TEMPEST talks

2022

TEMPEST talks 2022

CIBERESILIÊNCIA DE REDES DE AUTOMAÇÃO E SISTEMAS INDUSTRIAIS

VITOR SENA

TEMPEST talks 2022

Agenda

01 REVOLUÇÃO INDUSTRIAL E INDUSTRIA 4.0

02 RISCOS E INCIDENTES CIBERNÉTICOS EM OT

03 ARQUITETURA ICS/OT SECURITY

04 ROTINA OPERACIONAL DE OT SECURITY

05 RESULTADOS

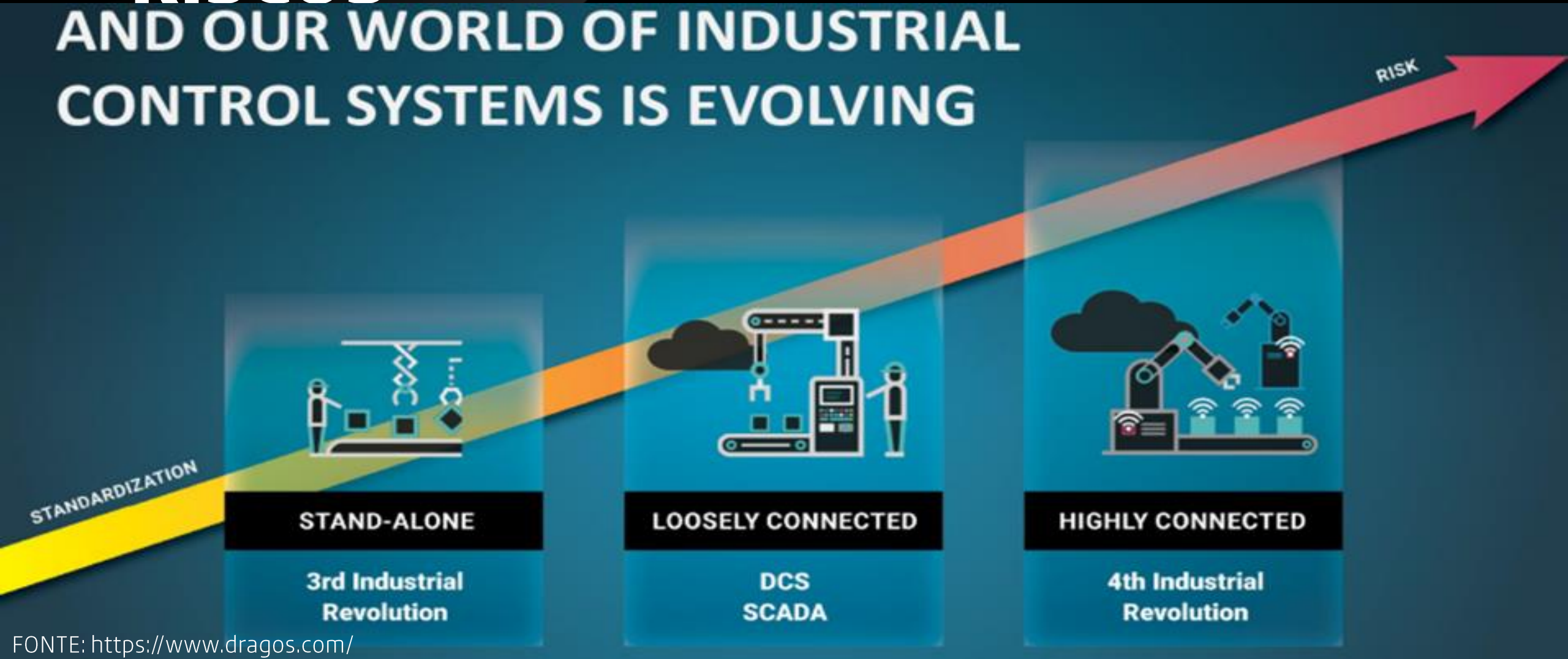
Revolução Industrial

TEMPEST talks 2022

FONTE: SALESFORCE

HIPERCONECTIVIADE E EXPOSIÇÃO A NOVOS RISCOS

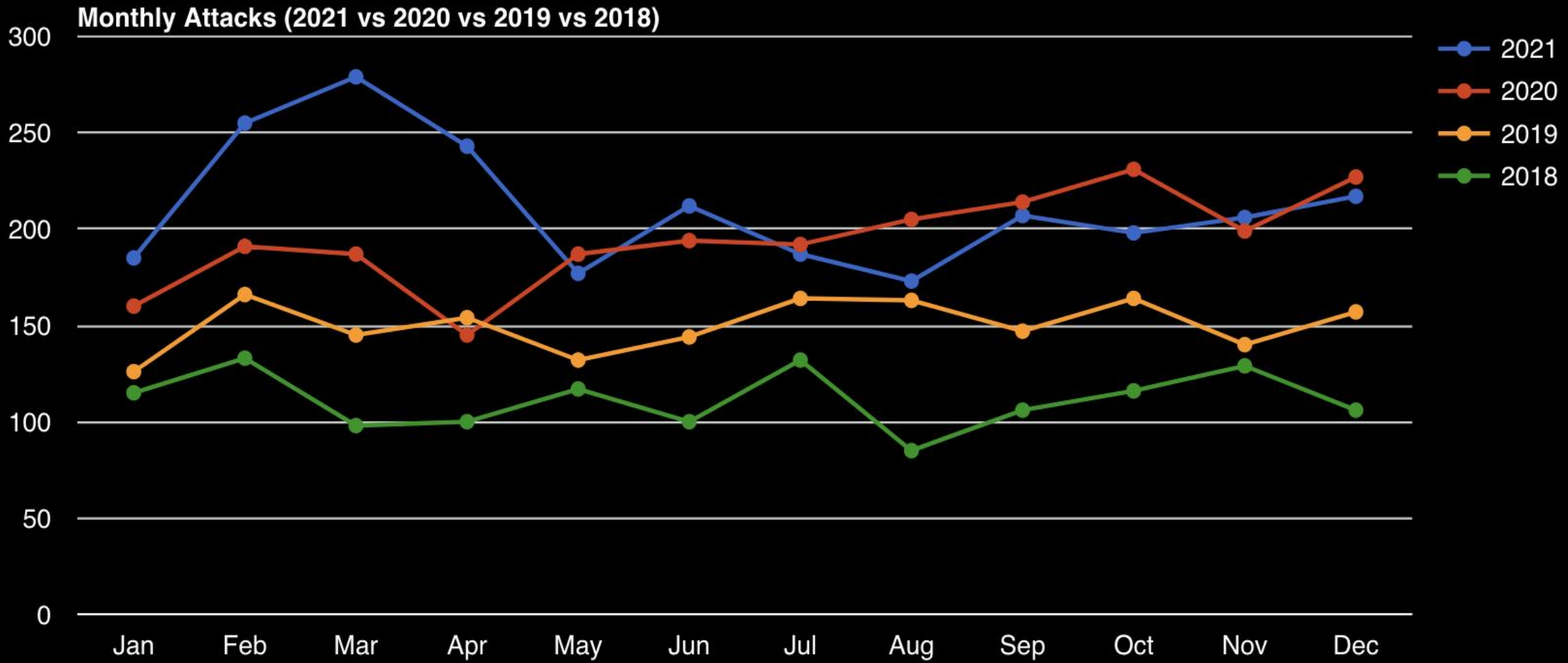
'TEMPEST' talks 2022



FONTE: https://www.dragos.com/

AUMENTO DOS ATAQUES DIRECIONADOS AS REDES INDUSTRIAIS

TEMPEST talks 2022



FONTE: IBM

ESPECIALIZAÇÃO DO ATACANTES

'TEMPEST' talks 2022

THREAT PROLIFERATION: ACTIVITY GROUPS

7 activity groups operate across verticals:

- **MAGNALIUM, PARISITE, HEXANE, CHRYSENE, XENOTIME, DYMALLOY, WASSONITE**

FONTE: https://www.dragos.com/

MATERIALIZAÇÃO E IMPACTOS TANGÍVEIS

TEMPEST talks 2022

PONTOS EM COMUM

TEMPEST talks 2022

KEY LESSONS FROM INCIDENT RESPONSE

Weak Perimeters

100% adversary accessed direct from the internet.

Wrong Information

51% of cases identified existing architecture diagrams were lacking or presented false information.

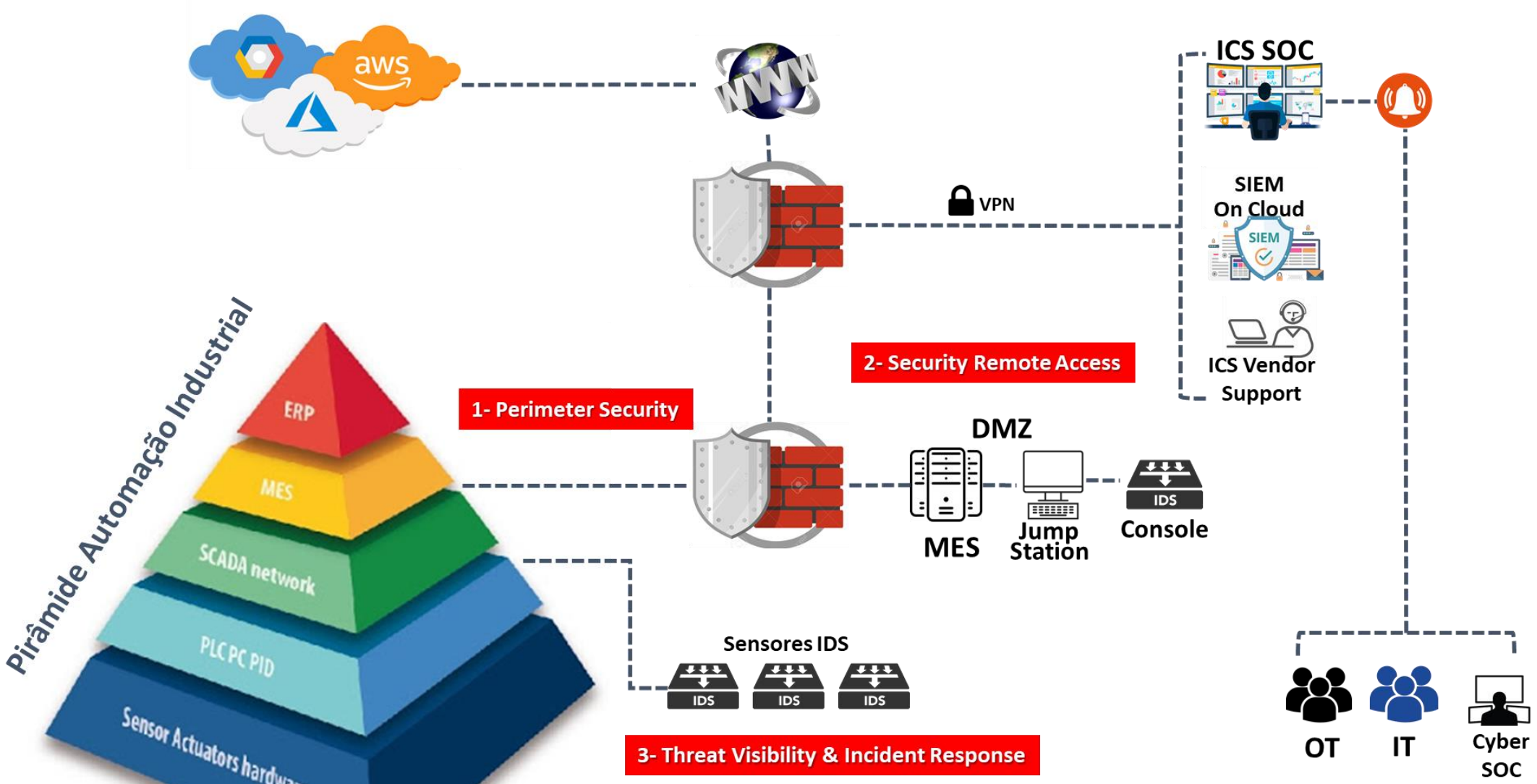
Poor Visibility

0% of IR cases were facilitated by aggregated logging or passive visibility into the ICS networks. Every case involved manual retrieval of logs and distributed analysis.

FONTE: https://www.dragos.com/

ARQUITETURA ICS/OT SECURITY

TEMPEST talks 2022



ROTINA OPERACIONAL ICS/OT SECURITY

TEMPEST talks 2022

POLÍTICAS E DIRETRIZES

DEFINIÃO DE PAPEIS E RESPONSABILIDADE (MATRIZ RACI TI/OT)

DEFINIÃO DE ARQUITETURAS DE REFERÊNCIA

GESTÃO DA OPERAÇÃO DE ICS/OT COM FOCO EM CIBERESILIÊNCIA

1. GESTÃO DE ATIVOS
2. SEGURANÇA FÍSICA E DO AMBIENTE
3. USO DOS DISP. EM REDES INDUSTRIAIS
4. DADOS E BACKUP DE CONFIG
5. CONTROLE DE ACESSOS DE USUÁRIOS
6. SEGURANÇA DOS DISPOSITIVOS


TEMPEST talks
2022
RESULTS

OBRIGADO!!

../in/vitorsena

@Vitor_Sena

TEMPEST talks 2022