



Setting the Standard for Automation™

ISA São Paulo Section

Segurança Cibernética no Ambiente Industrial

Daniel Borges Quintão

30 de agosto de 2017

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

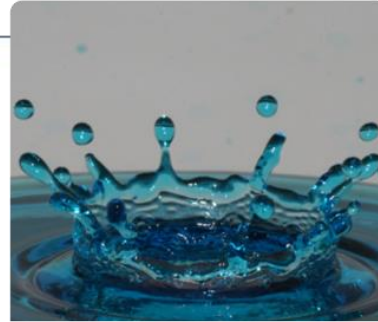
Infraestruturas críticas



Food and Agriculture



Telecommunication



Water and Wastewater



Energy



Critical Manufacturing



Chemical



Public health



Government



Information & Technology



Transportation System



Financial



Emergency Services

Evolução dos Sistemas de Controle Industriais (ICS)



Passado

- Total integração entre sistemas;
- Utilização de soluções de “prateleira”;
- Automação = *Smart factory*.



Presente

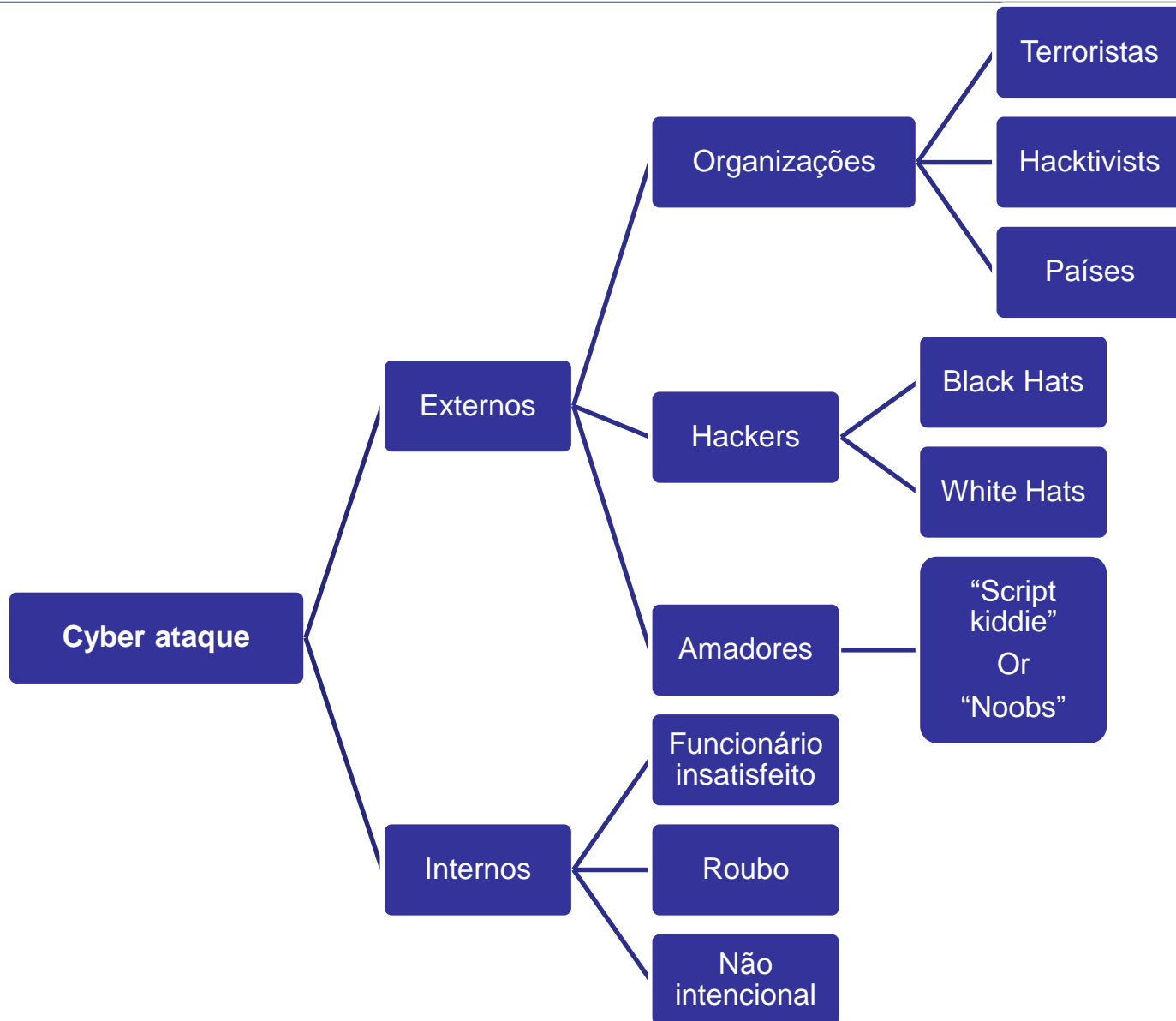


Evolução dos Sistemas de Controle Industriais (ICS)

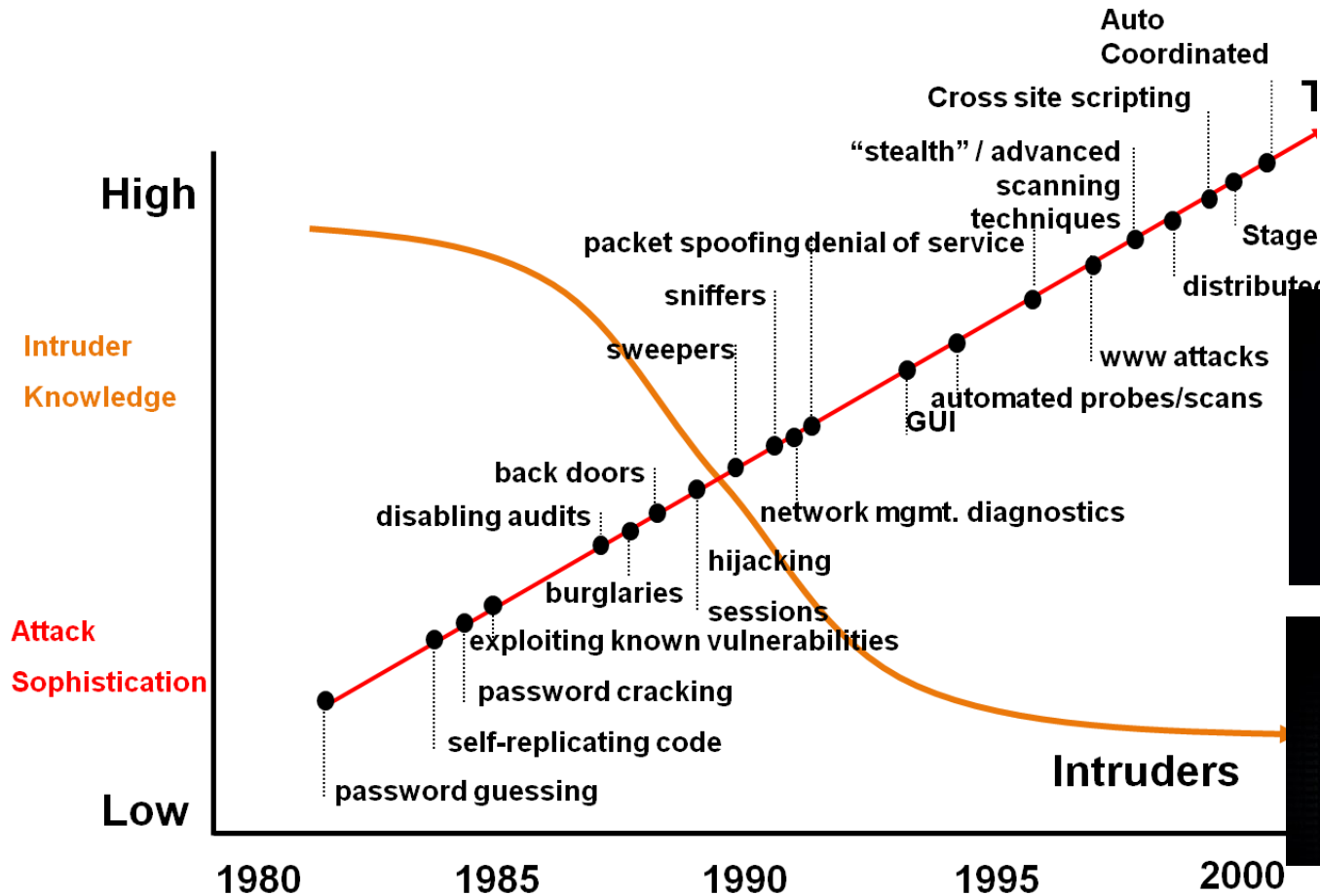


- Virtualização, Cloud computing, Data Analytics, **Industrial IoT**, Docker containers, etc...
 - IoT previsão de 20 bilhões de dispositivos conectados em 2020;
- Incidentes cibernéticos estão ficando cada vez mais comuns no ambiente industrial;
- Quanto mais tecnologias, mais serviços precisam ser gerenciados e mais especialista a equipe deve ser.

Motivação para um ataque cibernético



Conhecimento técnico necessário para realizar um ataque



Sistemas Industriais como alvo



black hat
USA 2017

REGISTER NOW

JULY 22-27, 2017
MANDALAY BAY/LAS VEGAS, NV

REGISTRATION | BRIEFINGS | TRAINING | ARSENAL | SCHEDULE | SPONSORS | SPECIAL EVENTS | CFP | TRAVEL

WELCOME TO BLACK HAT USA 2017

Now in its 20th year, Black Hat is the world's leading information security event, providing attendees with the very latest in research, development and trends. Black Hat USA 2017 kicks off with four days of technical Trainings (July 22-25) followed by the two-day main conference (July 26-27) featuring Briefings, Arsenal, Business Hall, and more.

TRAININGS

Saturday, July 22 - Tuesday, July 25

Often designed exclusively for Black Hat, Trainings provide hands-on skill building for both offensive and defensive hackers. Black Hat Trainings are taught by industry experts with the goal of defining and

BRIEFINGS

Wednesday, July 26 - Thursday, July 27

Learn the very latest in information security risks and trends at The Black Hat Briefings. Security experts will take the stage to share ground breaking research, open-source tools, and zero day exploits. Check back soon for Briefings information.

BUSINESS HALL

Wednesday, July 26 - Thursday, July 27

Network with more than 15,000 InfoSec professionals and evaluate a range of security products and solutions offered by Black Hat sponsors. The 2017 Business Hall brings more opportunities for attendees to meet with vendors, and community engagement.

FTP	83
NetBIOS	39
8081	37
Modbus	23

TOP ORGANIZATIONS

Mobile data webpro.be	66
-----------------------	----

157.157.40.210
Siminn

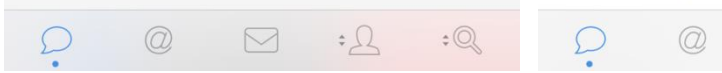
Contact Us | New to Shodan? | Login or Register

```
ification: Schneider Electric BMX PRA0100 v2.6
MX PRA0100
BMXRMS008MP
ation: Project - V7.0  CUNCUN E:\Dropbox (ezChlor)\Client SCADA\Riverton City JV Connectio
sion: 0.0.76
modified: 2016-...

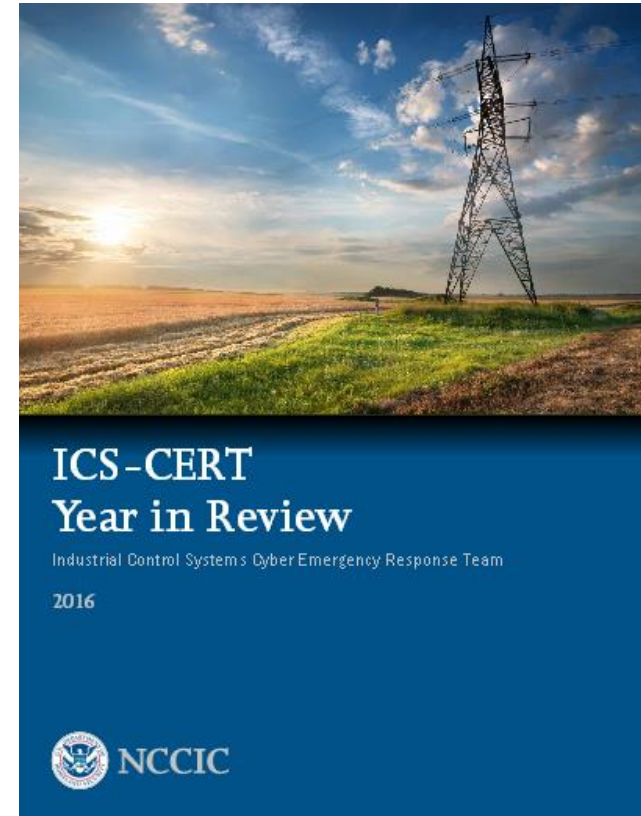
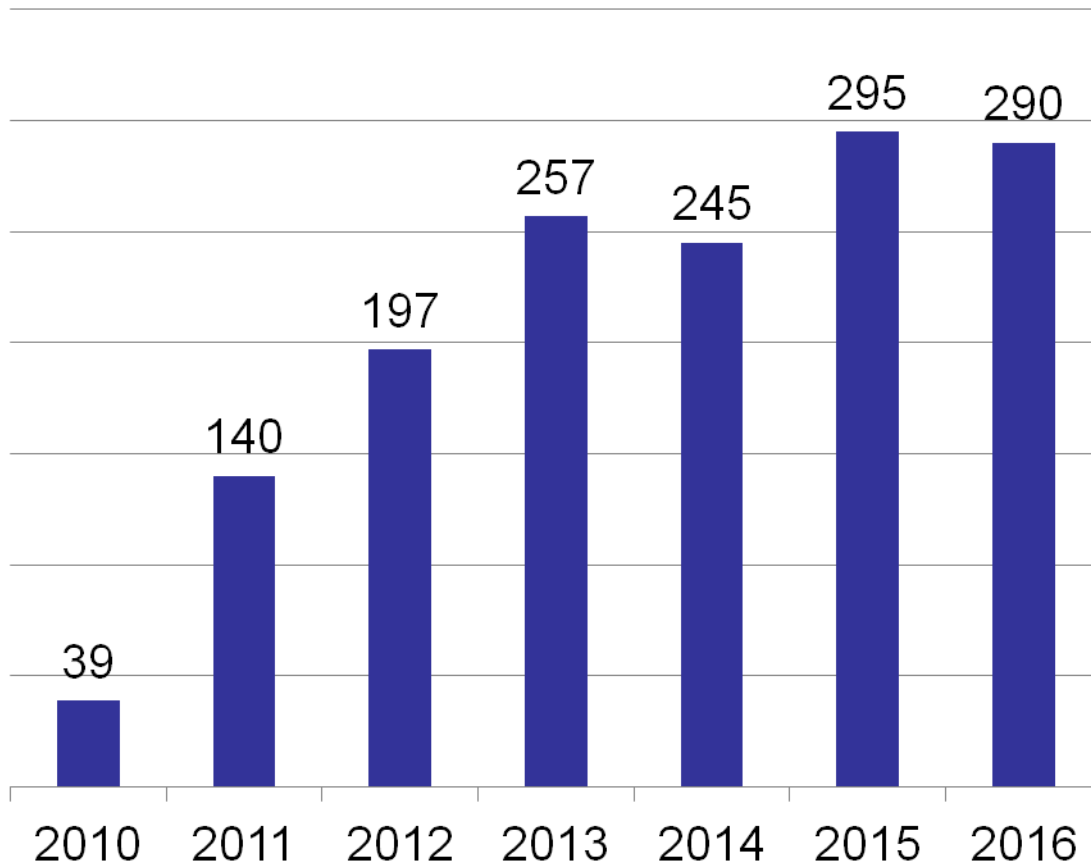
private
xt/html; charset=utf-8
ft-IIS/7.5
t: 4 0 30319
```

ABSOLUTE SCADA: RED TEAM EDITION

New for 2017, this two day course will take a deep-dive into the world of red-teaming industrial control systems; while teaching the fundamentals of SCADA security that are required to successfully penetrate industrial control system environments. The course will also provide students with methodologies through which security research may be performed against SCADA devices in order to identify Oday flaws in some of the world's most critical systems. During the course, students will have the opportunity to engage in live attacks against programmable logic controllers (PLC's) and other industrial control systems, to include activities such as SCADA RTOS firmware reversing, ICS hardware hacking and SCADA protocol fuzzing.



ICS Incident Reports

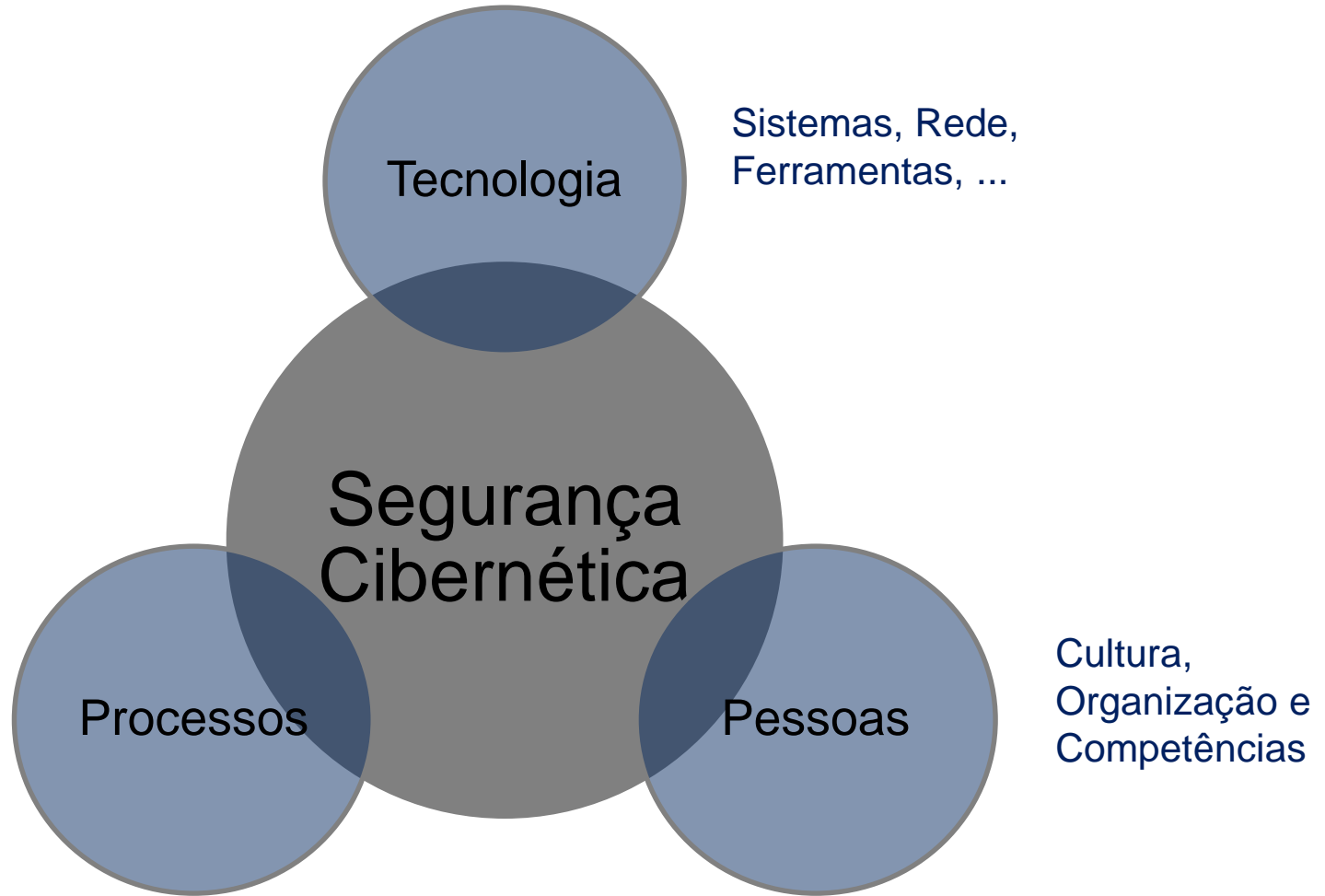


Segurança Cibernética não se restringe a proteção contra intrusão

- ✓ Segurança de Rede;
- ✓ Segurança Física;
- ✓ Continuidade de negócios;
- ✓ Segurança de Informação;
- ✓ Disponibilidade;
- ✓ Proteção dos Ativos;
- ✓ Gestão da Configuração;
- ✓ Gestão de Atualizações;
- ✓ Definição de Responsabilidades;
- ✓ Proteção da Reputação;

Segurança Cibernética é se proteger contra qualquer ameaça que afete a DISPONIBILIDADE, INTEGRIDADE e/ou CONFIDENCIALIDADE do ambiente.

Não existe um único produto que resolva todos os problemas...



Sistemas, Rede,
Ferramentas, ...

Tecnologia

Segurança
Cibernética

Processos

Pessoas

Cultura,
Organização e
Competências

O que fazer,
Como, Onde,
Quando...



Ooops, your files have been encrypted!

English



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

GMT from Monday to Friday

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

<http://petya37h5tbhyvki.onion/P9UUR3>

<http://petya5koahtsf7sv.onion/P9UUR3>

3. Enter your personal decryption code there:

cdSPP4-JUZrRr-pMSxia-gXpmfB-vGWRf-FfMph1-XTUzUn-QmFeeV-ofb94y-HuScaa-rB1gmU-djYAEH-8WEakz-wrQ85W-BbsCzw

If you already purchased your key, please enter it below.

Key: 8x3qrMHjmkRN9jfd

Decrypting sector 83234 of 126464 (65%)

Segurança fim a fim



Identificação das principais ameaças, ativos críticos para a atividade fim da empresa e priorização de riscos de segurança.

Definição dos riscos intoleráveis, seleção de controles apropriados para implantação.

Serviços contínuos para assegurar a efetividade dos controles sobre os riscos existentes.

- **ISA/IEC 62443** Industrial Automation & Control Systems Security series
- **NIST SP 800-53** – Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST SP 800-82** – Guide to Industrial Control Systems (ICS) Security
- NERC CIP, CFATS
- Regulamentações de diversos países para :
 - USA, Canadá, União Europeia, Brasil*, etc..

Daniel Borges Quintão

Senior Engineer – Industrial IT Solutions

Chemtech – A Siemens Company

LinkedIn: <https://www.linkedin.com/in/danielquintao/>

Phone: +55 31 3238 1666

E-mail: daniel.quintao@chemtech.com.br