Klabin

Apresentação

Rodrigo Nunes de Oliveira

Riscos de Segurança Cibernética

AGENDA

Contextualização

1

Incidentes cibernéticos & Normas

2

3

Desafios & Controles

Contextualização

Fomentados pela transformação digital, com objetivo de incorporar o uso da tecnologia digital às soluções de problemas tradicionais, e alinhado com a busca de informações em tempo real, integrações, conectividades entre sistemas ou negócios, empregam um volume cada vez maior de dispositivos que a grande maioria não houve um design nas questões de segurança cibernética.

Saúde 4.0

Industria 4.0

Cidades Inteligentes

Estes sistemas ou dispositivos são alvo crescente de ameaças cibernéticas, nesse contexto, existe o risco de algumas dessas troca de informações serem indesejadas ou mesmo mal-intencionadas, o que pode comprometer o sistema como um todo. Com estes fatores mencionados elevam exponencialmente os riscos das organizações.

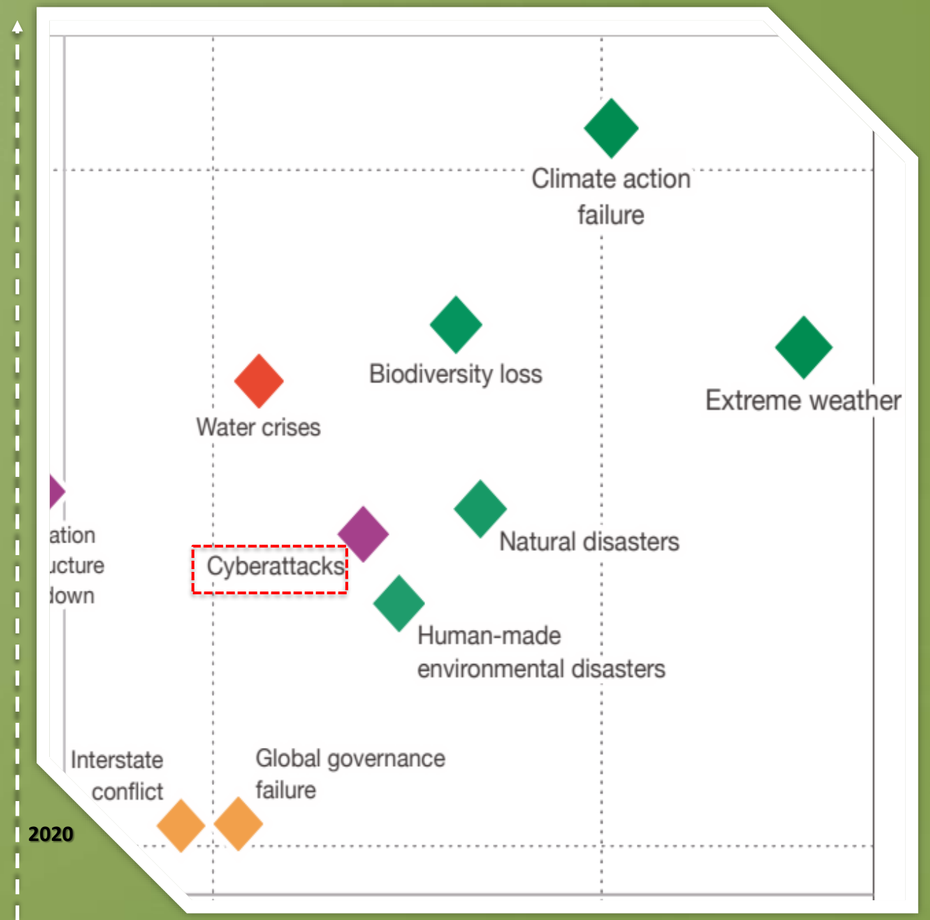
Incidentes cibernéticos

"Os ataques cibernéticos em infraestrutura crítica e ativos industriais estratégicos são agora um dos cinco principais riscos globais ".

World Economic Forum
Global Risk Report, 2019

Custo estimado médio de ataque cibernético

$1.7M



Probabilidade

Fontes: Wired, Wall Street Journal, UK Telegraph, Threat post

Normativas e Referências

IEC62443

Norma de Segurança Cibernética para Sistemas de Automação.

CISA

Fornece amplo conhecimento e práticas de segurança cibernética à infraestrutura criticas.

ISO27001

Norma padrão e de referência Internacional para a gestão da Segurança da informação

SP. 800-82r2

O NIST é um dos laboratórios mais antigos de pesquisa e ciências tecnológicas e suportam a menor das tecnologias às maiores e mais complexas feitas pelo homem.

CIS

Sua missão é "identificar, desenvolver, validar, promover e manter soluções de melhores práticas para defesa cibernética e criar e liderar comunidades para permitir um ambiente de confiança em ciberespaço

Desafios

Ameaças cada vez mais sérias

Apenas 43% utilizam os Firewalls como camada de proteção do SIS (Safety Instrumented System).

TECNOLOGIAS

- ✗ Idade avançada dos ativos;
- ✗ Herança insegura: Sistemas legados nas redes de automação (Windows XP, 2000, 2003);
- ✗ Sistemas de automação não foram feitos para segurança cibernética;

PROCESSOS

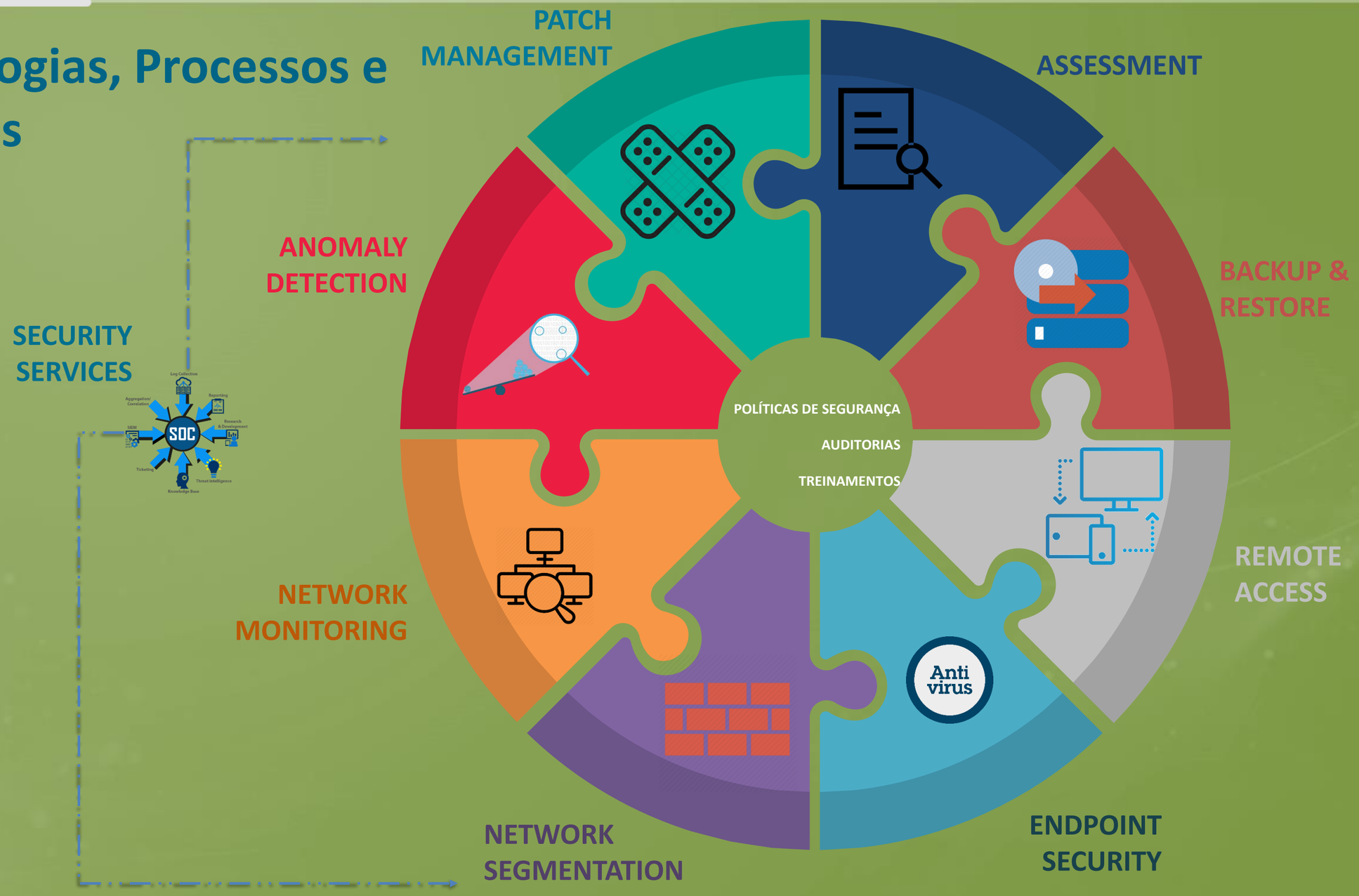
- ✗ Criação, adoção de políticas de segurança e procedimentos de como implementar e manter ativas as proteções;
- ✗ Falta de inventário abrangente dos sistemas de automação;
- ✗ Polarização entre “TI” & “TA”;

PESSOAS

- ✗ Baixo conhecimento com as tecnologias de segurança cibernética;
- ✗ Preocupação inexistente com segurança cibernética;
- ✗ Falta de recursos (pessoas) para atuar com foco em segurança cibernética;

Controles

Tecnologias, Processos e Pessoas



Controles

1 Prepare for Incidents

Identify
Backup
Key partners
Incident Plan
Test your staff's

2 Identify what's happening

Analyse antivirus, audit logs, firewall
Analyse services, program, hardwares
SIEM

3 Resolve the incident

Replacing infected hardware
Restoring services throught backups
Patching Software
Cleaning infected machines
Changing passwords

4 Report the incident

Keep your staff and customers informed
Keep your executive board informed

Learn from the incident

Review actions
Update your incident plan
Reassess your risk

“A segurança cibernética tem tudo a ver com o ***GERENCIAMENTO DE RISCOS”***

#CYBERSEC