet is a contemporary protocol for industrial networks that offers great importance in the market. Even tough had been developed recently, a traditional and well-known type of attack on digital networks, known as Denial of Service (DoS) can be easily accomplished in a Profinet network, that has no intrinsic mechanisms which make it blocks or hinder this type of attack.This article presents an overview of the main types of attack on digital communication networks and demonstrates an effective DoS attack if performed in a real Profinet network built in the laboratory. It could lead to major negative impacts in the industrial plant.

**Keywords**— RTE, Profinet, Security

EXPLOIT DATABASE

http://www.sbai2015.dca.ufrn.br/download/artigo/67

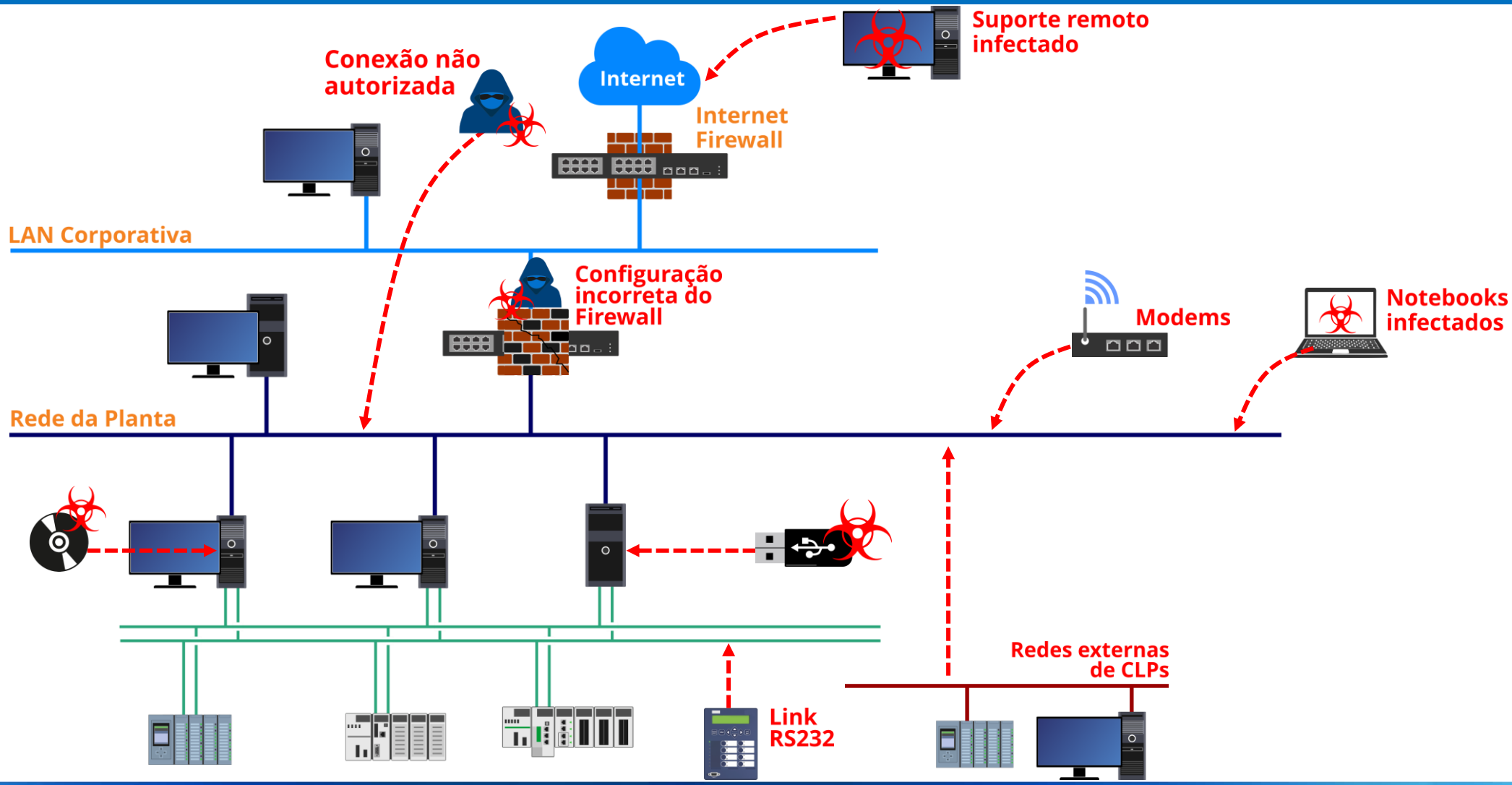
# Exemplos de malwares específicos para Indústria

**Fuxnet**
ICS Malware específico para protocolos de barramento serial como RS485 e Meter-Bus. Danifica sistemas de arquivos, firmware, e sobrecarrega comunicação.

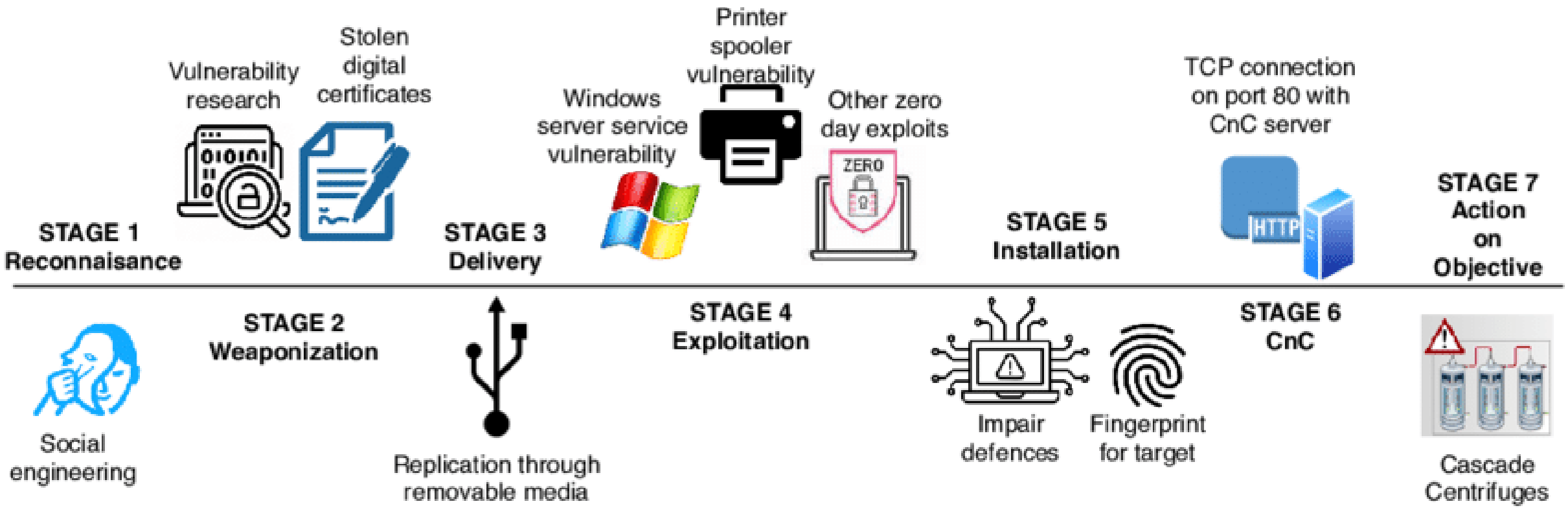
**FrostyGoop**
ICS Malware tem como alvo sistemas de controle com o protocolo Modbus/TCP, um padrão industrial comum.


**Chaya_003**
ICS Malware projetado para encerrar processos em execução em estações de engenharia TIA Portal da Siemens.

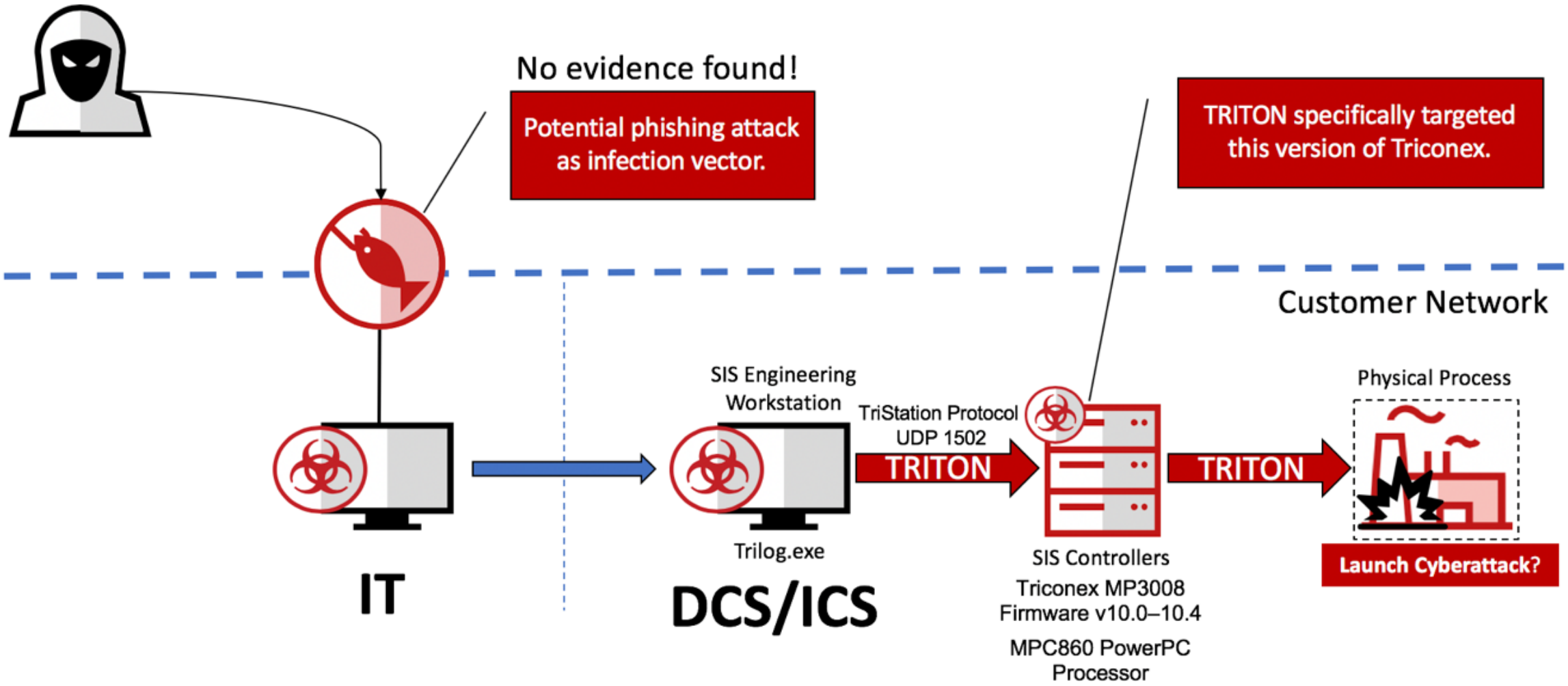
# Exemplos de Vetores de Ataques



# Exemplo de Ataque: STUXNET



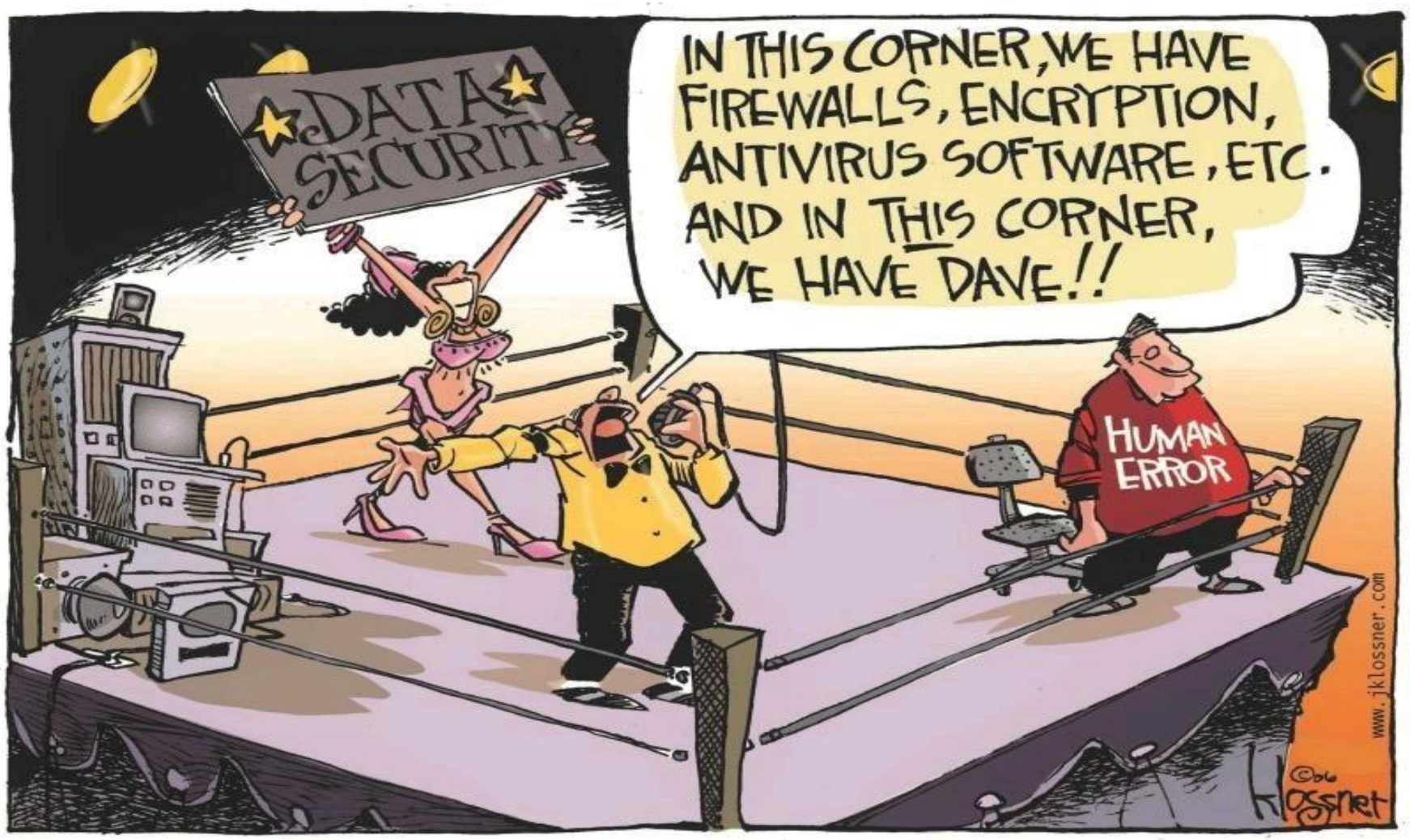
# Exemplo de Ataque: TRITON



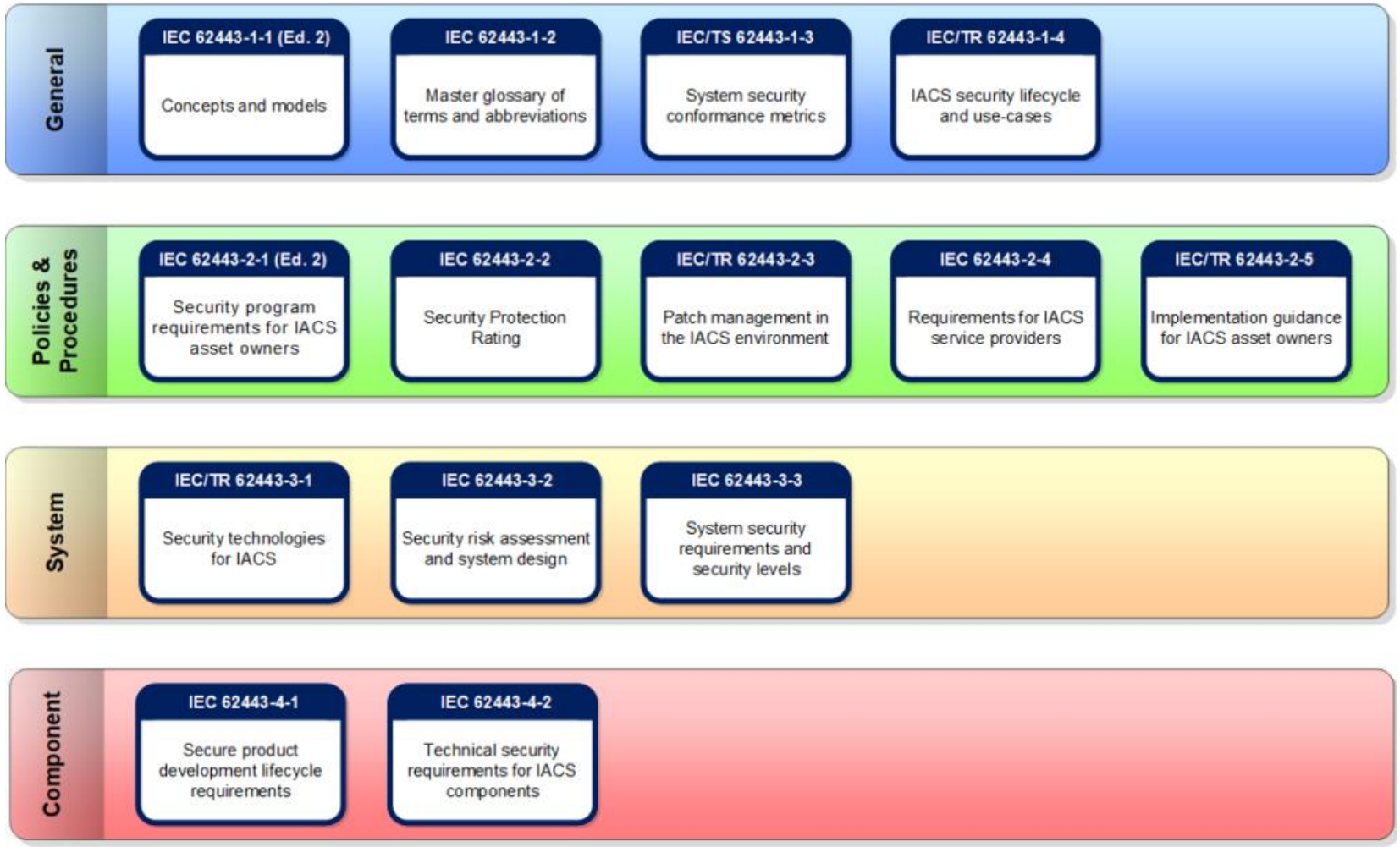
# Vulnerabilidades existentes no ambiente OT

- Sistemas operacionais (Ex.: Computadores, IHMs, Estações de Engenharia, etc)
- Aplicações WEB (Ex.: Inversores, Controladores, Switches, etc.)
- Aplicações Wireless (Ex.: Wi-Fi, Bluetooth, etc.)
- Aplicações Móveis (Ex.: Android, iOS, etc.)
- Firmwares dos dispositivos de Automação (Ex.: CLPs, Inversores de Frequência, Soft-starters, etc.)
- Softwares diversos (Ex.: Supervisórios, Programação de CLPs, OPCs, MES, etc.)
- Redes de dados (Conectando: computadores, IHMs, Controladores e outros dispositivos)
- Fator mais vulnerável: **Ainda é o fator HUMANO!**

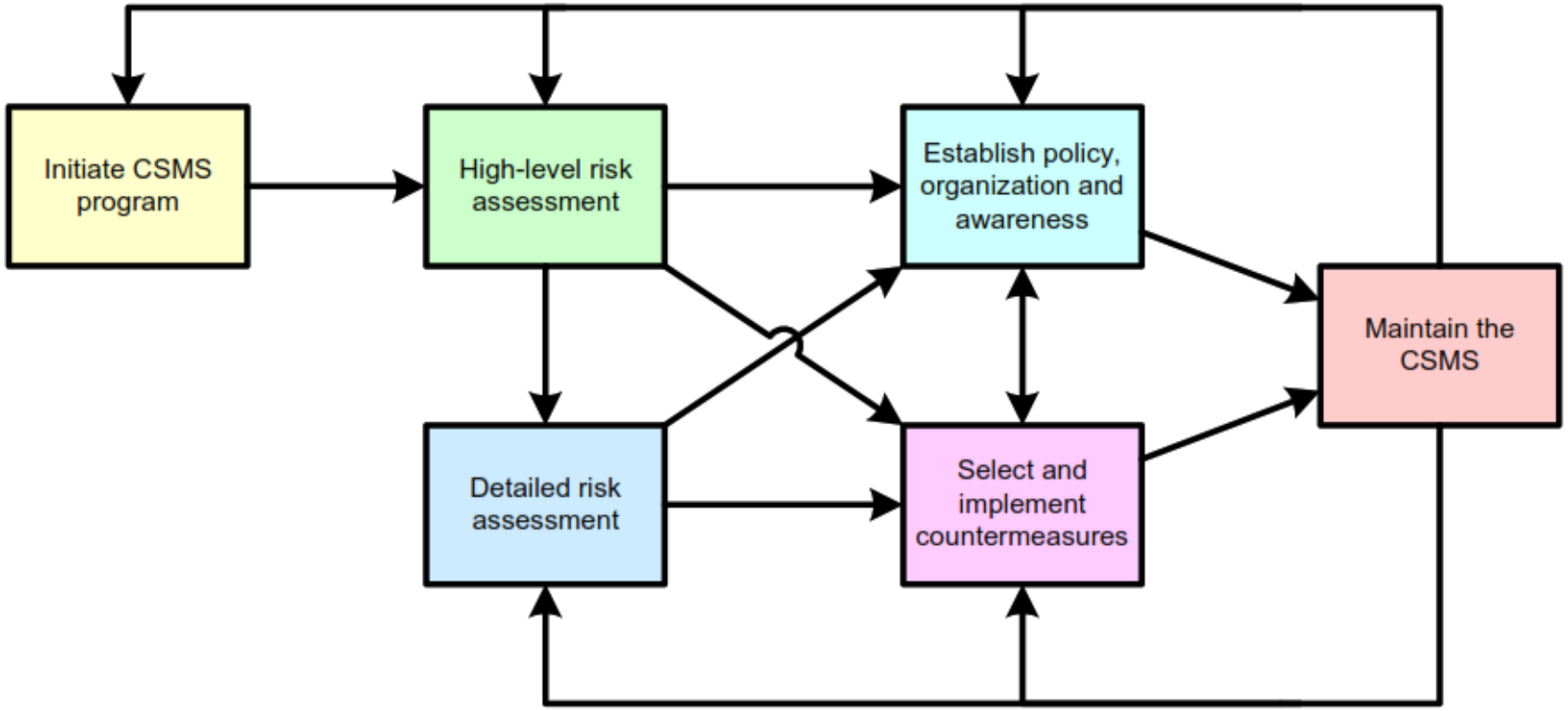
# Vulnerabilidades existentes no ambiente OT



# ISA/IEC 62443: um guia importante na sua jornada de CS / OT



# CSMS – Cybersecurity Management System



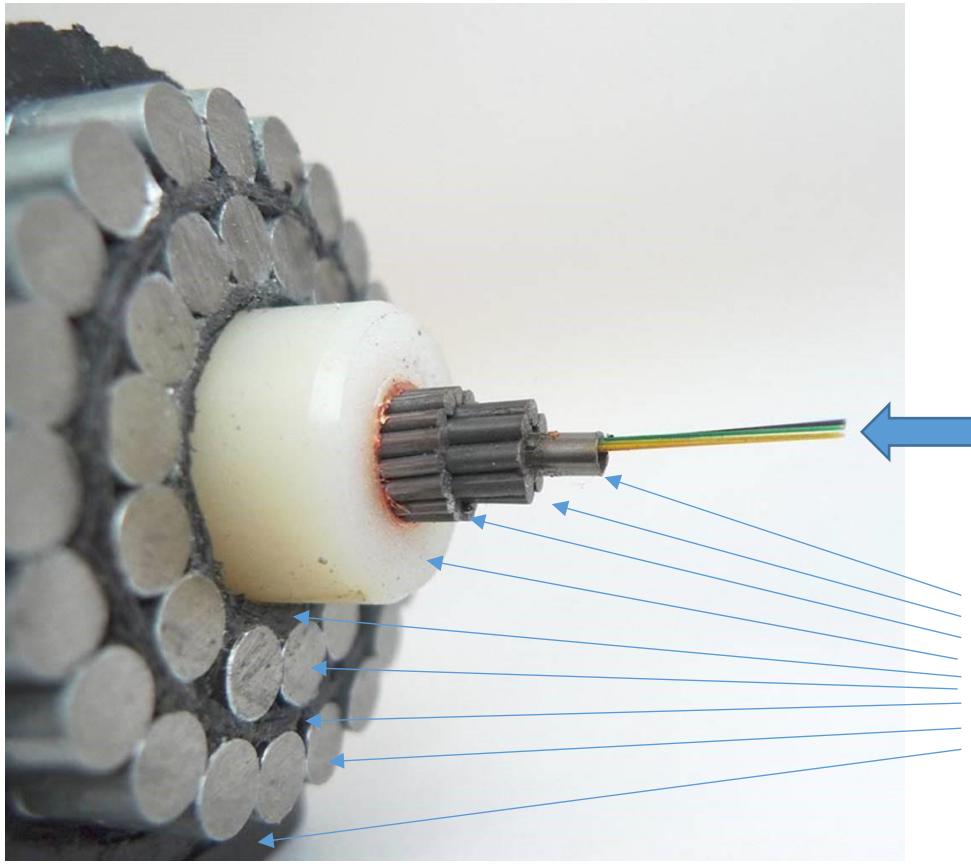

Cibersegurança não é um projeto, com início, meio e fim!
É um PROCESSO contínuo!

# Porque utilizar os conceitos de CSMS?

A solução mais popular é utilizar uma camada de proteção entre a rede de TI e a rede OT, porém, esta não é uma solução eficaz...

# Camadas de proteção

Um dos conceitos mais antigos e eficazes é inserir camadas de proteção

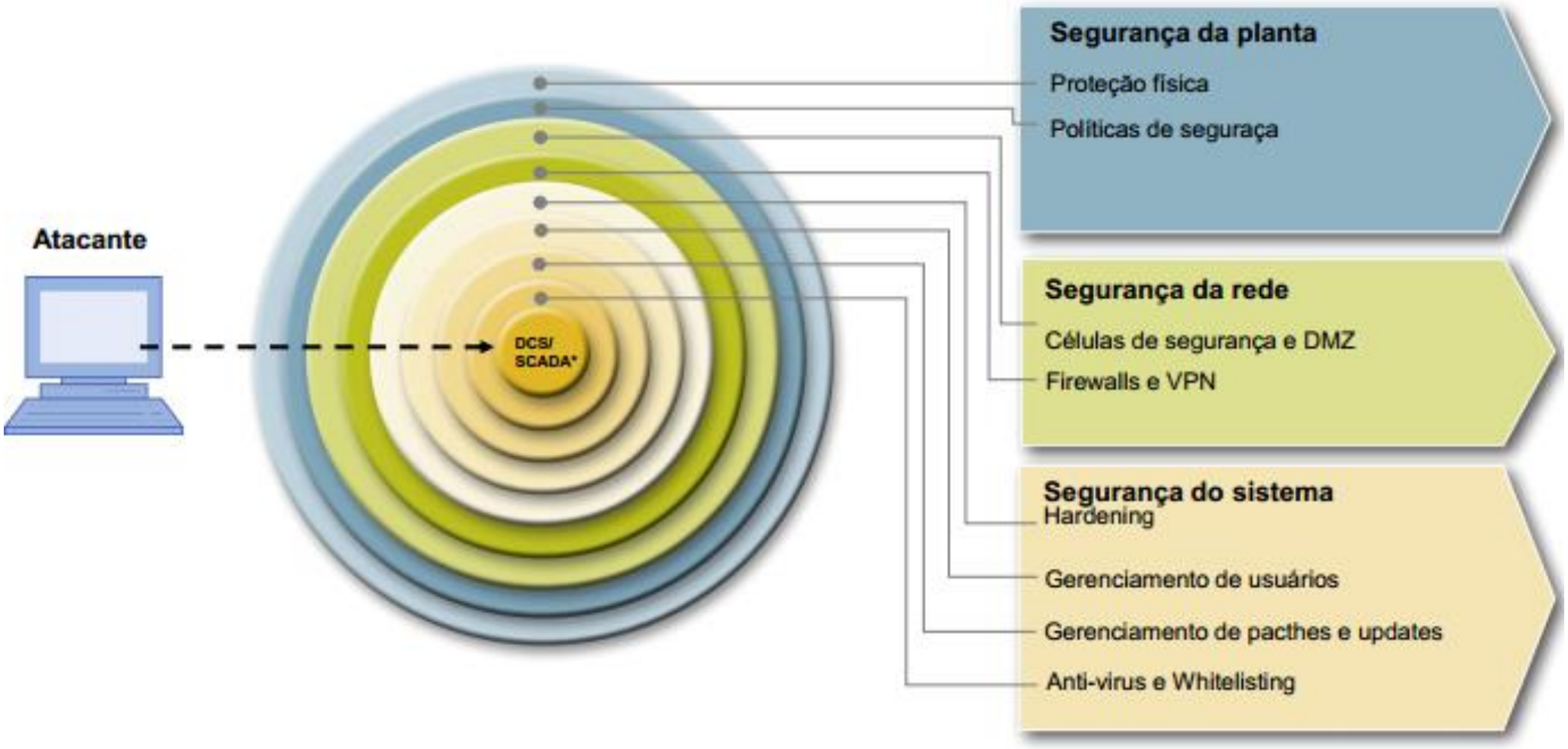


Proteger o que é vulnerável, entendendo a sua importância!

O que trafega nessas vias de fibras ópticas vale muito mais do que o investimento necessário para...

...prover estas camadas de proteção!

# Camadas de proteção para os sistemas industriais

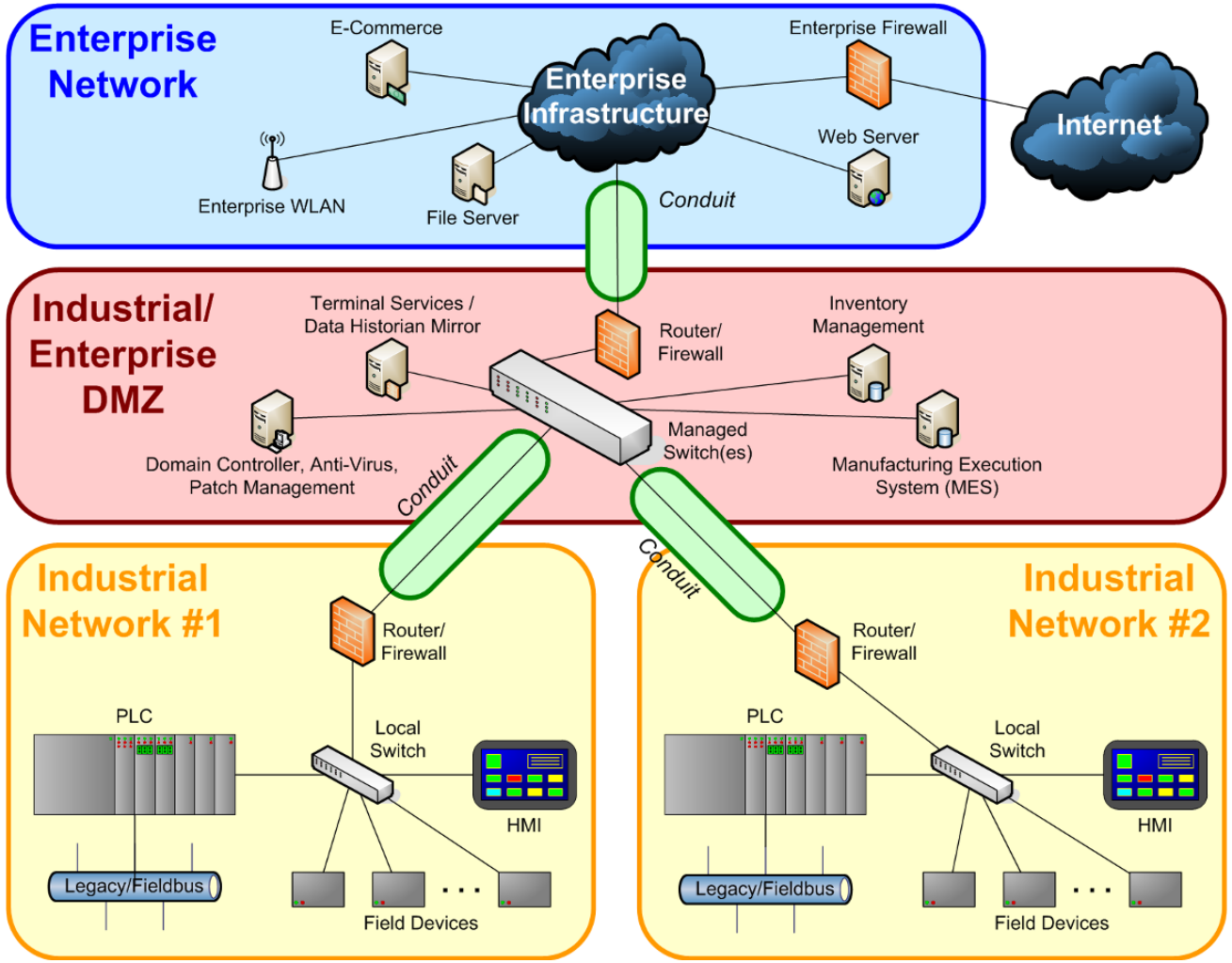


# ISA/IEC62443: Zonas e Conduítes

## DEFESA EM PROFUNDIDADE
## MODELOS DE ZONAS E CONDUÍTES

### ZONA

Uma zona é definida como um grupo de ativos, sejam físicos ou lógicos, que compartilham recursos e requisitos de segurança. Cada zona é claramente definida por uma barreira, física ou lógica dependendo do tipo de ativos, que separa os componentes que fazem parte e os que não.

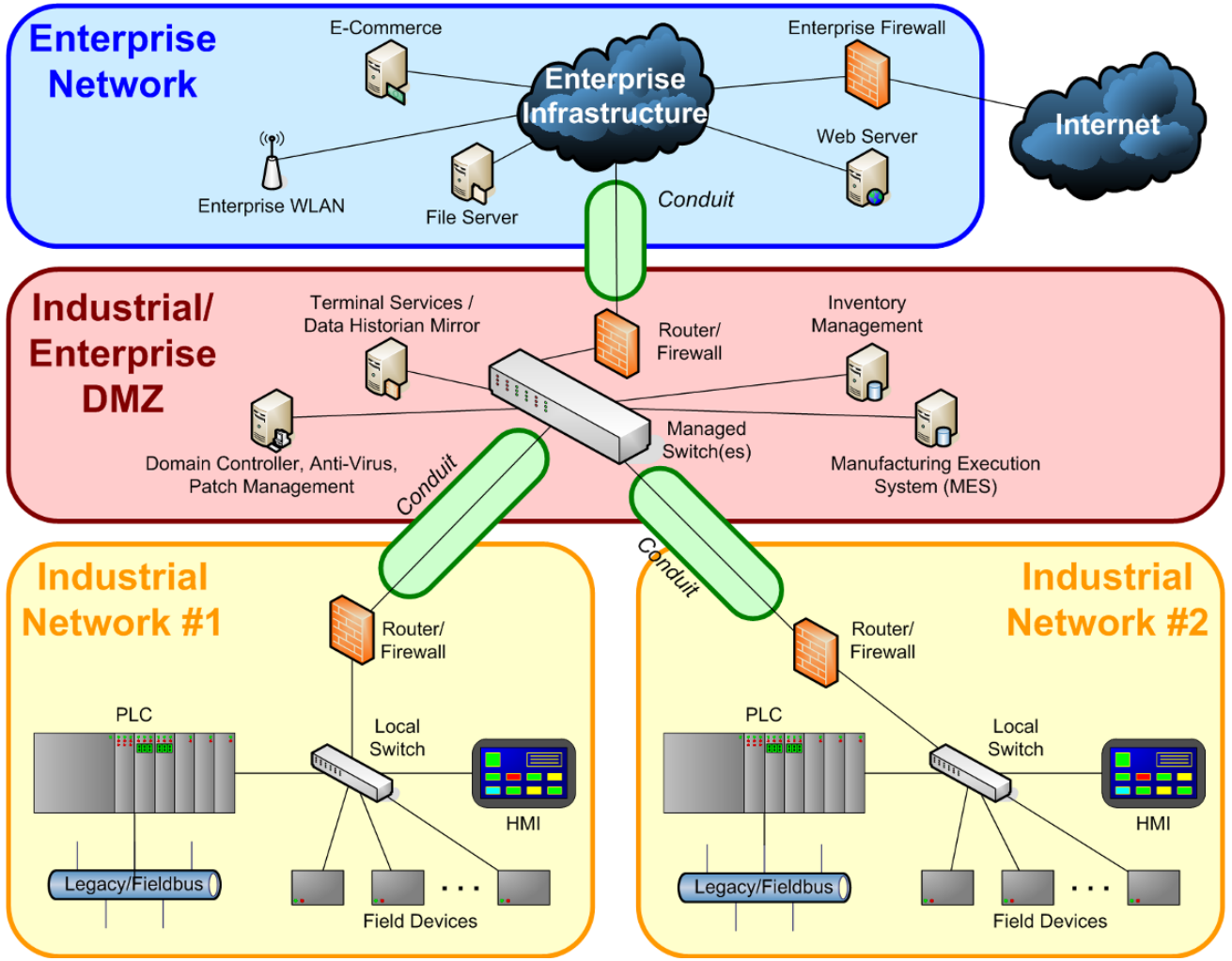


# ISA/IEC62443: Zonas e Conduítes

## DEFESA EM PROFUNDIDADE
## MODELOS DE ZONAS E CONDUÍTES

### CONDUÍTE

Qualquer comunicação entre duas zonas diferentes requer um conduíte de comunicação. Cada conduite garante segurança e define as funções permitidas entre as duas zonas. Não pode haver comunicação entre zonas diferentes que não seja através deste meio.



# ISA/IEC62443: Níveis de Segurança (SLs)

# ISA/IEC62443: Níveis de Segurança (SLs)

**Nível de segurança Target (SLT)**

É o nível de segurança desejado para um determinado sistema. O nível de segurança objetivo é determinado por uma análise de risco a cada sistema, o que identifica o nível de segurança necessário para a operação adequada.

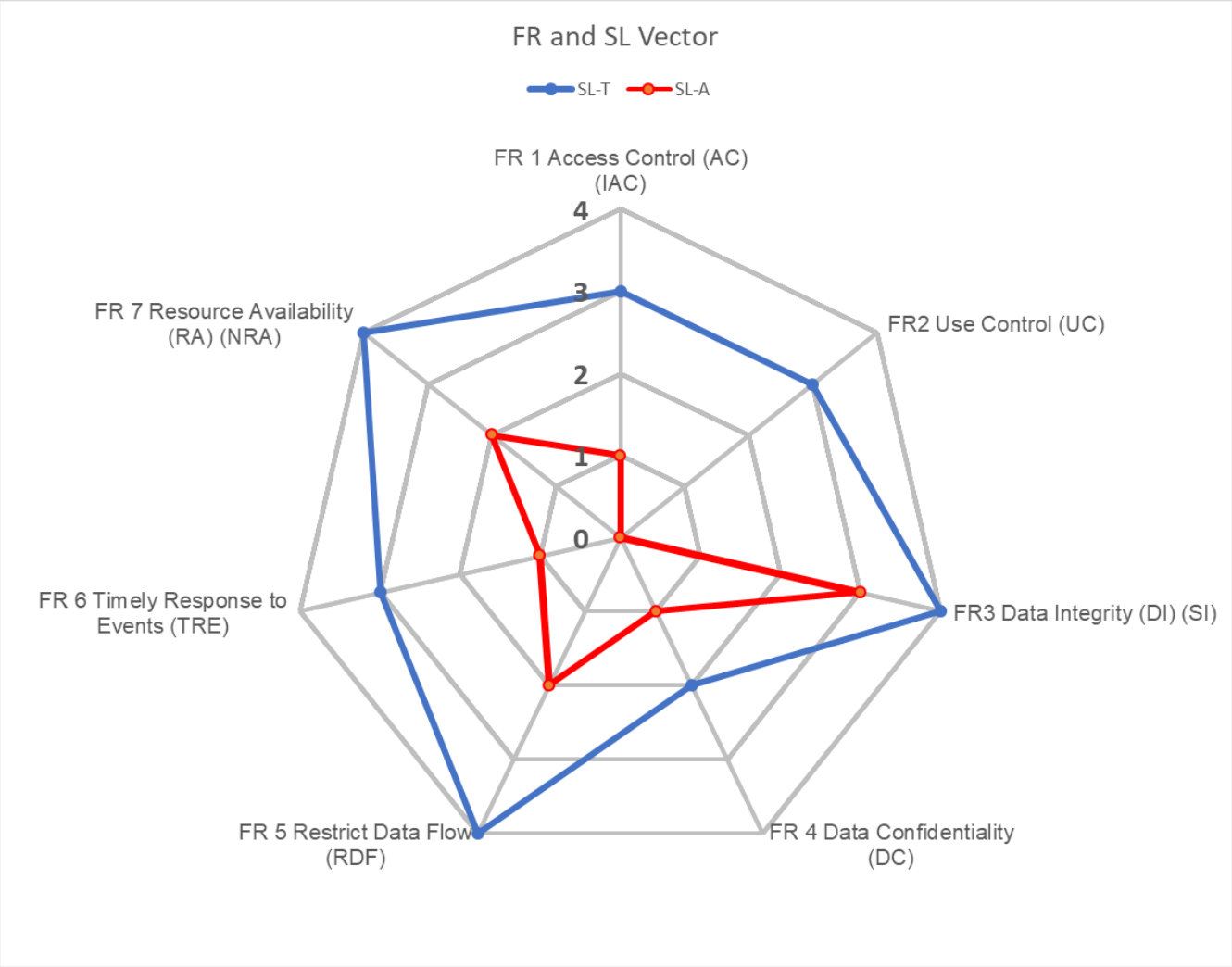
**Nível de segurança Achieved (SLA)**

É o nível de segurança atual para um sistema específico O nível de segurança alcançado deve refletir o nível atual do sistema, quando o sistema já está instalado e em operação. SLA deve ser maior ou igual ao SLT

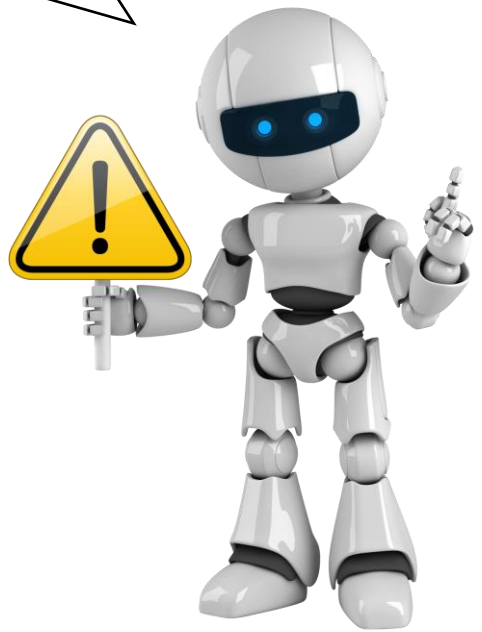
**Nível de segurança Capability (SLC)**

É o nível de segurança que um sistema pode conceder quando configurado corretamente. Este nível permite determinar se um sistema é capaz de atingir o nível de segurança desejado (SLT) sem a necessidade de medidas compensatórias. Se o SLC do sistema não atinge o SLT, será necessário incluir medidas de segurança compensatórias para que o SLA se aproxime do SLT.

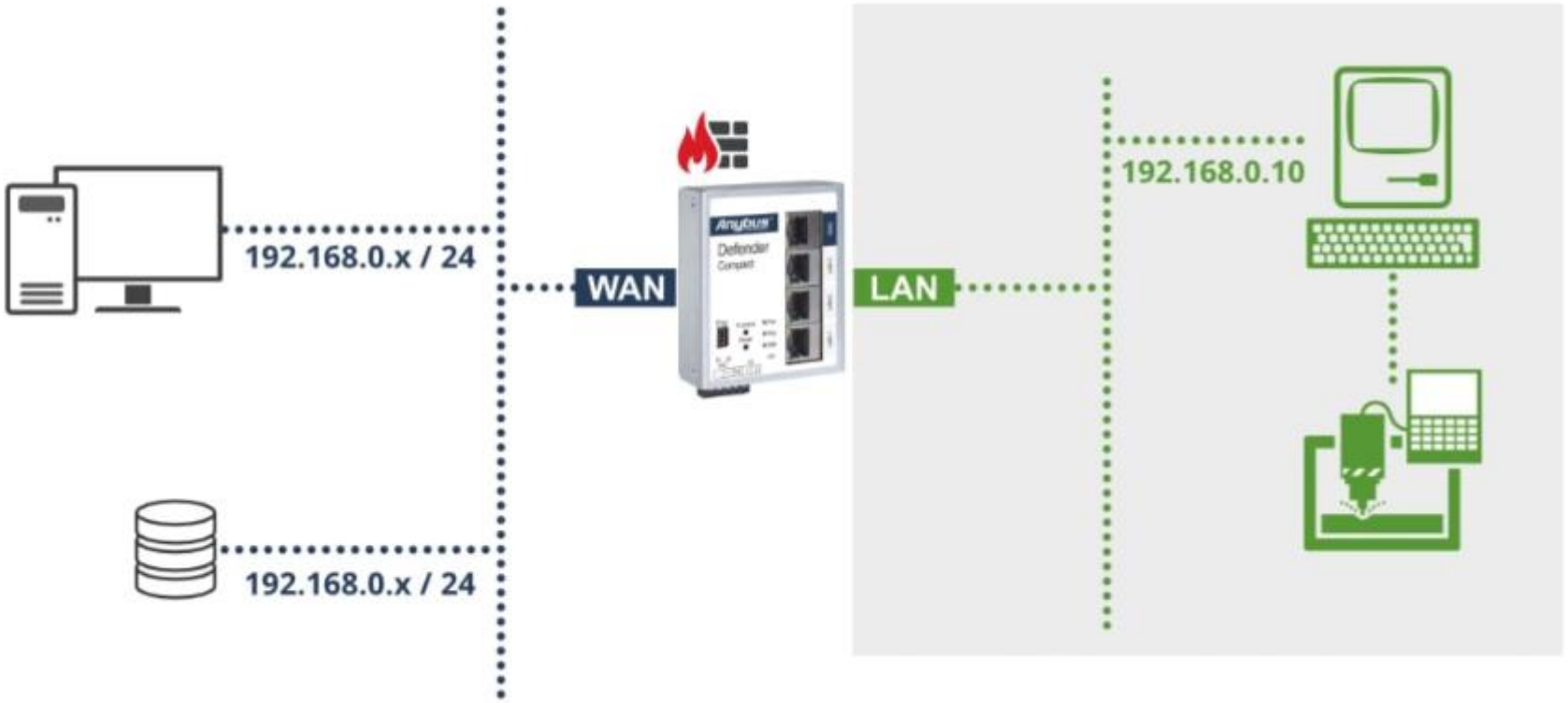
# ISA/IEC62443: Níveis de Segurança (SLs)




Verifique se o dispositivo é certificado **IEC-62443-4-2** para **Cibersegurança OT.**



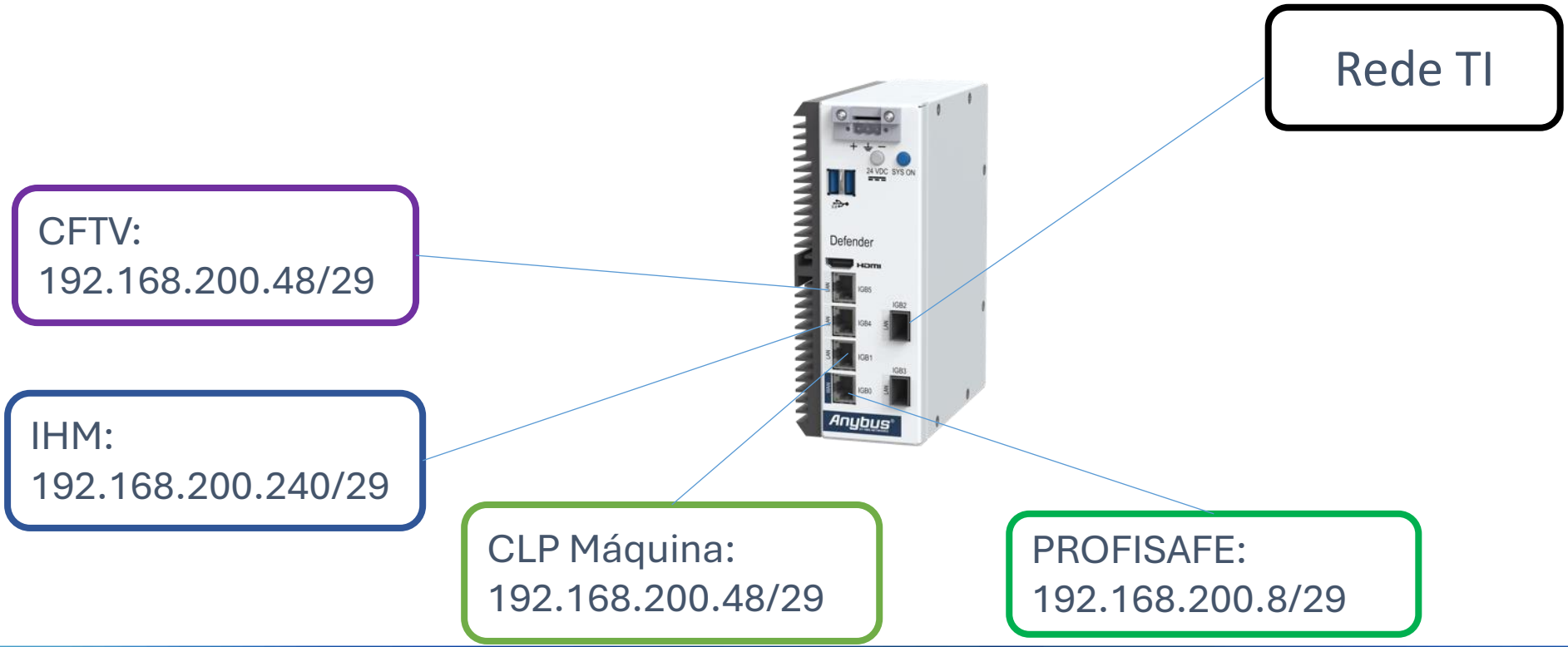
# Camadas de Proteção: Firewall Industrial




O **firewall** monitora e controla o tráfego de rede, bloqueando ou permitindo o acesso com base em regras predefinidas (MAC, IP, pacotes...), protegendo redes internas contra acessos não autorizados e ataques externos.

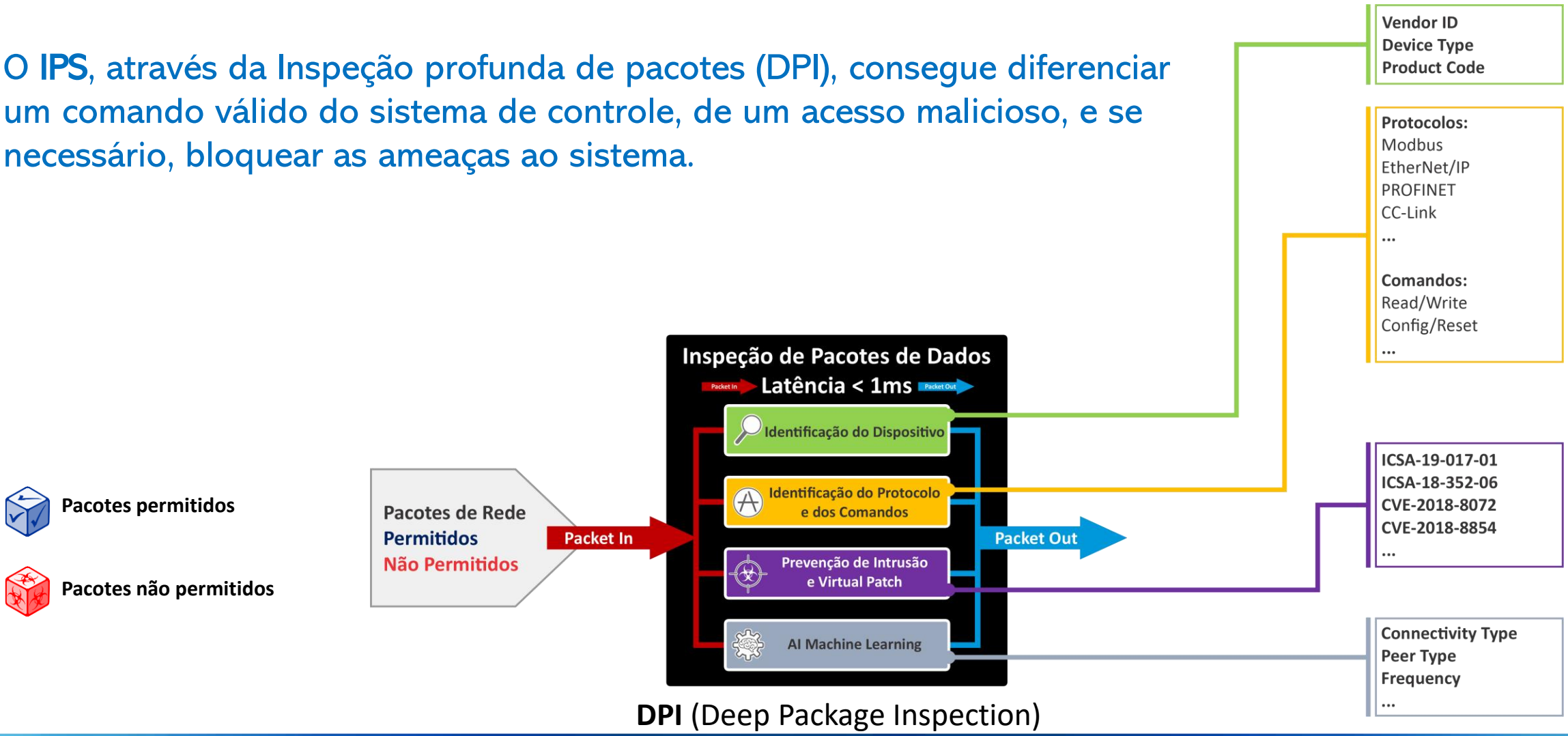
# Camada de Proteção: Firewall Indsutrial - Next Generation

Um **NGFW** (Next-Generation Firewall) combina funções tradicionais de **firewall** com recursos adicionais, como **DPI**, **Virtual patching**, prevenção de intrusões (**IPS**), e proteção contra malware, proporcionando segurança mais robusta e visibilidade detalhada do tráfego de rede.



# Camada de Proteção: IPS – Intrusion Protection System

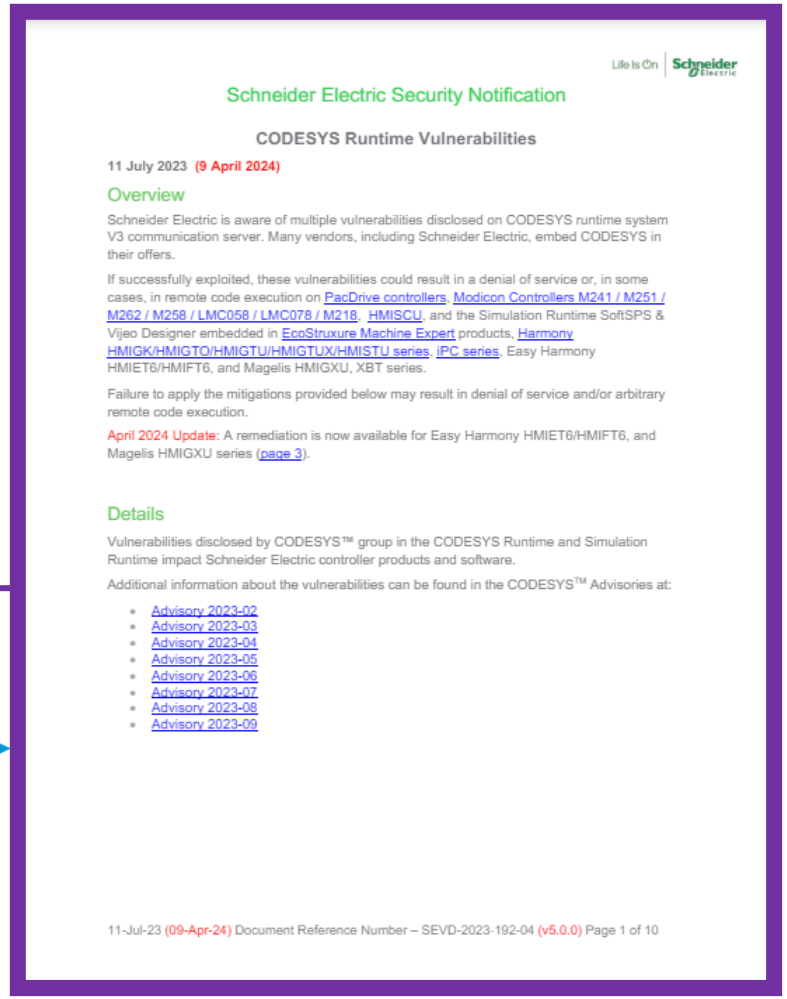
O **IPS**, através da Inspeção profunda de pacotes (DPI), consegue diferenciar um comando válido do sistema de controle, de um acesso malicioso, e se necessário, bloquear as ameaças ao sistema.




**DPI** (Deep Package Inspection)

# Camada de Proteção: Virtual Patching

**Virtual Patching** é uma técnica de segurança que aplica correções para vulnerabilidades de software sem modificar o código original, protegendo sistemas contra ataques até que um patch oficial seja implementado.

Life is On Schneider Electric

Schneider Electric Security Notification

CODESYS Runtime Vulnerabilities

11 July 2023 (9 April 2024)

Overview

Schneider Electric is aware of multiple vulnerabilities disclosed on CODESYS runtime system V3 communication server. Many vendors, including Schneider Electric, embed CODESYS in their offers.

If successfully exploited, these vulnerabilities could result in a denial of service or, in some cases, in remote code execution on PacDrive controllers, Modicon Controllers M241 / M251 / M262 / M258 / LMC058 / LMC078 / M218, HMISCU, and the Simulation Runtime SoftSPS & Vijeo Designer embedded in EcoStruxure Machine Expert products, Harmony HMIGK/HMIGTO/HMIGTU/HMIGTUX/HMISTU series, iPC series, Easy Harmony HMIET6/HMIFT6, and Magelis HMIGXU, XBT series.

Failure to apply the mitigations provided below may result in denial of service and/or arbitrary remote code execution.

April 2024 Update: A remediation is now available for Easy Harmony HMIET6/HMIFT6, and Magelis HMIGXU series (page 3).

Details

Vulnerabilities disclosed by CODESYS™ group in the CODESYS Runtime and Simulation Runtime impact Schneider Electric controller products and software.

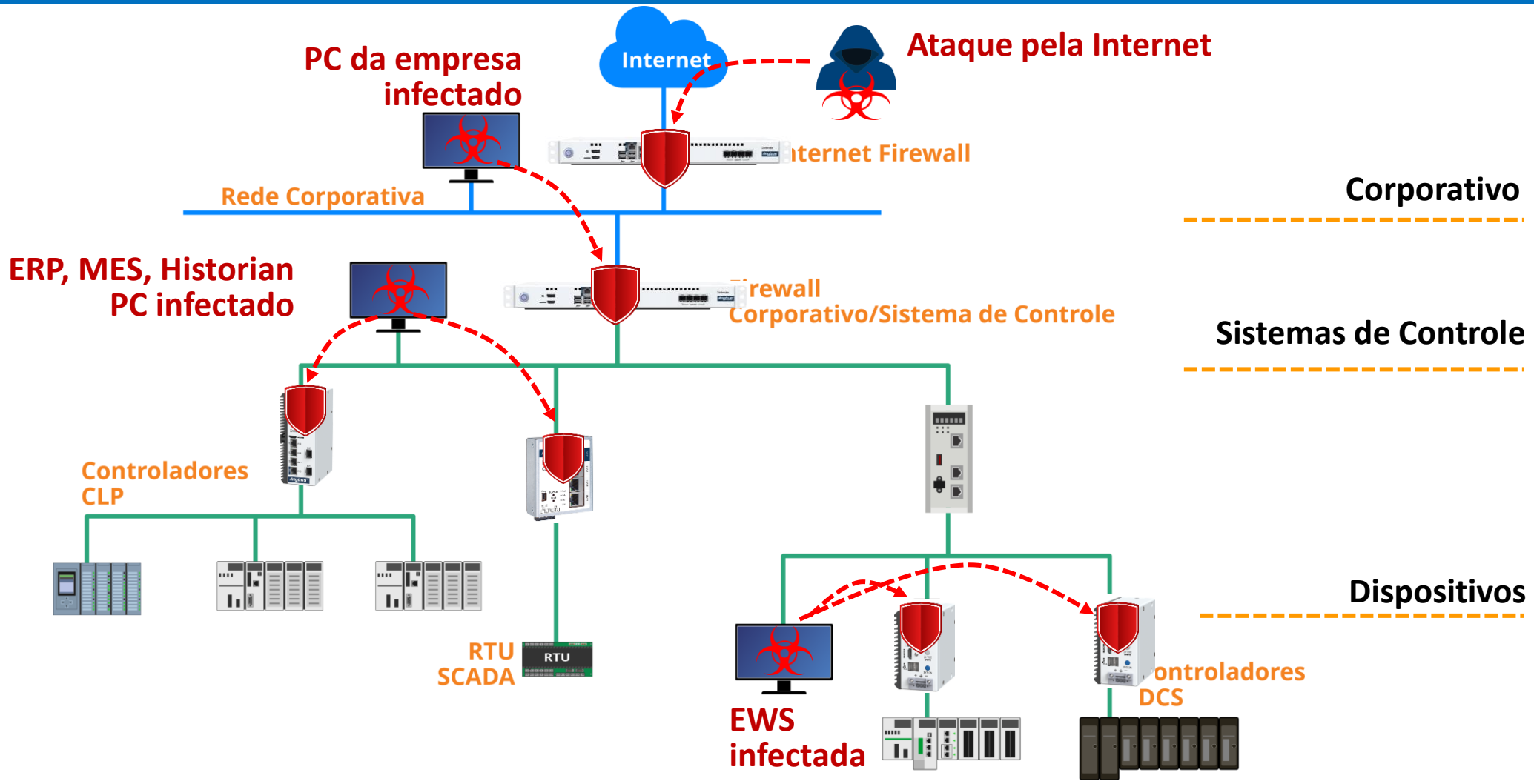
Additional information about the vulnerabilities can be found in the CODESYS™ Advisories at:

- Advisory 2023-02
- Advisory 2023-03
- Advisory 2023-04
- Advisory 2023-05
- Advisory 2023-06
- Advisory 2023-07
- Advisory 2023-08
- Advisory 2023-09

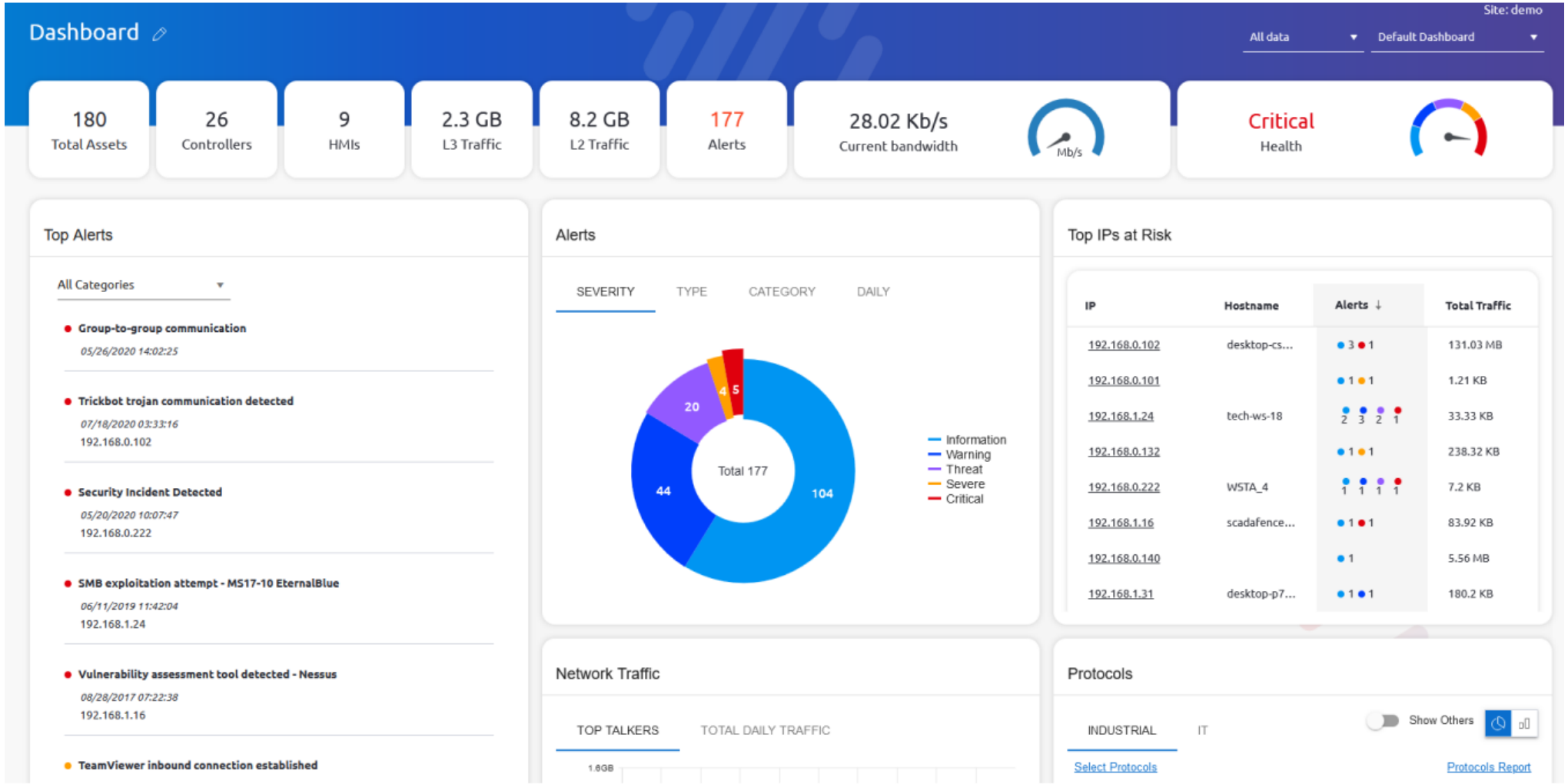
11-Jul-23 (09-Apr-24) Document Reference Number – SEVD-2023-192-04 (v5.0.0) Page 1 of 10

Schneider CyberSecurity Portal

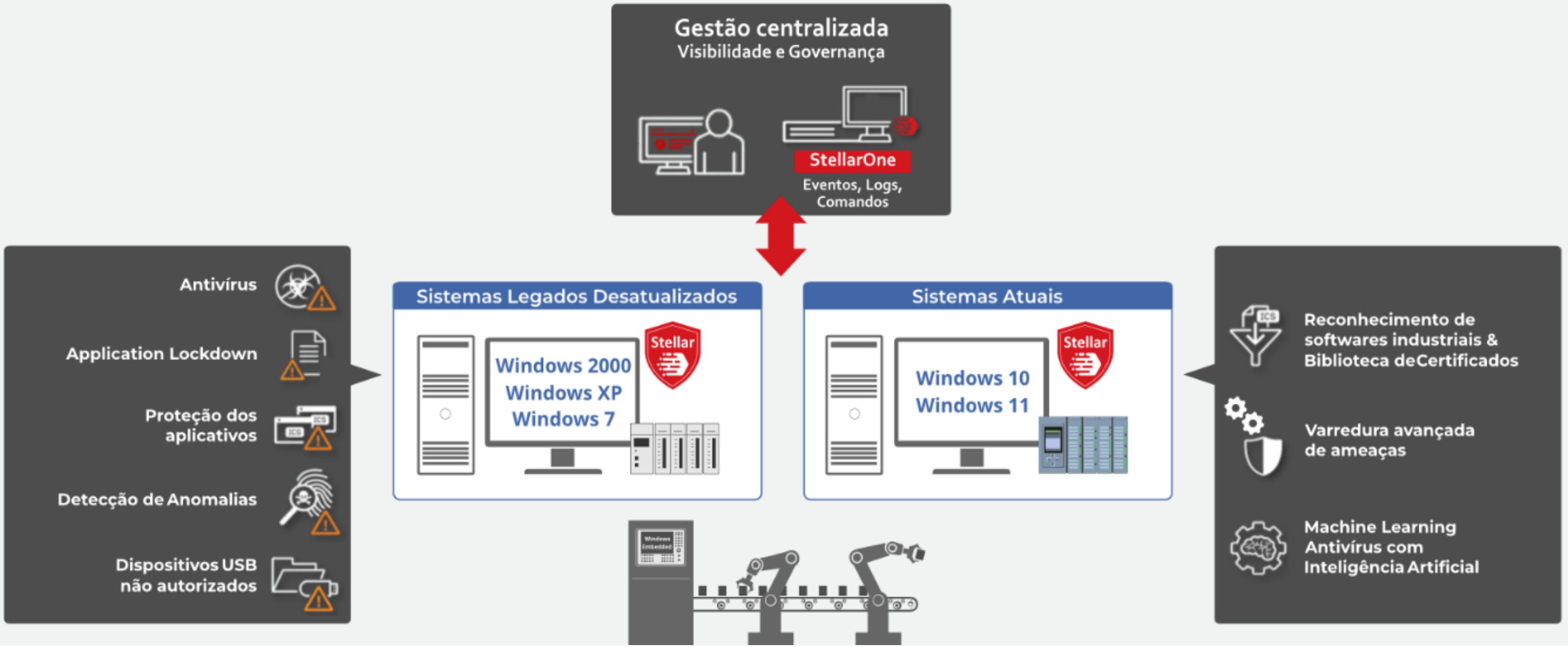
# Camadas de Proteção: Maior Resiliência



# Monitoramento Contínuo do Ambiente OT: IDS



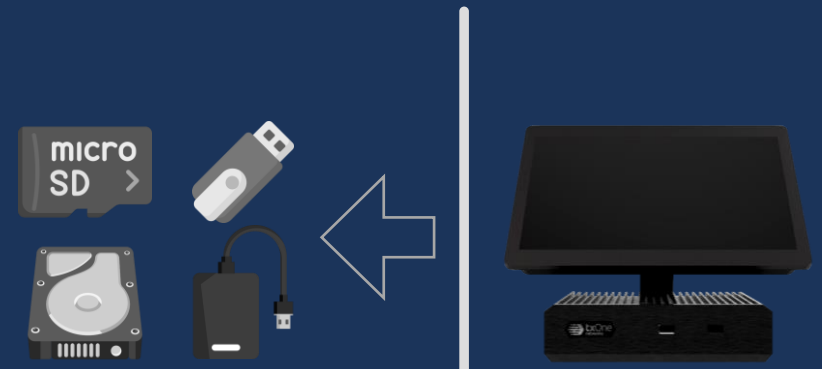
# EDR – Endpoint Detection and Response



# Sanitizador de Mídias e Dispositivos Isolados

## Uma ótima opção para a gestão de dispositivos de terceiros

### Inspeção de Mídias Removíveis




SANITIZADOR DE PENDRIVE, HD EXTERNO...

### Inspeção de Dispositivos Isolados

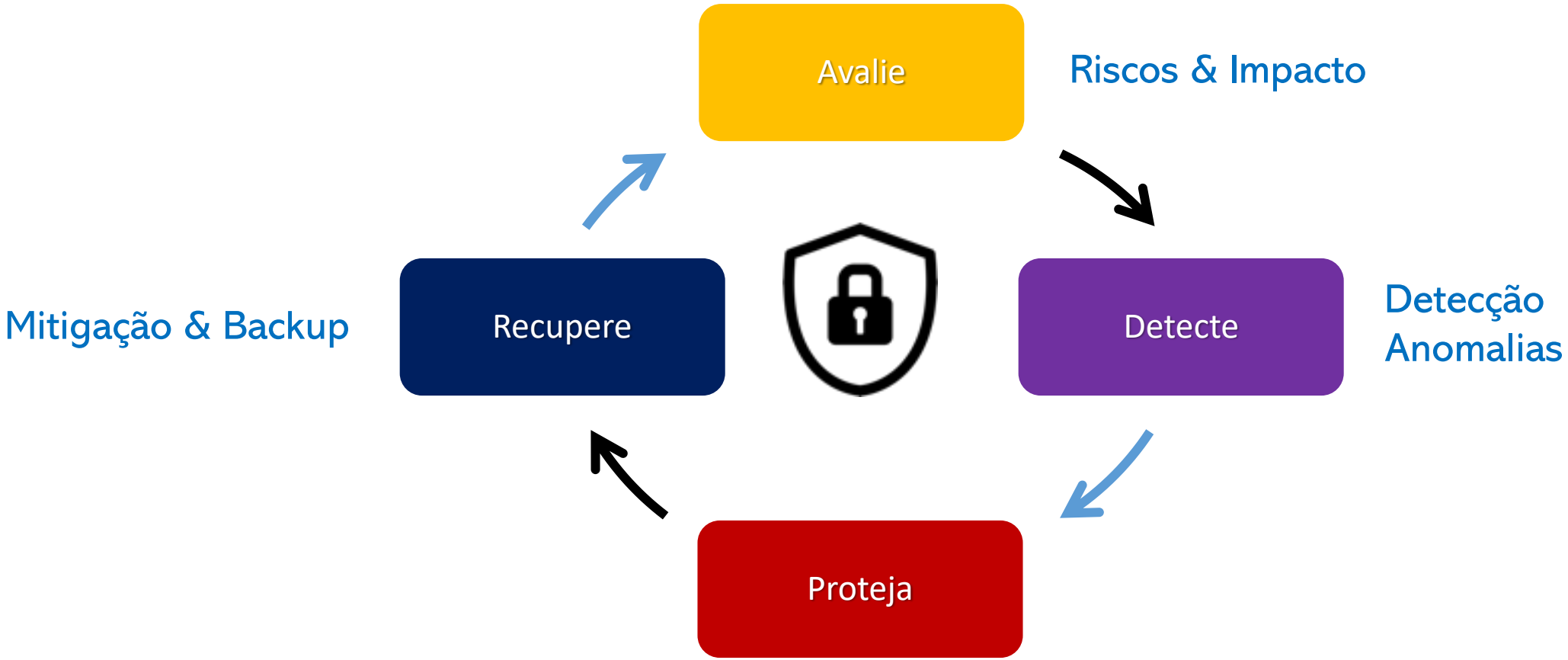

SANITIZADOR DE COMPUTADOR, NOTEBOOK OU IHM, ISOLADOS

# Passos fundamentais para a proteção cibernética no Ambiente OT

- Criação de comitê de cibersegurança para ambiente OT (Envolvendo pessoas de OT e IT)
- Criação de políticas e diretrizes para toda a equipe do ambiente OT e terceiros
- Treinamentos e campanhas recorrentes sobre o tema cibersegurança
- Monitoramento constante do ambiente OT (Sistemas IDS)
- Segmentação de redes OT: Defesa em profundidade (VLANS, Firewalls, IPS)
- Proteção de Endpoints (Softwares anti-malware com funcionalidades de bloqueio de aplicações não utilizadas no equipamento, incluindo proteção de portas USB, e suporte a sistemas legados)
- Inspeção de Ativos internos e externos (Computadores, notebooks, mídias removíveis)
- Security by design: ao desenvolver novos projetos e na aquisição de novos equipamentos

# Assuma a violação e se prepare!


# Assuma a violação e se prepare!



Leandro Cunha e Souza

# Obrigado

leandro@wii.com.br

(11) 99549-6878 / (11) 5561-7488

www.wii.com.br