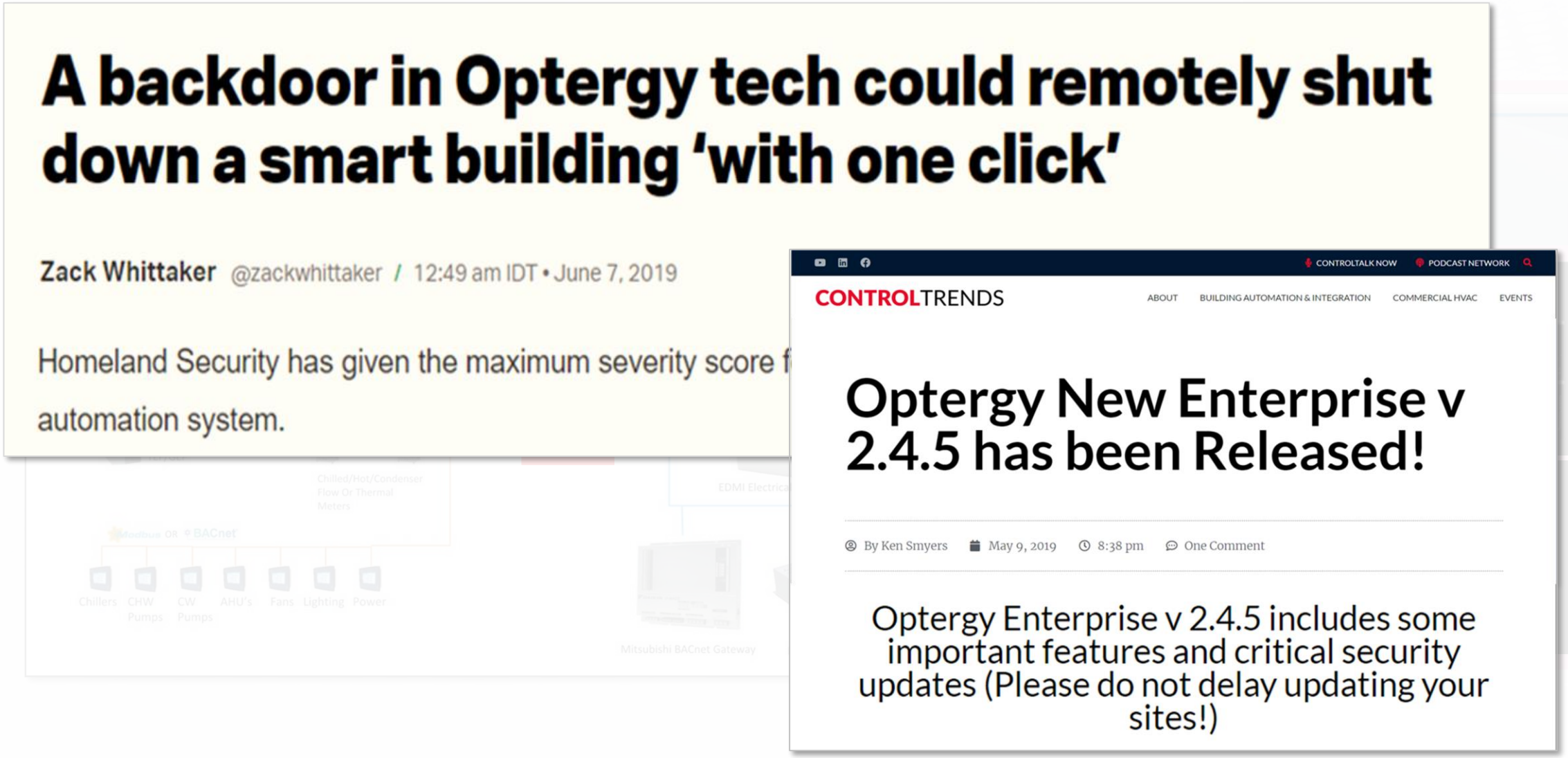
Check Point
SOFTWARE TECHNOLOGIES LTD

PROTEGENDO SUA INFRAESTRUTURA CRÍTICA - IOT/ICS

Ricardo Bacelar | Security Engineer

rbacelar@checkpoint.com

ASSUMINDO CONTROLE EM SMART BUILDING



A backdoor in Optergy tech could remotely shut down a smart building 'with one click'

Zack Whittaker @zackwhittaker / 12:49 am IDT • June 7, 2019

Homeland Security has given the maximum severity score f

automation system.

CONTROLTALK NOW PODCAST NETWORK

CONTROLTRENDS

ABOUT BUILDING AUTOMATION & INTEGRATION COMMERCIAL HVAC EVENTS

Optergy New Enterprise v 2.4.5 has been Released!

By Ken Smyers May 9, 2019 8:38 pm One Comment

Optergy Enterprise v 2.4.5 includes some important features and critical security updates (Please do not delay updating your sites!)

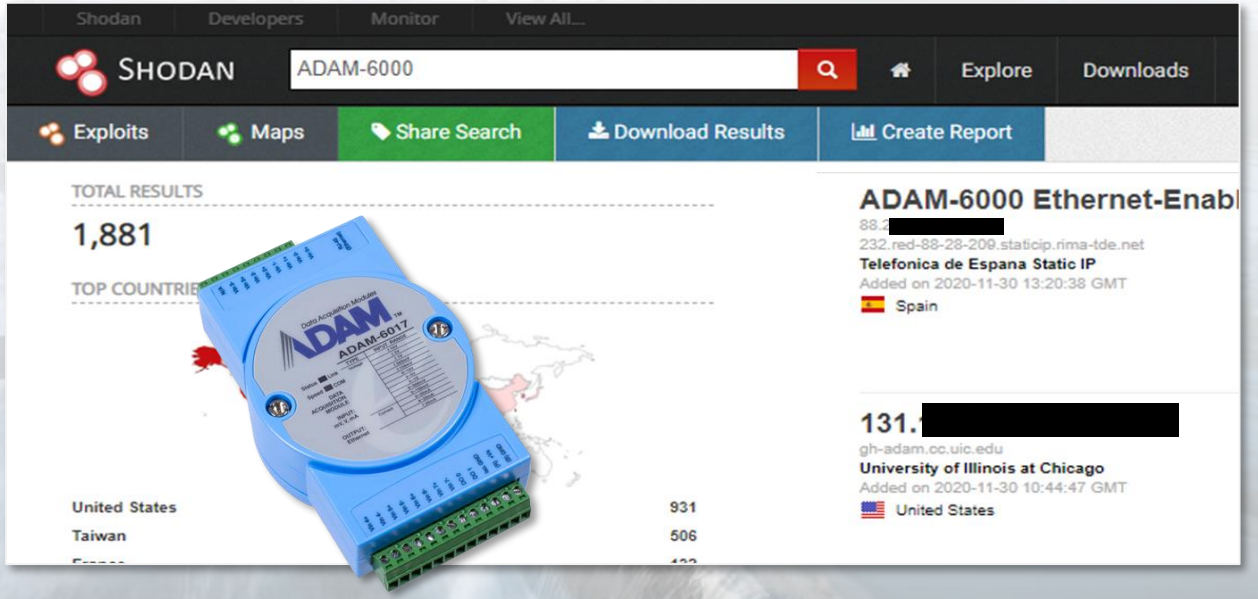
©2021 Check Point Software Technologies Ltd.

ASSUMINDO CONTROLE EM AMBIENTES INDUSTRIAIS

THE TIMES OF ISRAEL

Cyber attacks again hit Israel's water system, shutting agricultural pumps

Illustrative: A worker at the Eshkol Water Filtration Plant in Northern Israel, operated by Israel's National Water Company Mekorot (photo credit: Moshe Shai/Flash90)



Vulnerability Details : CVE-2008-5848

The Advantech ADAM-6000 module has 00000000 as its default password, which makes it easier for remote attackers to obtain access through an HTTP session, and (1) monitor or (2) control the module's Modbus/TCP I/O activity.

©2021 Check Point Software Technologies Ltd.

ASSUMINDO CONTROLE EM AMBIENTES INDUSTRIAIS

US fuel pipeline hackers 'didn't mean to create problems'

By Mary-Ann Russon
Business reporter, BBC News

10 May

©2021 Check Point Software Technologies Ltd.

ASSUMINDO CONTROLE EM AMBIENTES INDUSTRIAIS

CNBC MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV WATCHLIST PRO

JBS cyberattack: From gas to meat, hackers are hitting the nation, and consumers, where it hurts

PUBLISHED WED, JUN 2 2021•1:19 PM EDT | UPDATED FRI, JUN 4 2021•1:38 PM EDT

- The ransomware attack on meat processing giant JBS raises the issue of food security as a national security threat caused by criminal hacking.
- It was just a month ago that the U.S. faced a ransomware attack on the Colonial Pipeline which escalated energy security concerns and led to panic buying of gas by consumers.
- The recent targeted attacks on critical infrastructure controlled by private enterprise are a strategic ploy by hackers to hit companies at key points in supply chains and more effectively leverage ransom demands, and there are consequences in commodities and consumer markets.

©2021 Check Point Software Technologies Ltd.

Check Point IoT Protect

PREVENIR. ADAPTAR. EM TODO LUGAR.

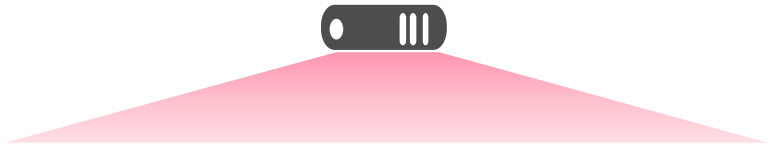
DESCOBERTA IoT & ANÁLISE DE RISCO

SEGMENTAÇÃO ZERO-TRUST

PREVENÇÃO DE AMEAÇAS IoT

©2021 Check Point Software Technologies Ltd.

Classificação de ativos e Auto-Discover



Industrial Control System

HMI

PLC

RTU

SCADA

sensor

Smart Building

Smart Thermostat

IP Camera

Smart elevator

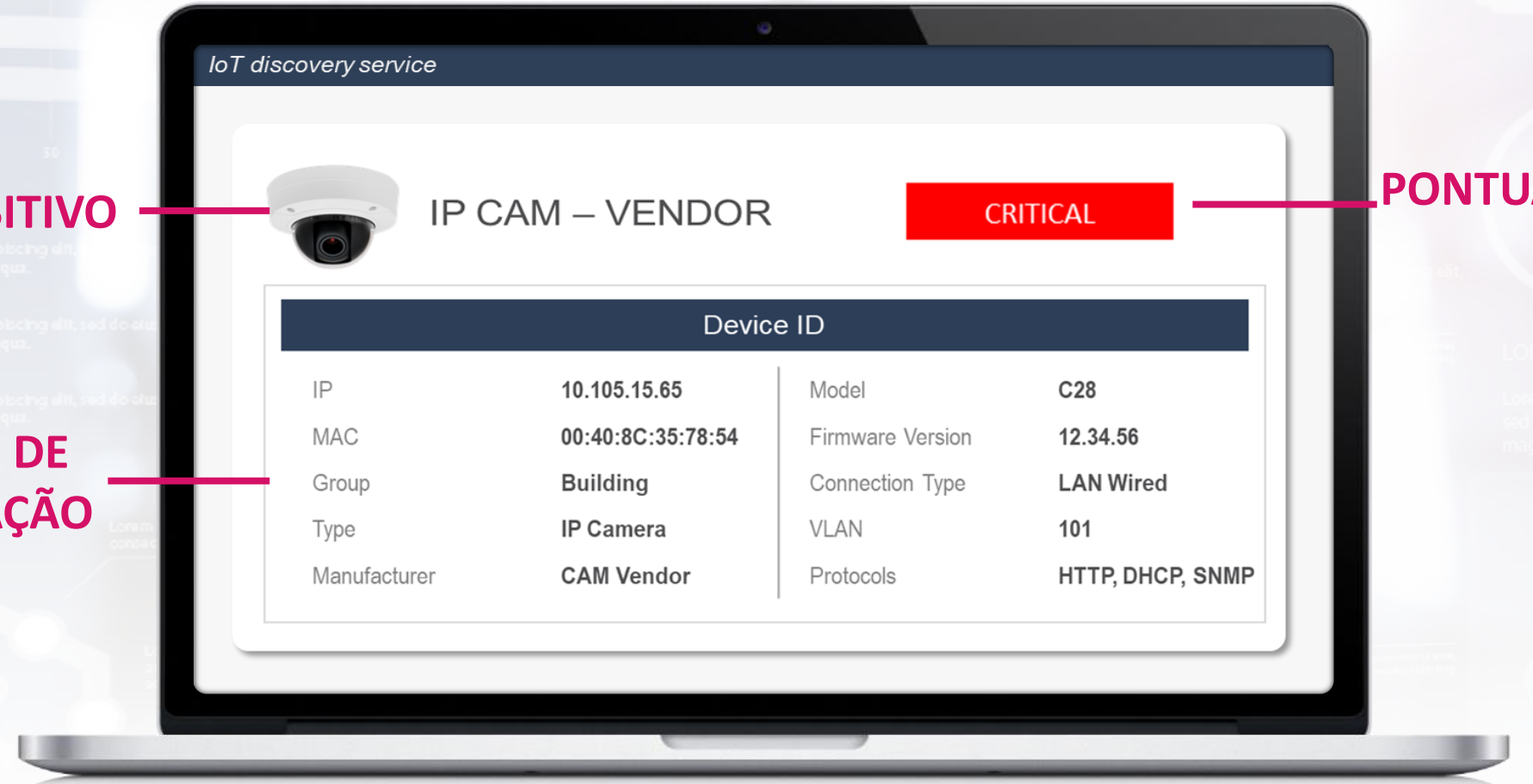
©2021 Check Point Software Technologies Ltd.

Forneça detalhes de identidade granular para cada dispositivo

TIPO DE DISPOSITIVO

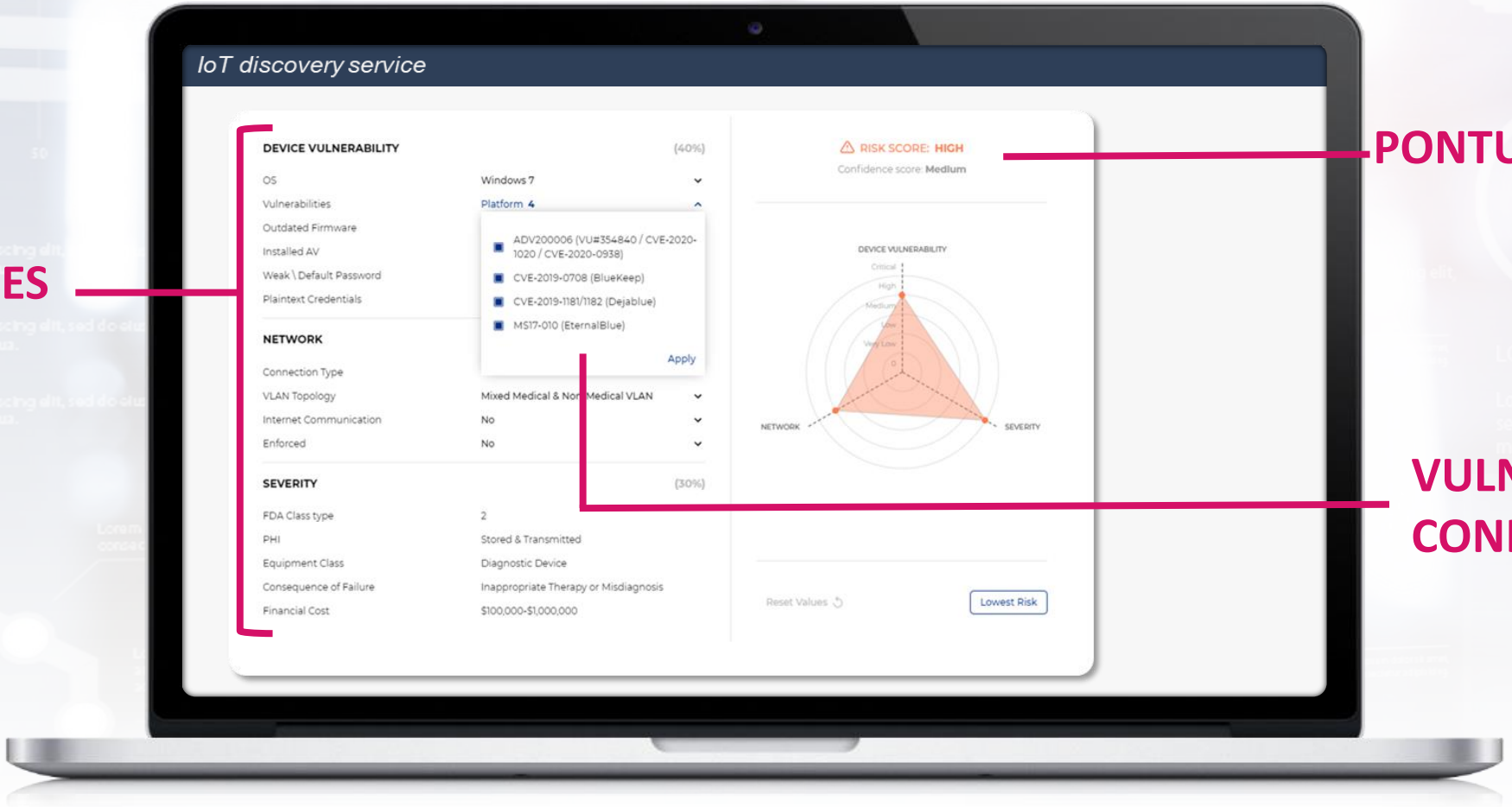
DETALHES DE IDENTIFICAÇÃO

PONTUAÇÃO DE RISCO



©2021 Check Point Software Technologies Ltd.

Analisar a Postura de Risco do Dispositivo



INDICADORES DE RISCO

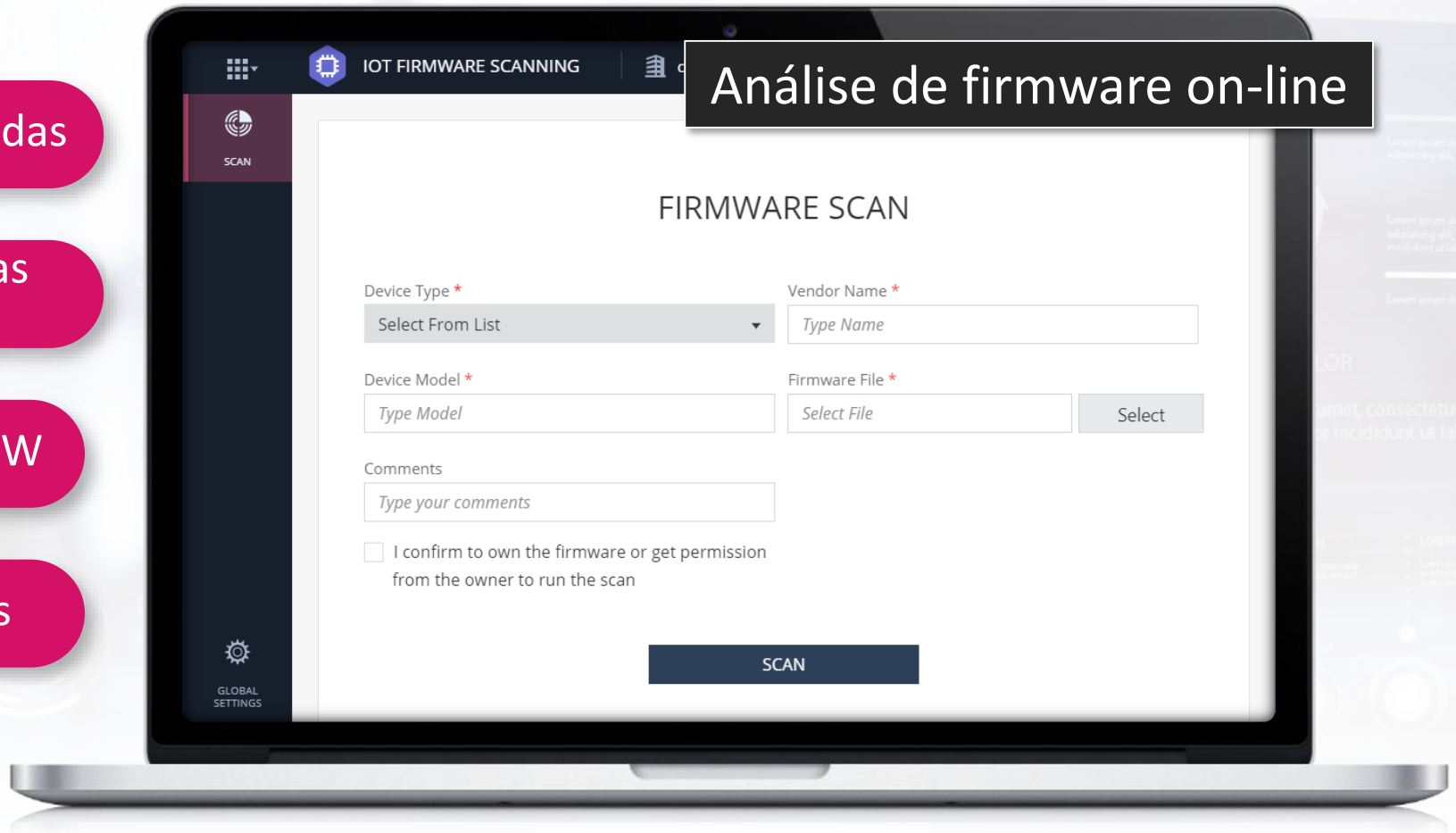
PONTUAÇÃO DE RISCO

VULNERABILIDADES CONHECIDAS

©2021 Check Point Software Technologies Ltd.

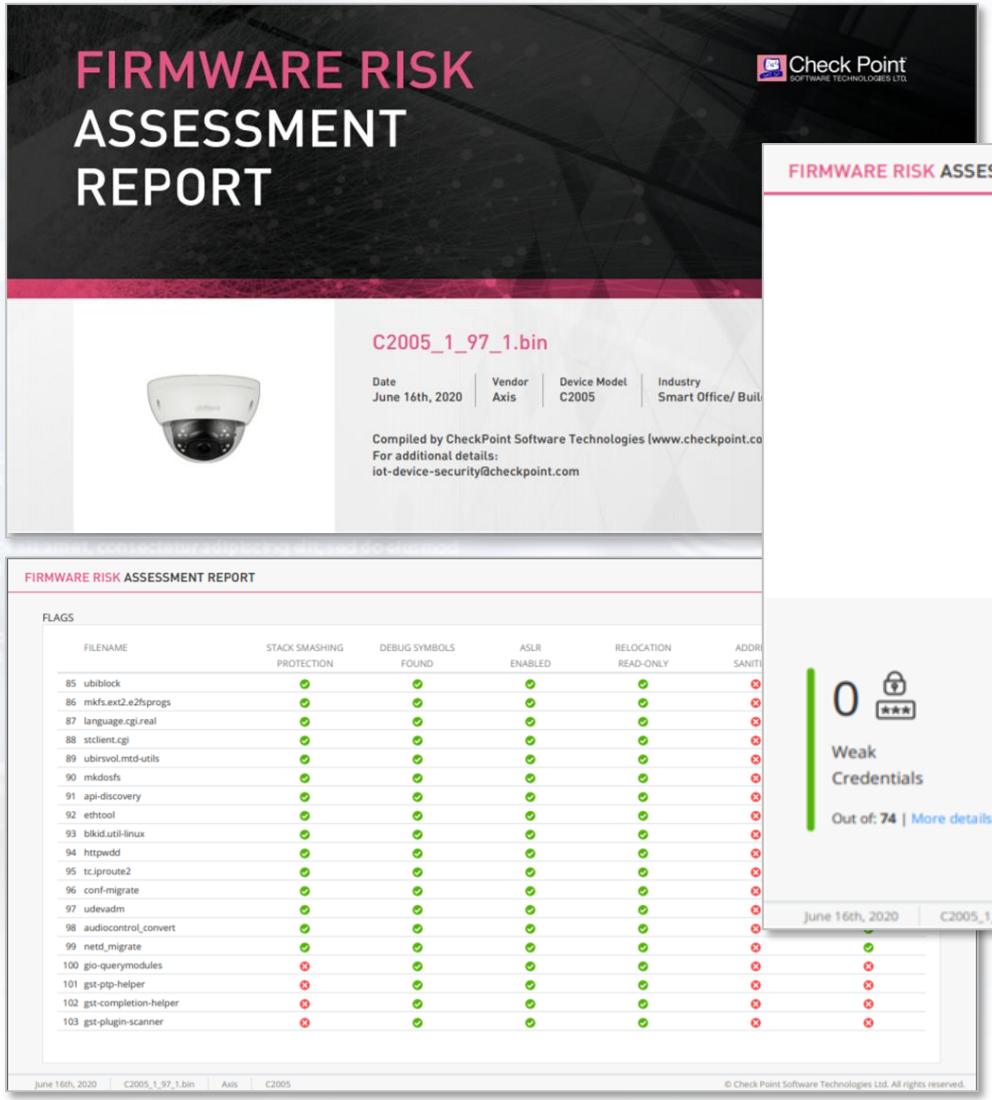
Implantar dispositivos com firmware seguro para uso

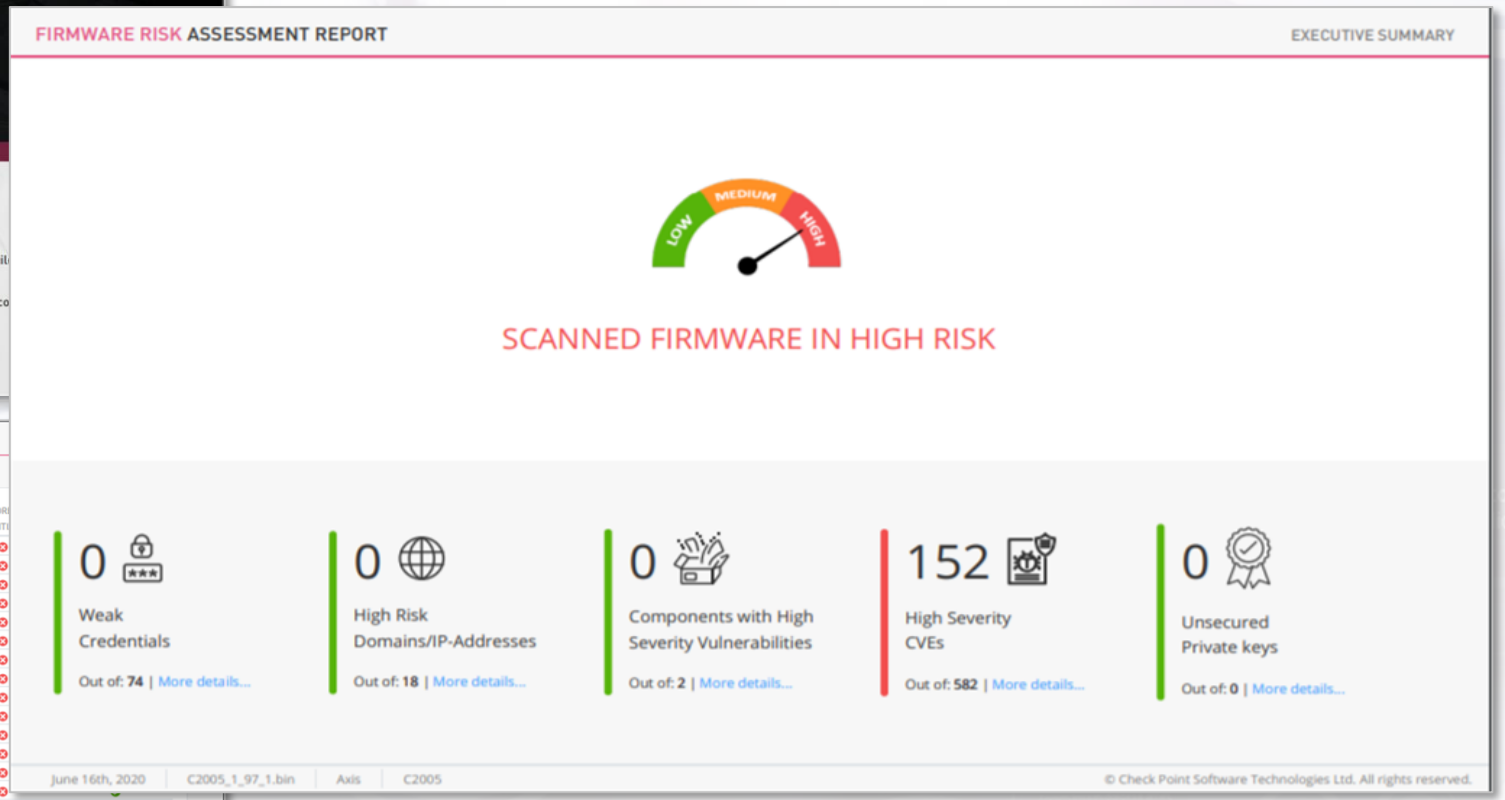
- Credenciais fracas/Conhecidas
- Vulnerabilidades conhecidas (CVEs)
- Configurações erradas de SW
- Domínios listados suspeitos



©2021 Check Point Software Technologies Ltd.

Relatório de Avaliação de Risco do Firmware

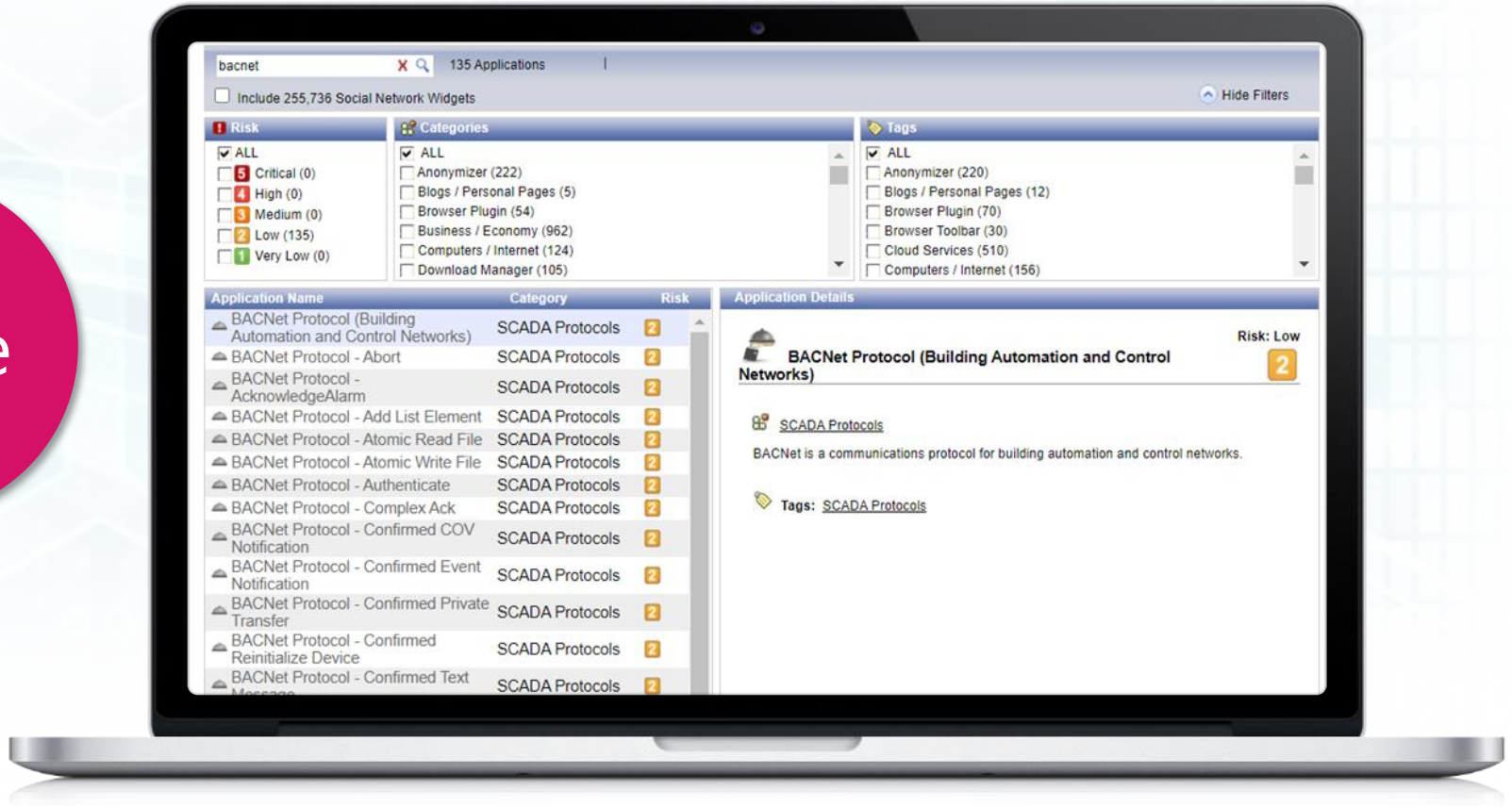




©2021 Check Point Software Technologies Ltd.

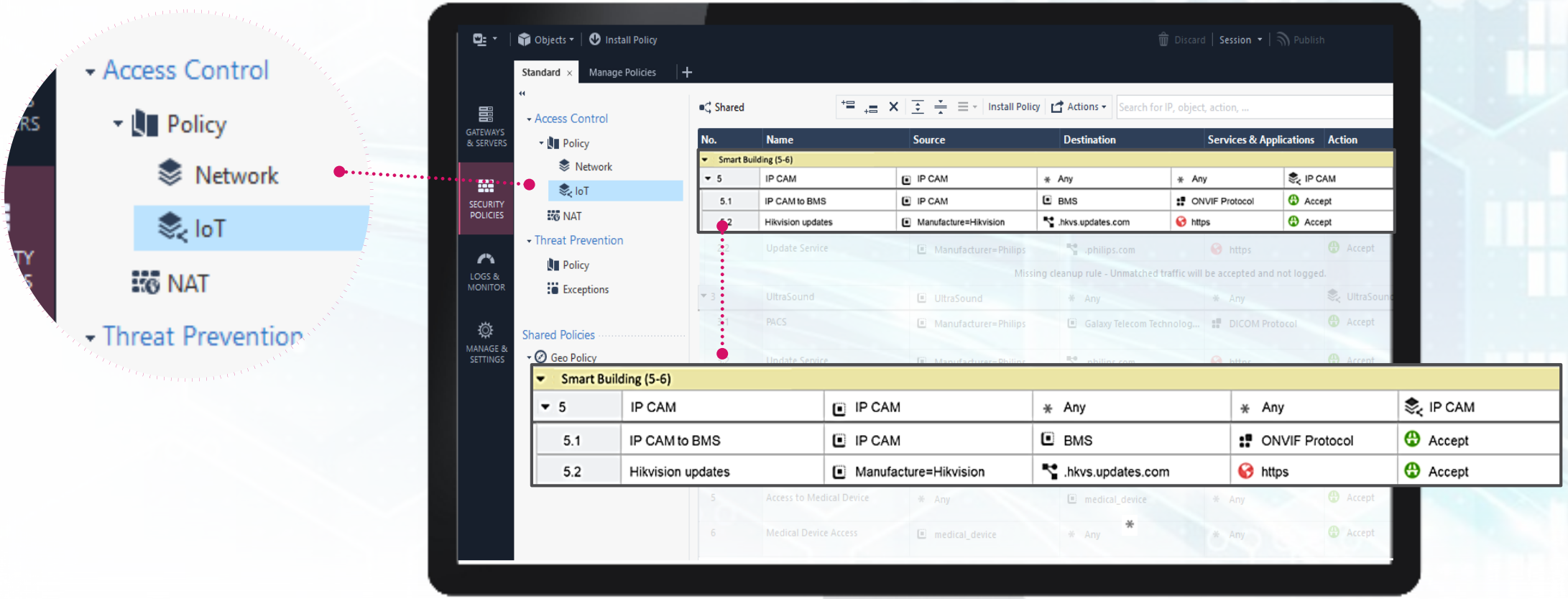
Crie Políticas Perfeitamente Adequadas com o Controle de Aplicações Mais Amplo do Setor

Mais de 1,600
Aplicações, Protocolos e Comandos de IoT e OT



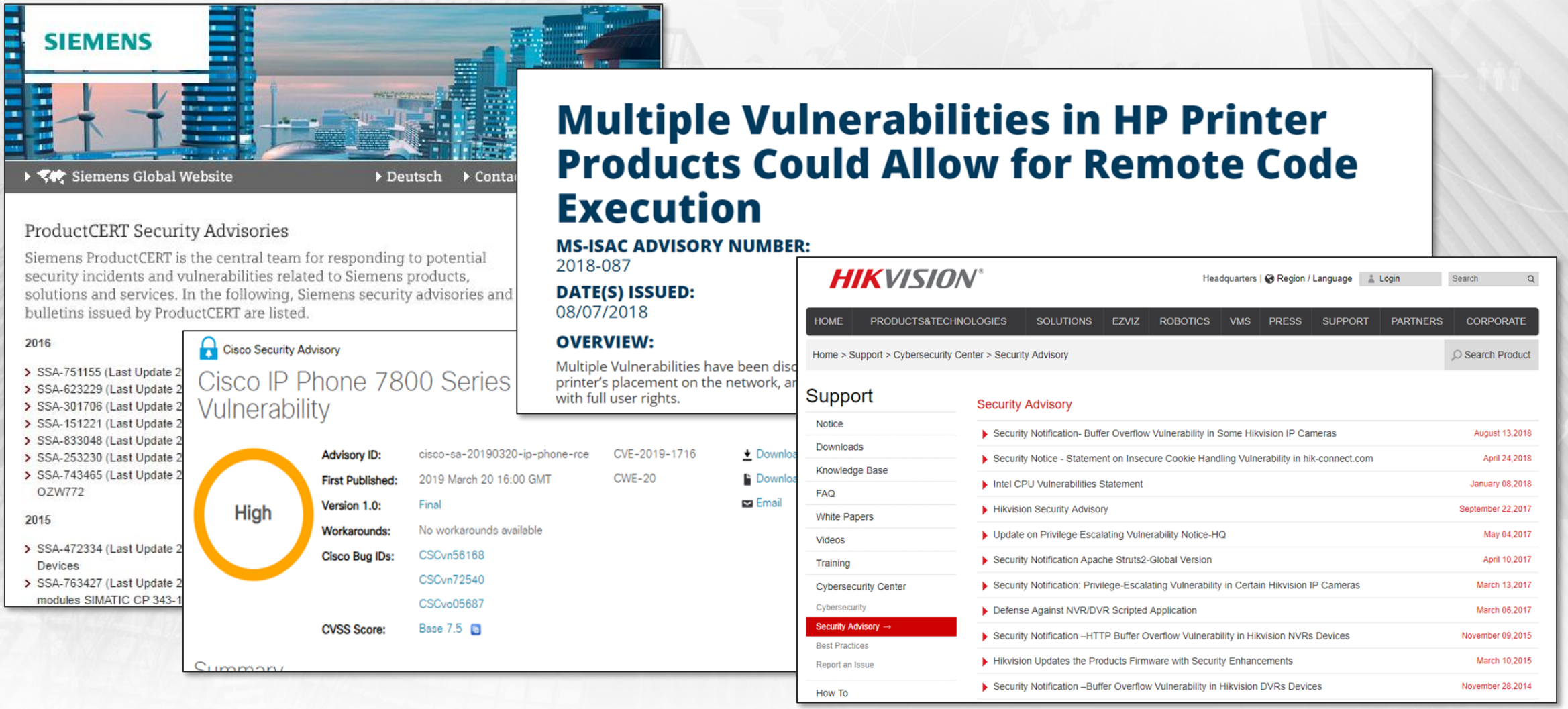
©2021 Check Point Software Technologies Ltd.

Transforme Perfeitamente o Mapa de Inteligência de IoT em uma Política de Segurança de IoT



©2021 Check Point Software Technologies Ltd.

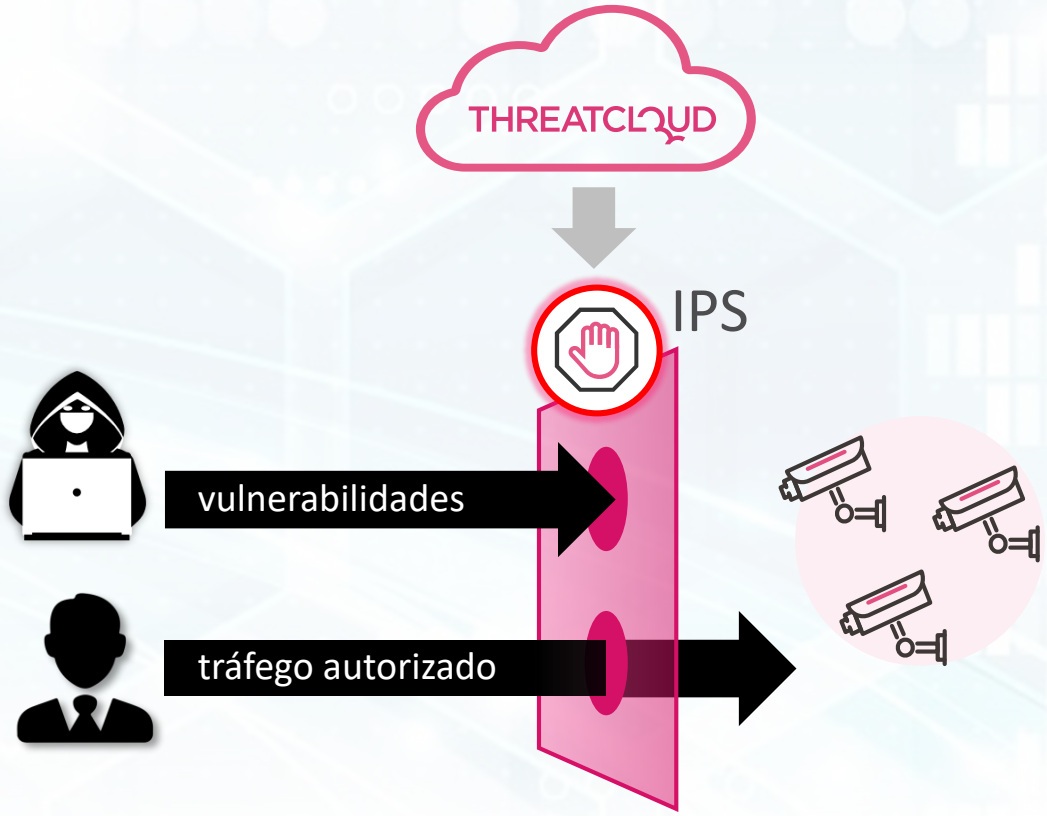
Você Pode Corrigir Seus Dispositivos IoT?



©2021 Check Point Software Technologies Ltd.

Protege Dispositivos de Explorações Conhecidas com Patches Virtuais

- 300+ assinaturas para ICS
- 10,000+ proteções para TI
- Proteções para 50+ fabricantes
- Atualizações contínuas da ThreatCloud



©2021 Check Point Software Technologies Ltd.

Check Point
SOFTWARE TECHNOLOGIES LTD

OBRIGADO

Ricardo Bacelar | Security Engineer

rbacelar@checkpoint.com