INDUSTRIAL CYBERSECURITY: INNOVATION IN CYBERATTACK VERSUS INNOVATION IN PROTECTION

XX Congreso Internacional de Ciberseguridad Industrial en Latinoamérica 2023 – Lima – 20.06.2023

INTRODUCTION

- President, CEO, Ampere Industrial Security, Inc.
- Former utility staff (telecommunications, water & electric)
- Drafter of NERC CIP standards and formal interpretations
- NERC CIP Supply Chain Working Group contributor
- First NERC CIP auditor/regulator
- Former Manager, CIP Audits and Investigations – WECC Region (NERC)
- Former Principal Investigator US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, Former Director, Former Instructor and President Emeritus
- SANS ISC456 Instructor: Essentials for NERC Critical Infrastructure Protection
- US Coordinator, Centro de Ciberseguridad Industrial (CCI)
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- National Telecommunications and Information Administration (NTIA) and Idaho National Lab (INL) Software Bill of Materials (SBOM) Energy POC Stakeholders
- DOE Solar Energy Technology Office (SETO) and National Renewable Energy Lab (NREL) Industry Advisory Board (IAB) for the Securing Solar for the Grid (S2G)
- Advisor to multiple industrial security hardware and software vendors
- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP

OPERATIONAL TECHNOLOGY TODAY

O.T. CHANGES OVER TIME

ATTACKERS OVER TIME

ATTACKER OBJECTIVES

- Loss
  - Loss of view
  - Loss of control
- Denial
  - Denial of view
  - Denial of control
  - Denial of safety
- Manipulation
  - Manipulation of view
  - Manipulation of control
  - Manipulation of sensors and instruments
  - Manipulation of safety

We have well-practiced plans for loss of view or control at a site level or for short periods

Plans are not comprehensive (ready) for when systems are available but do not perform as designed/expected

Few plans are ready for events when systems are available, but someone else is controlling them (possibly maliciously

ATTACKER TACTICS VS. DEFENSE

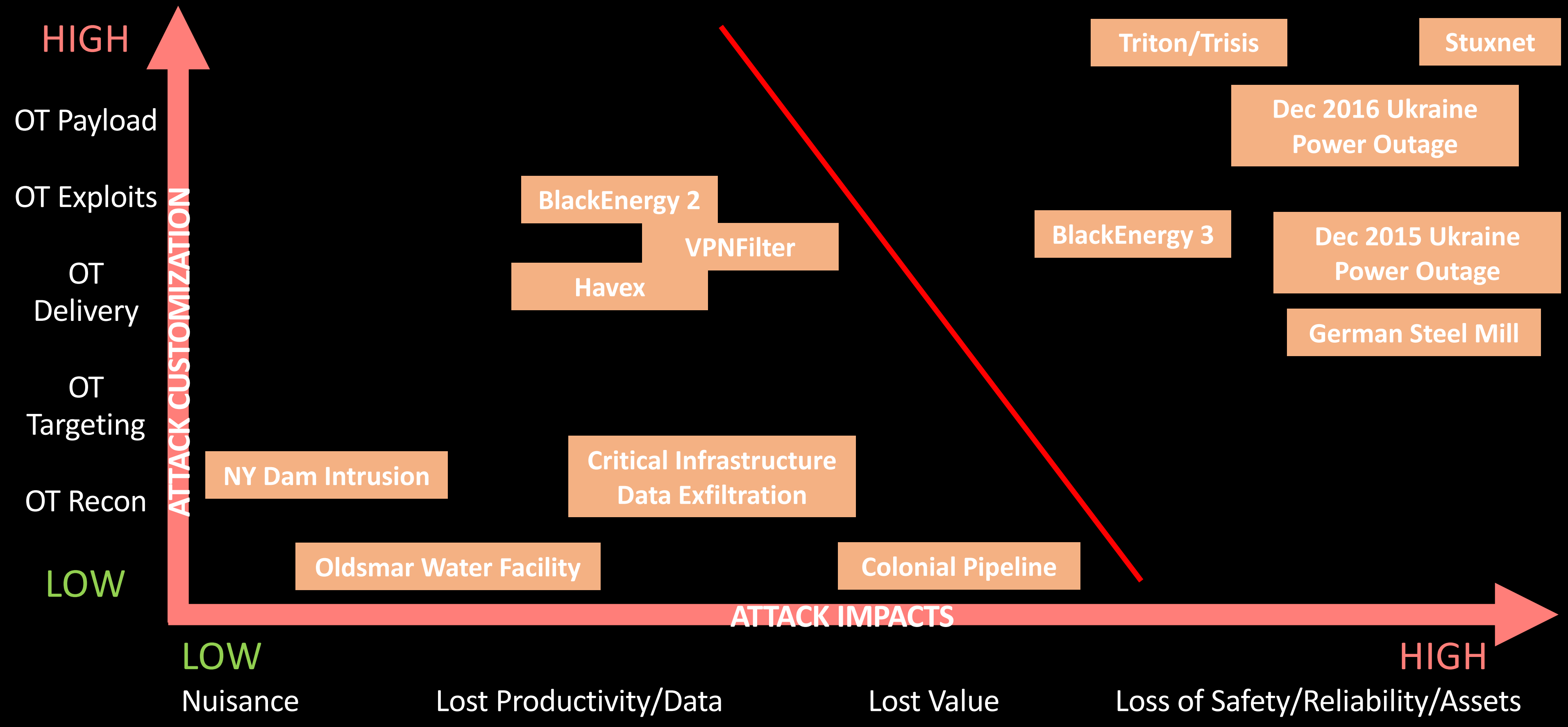
- ICS Opportunistic
  - Conficker, Petya/NotPetya, BlackEnergy 3
  - 2008, 2017, 2015
- ICS Focus
  - Dragonfly 2
  - 2016
- ICS Specific Access
  - BlackEnergy 2, Havex, Dragonfly 1
  - 2011, 2011, 2011, 2022-23

Governance, Standards, Regulation, Architecture, Cyber Hygiene
Passive Defense

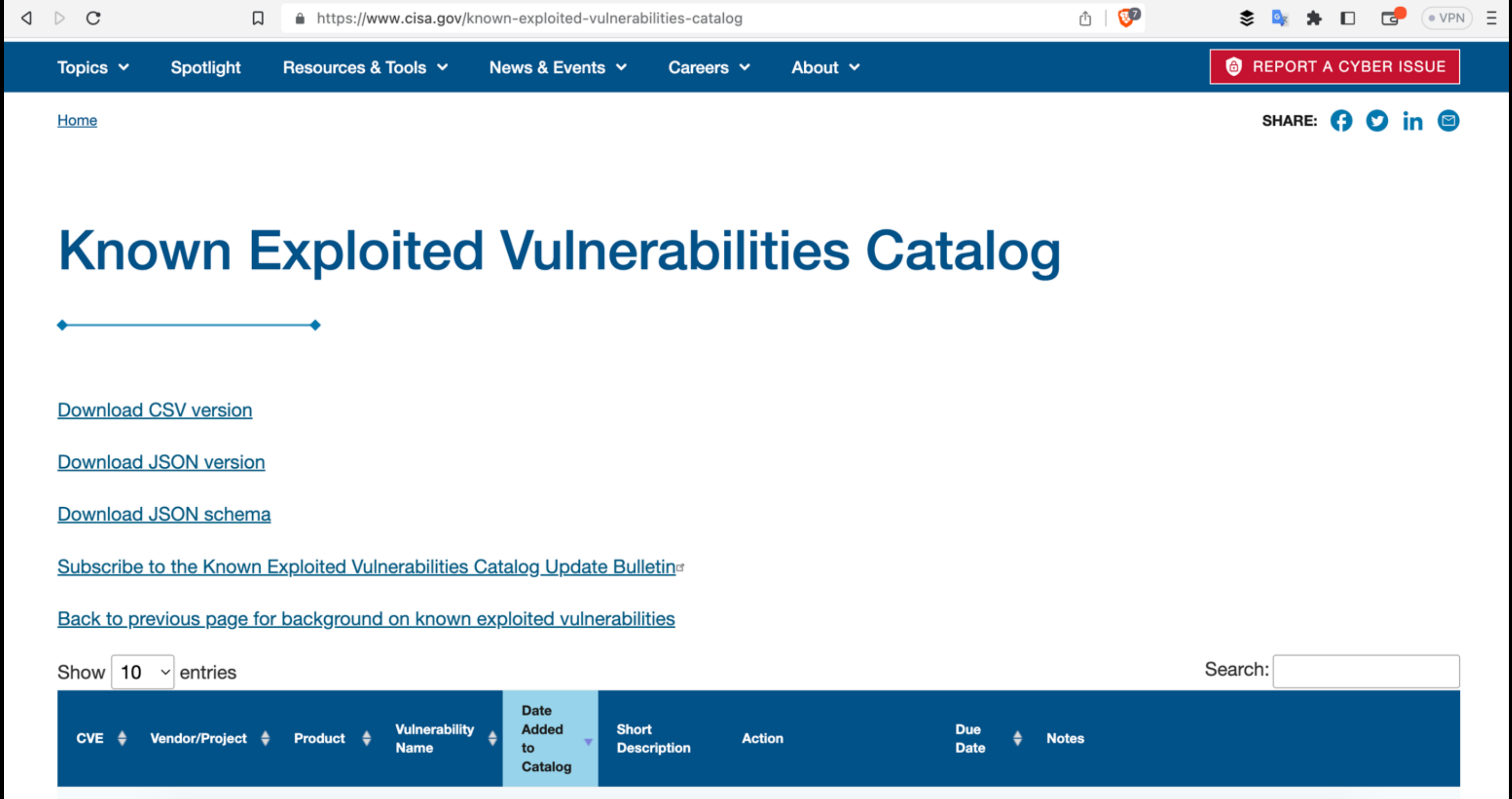
- ICS Specific Effect
  - Stuxnet, CrashOverride, Triton/Trisis
  - 2009, 2016, 2017, 2022-23

Operations, Resilience, Cyber Engineering,
Active Defense

OT INCIDENTS AND CAMPAIGNS



OT ATTACK INNOVATION



Known Exploited Vulnerabilities Catalog

Download CSV version

Download JSON version

Download JSON schema

Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin

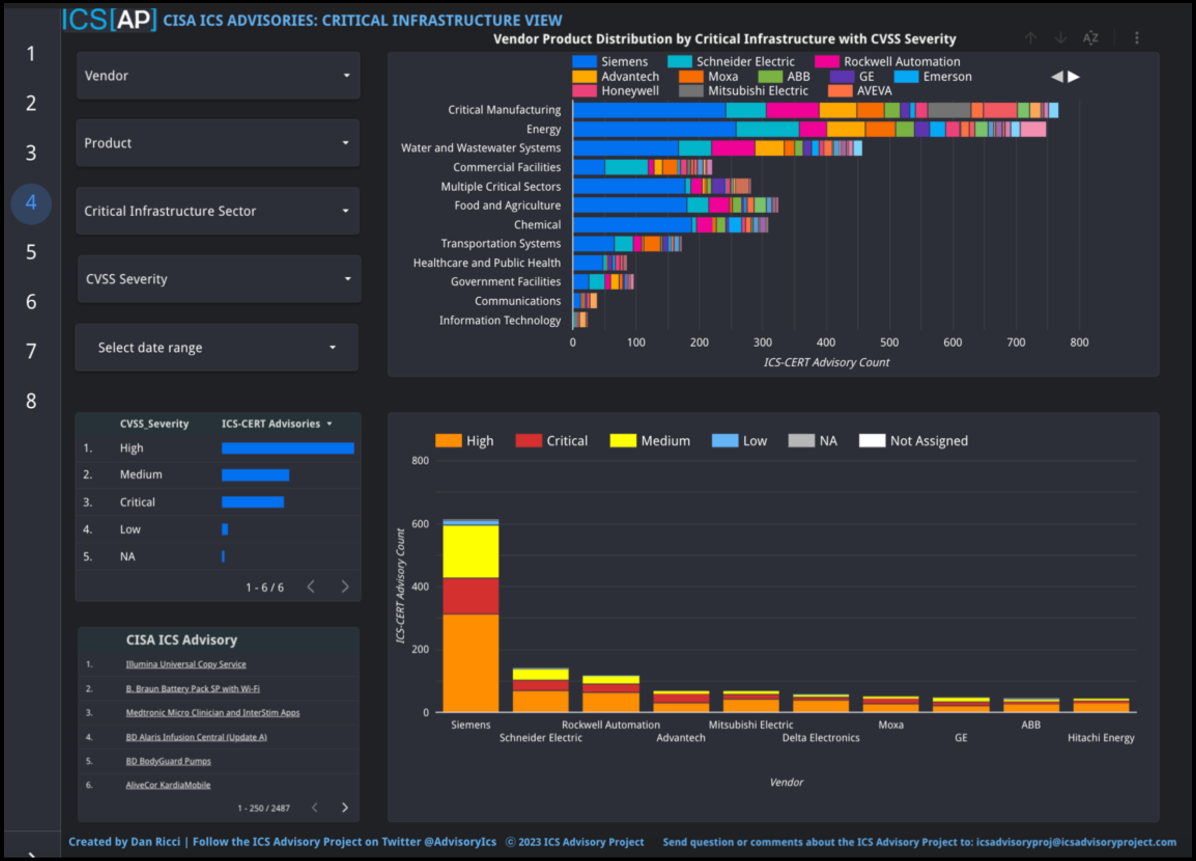
Back to previous page for background on known exploited vulnerabilities

Show 10 entries

Search:

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes

MORE VISIBILITY



	CVSS_Severity	ICS-CERT Advisories ▾
1.	High	
2.	Medium	
3.	Critical	
4.	Low	
5.	NA	

1 - 6 / 6

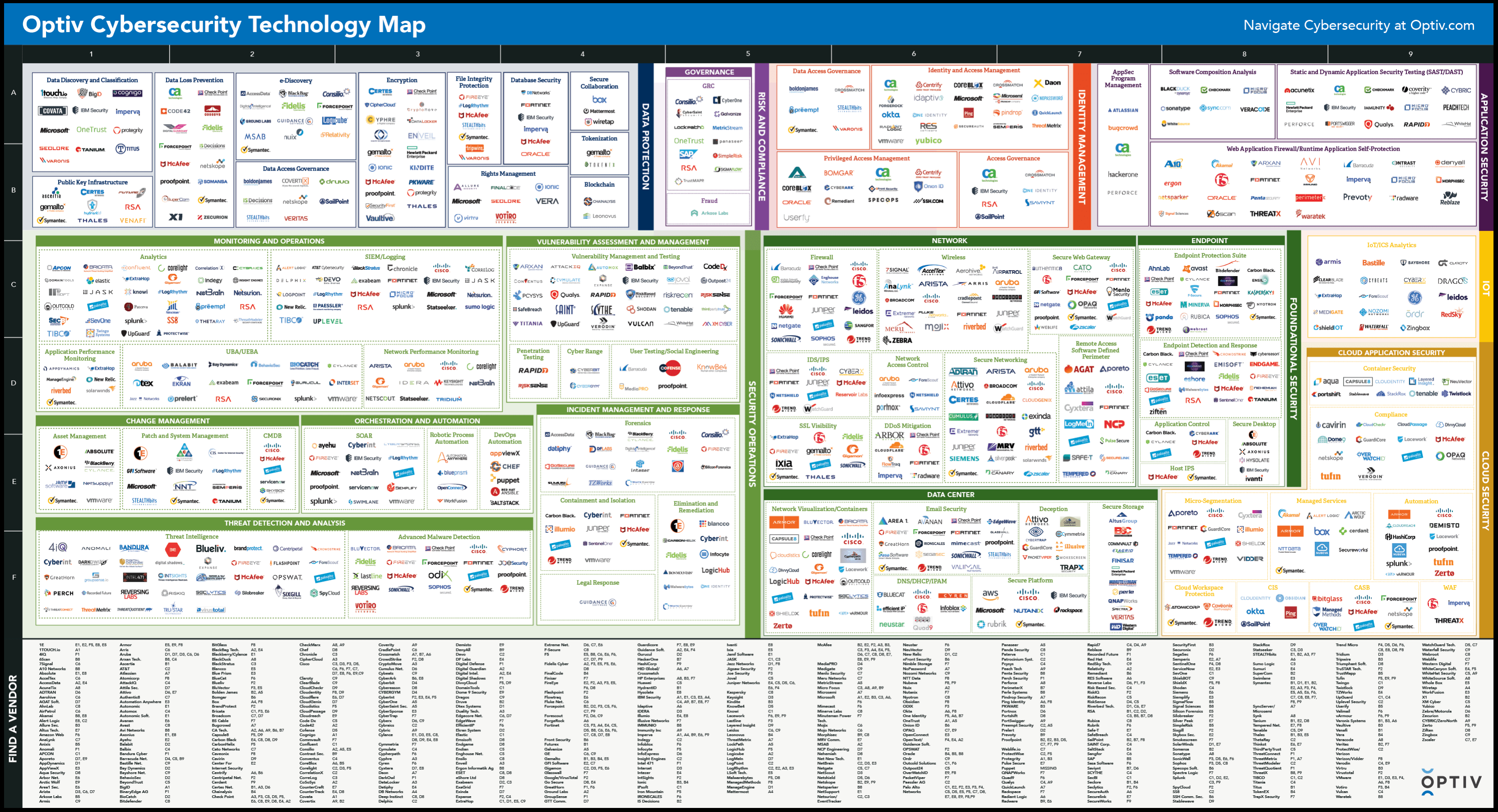
CISA ICS Advisory

1. Illumina Universal Copy Service
2. B. Braun Battery Pack SP with Wi-Fi
3. Medtronic Micro Clinician and InterStim Apps
4. BD Alaris Infusion Central (Update A)
5. BD BodyGuard Pumps
6. AliveCor KardiaMobile

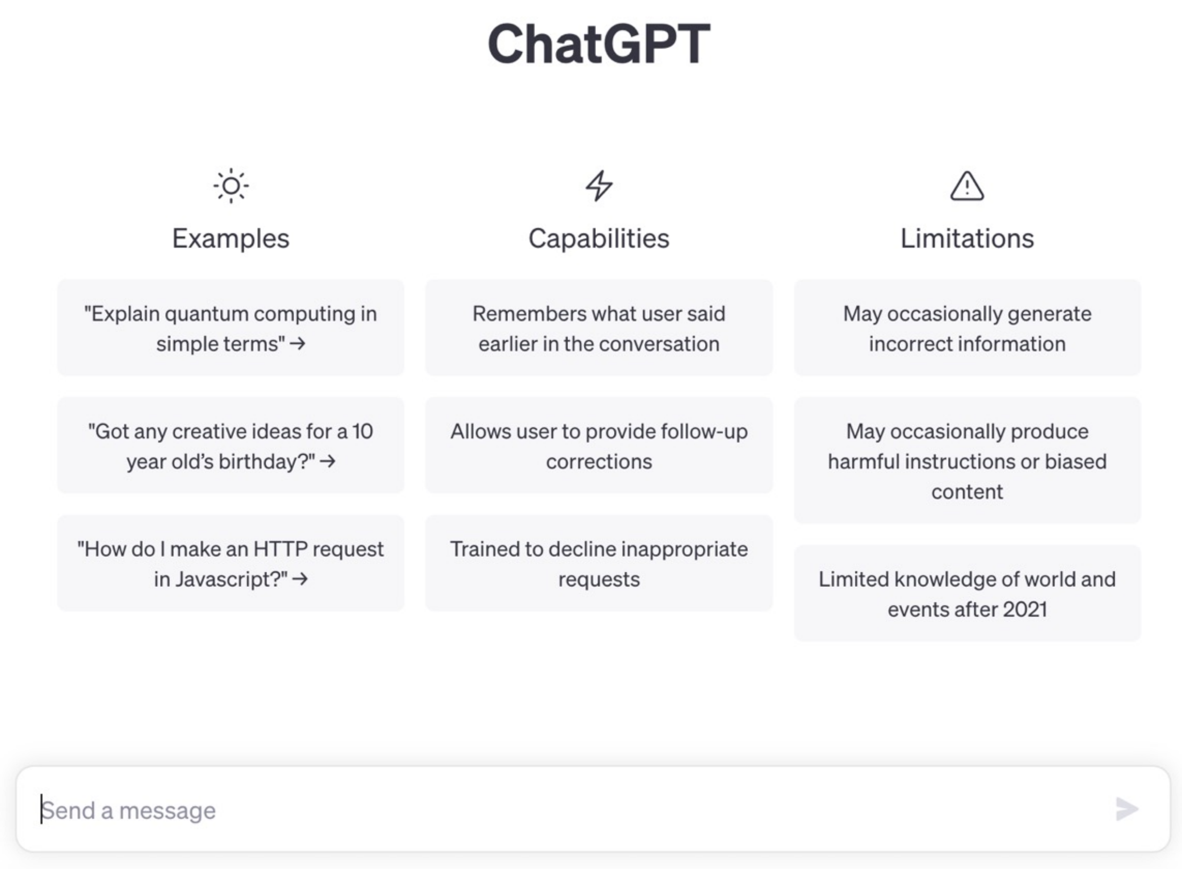
1 - 250 / 2487

Created by Dan Ricci | Follow the ICS Advisory Project on Twitter @AdvisoryIcs © 2023 ICS Advisory Project Send question or comments about the ICS Advisory Project to: icsadvisoryproj@icsadvisoryproject.com

MORE BLINKING LIGHTS


Optiv Cybersecurity Technology Map
Navigate Cybersecurity at Optiv.com
DATA PROTECTION
Data Discovery and Classification
Data Loss Prevention
e-Discovery
Encryption
File Integrity Protection
Database Security
Secure Collaboration
Tokenization
Public Key Infrastructure
Data Access Governance
Rights Management
Blockchain
RISK AND COMPLIANCE
GOVERNANCE
GRC
Fraud
IDENTITY MANAGEMENT
Data Access Governance
Identity and Access Management
Privileged Access Management
Access Governance
APPLICATION SECURITY
AppSec Program Management
Software Composition Analysis
Static and Dynamic Application Security Testing (SAST/DAST)
Web Application Firewall/Runtime Application Self-Protection
SECURITY OPERATIONS
MONITORING AND OPERATIONS
Analytics
SIEM/Logging
Application Performance Monitoring
UBA/UEBA
Network Performance Monitoring
VULNERABILITY ASSESSMENT AND MANAGEMENT
Vulnerability Management and Testing
Penetration Testing
Cyber Range
User Testing/Social Engineering
CHANGE MANAGEMENT
Asset Management
Patch and System Management
CMDB
ORCHESTRATION AND AUTOMATION
SOAR
Robotic Process Automation
DevOps Automation
INCIDENT MANAGEMENT AND RESPONSE
Forensics
Containment and Isolation
Elimination and Remediation
Legal Response
THREAT DETECTION AND ANALYSIS
Threat Intelligence
Advanced Malware Detection
FOUNDATIONAL SECURITY
NETWORK
Firewall
Wireless
Secure Web Gateway
IDS/IPS
Network Access Control
Secure Networking
Remote Access Software Defined Perimeter
SSL Visibility
DDoS Mitigation
DATA CENTER
Network Visualization/Containers
Email Security
Deception
Secure Storage
DNS/DHCP/IPAM
Secure Platform
ENDPOINT
Endpoint Protection Suite
Endpoint Detection and Response
Application Control
Secure Desktop
Host IPS
Micro-Segmentation
Managed Services
Automation
Cloud Workspace Protection
CIS
CASB
WAF
IOT
IoT/ICS Analytics
CLOUD SECURITY
CLOUD APPLICATION SECURITY
Container Security
Compliance
FIND A VENDOR
OPTIV

MORE ARTIFICIAL INTELLIGENCE



ChatGPT

Examples

"Explain quantum computing in simple terms" →

"Got any creative ideas for a 10 year old's birthday?" →

"How do I make an HTTP request in Javascript?" →

Capabilities

Remembers what user said earlier in the conversation

Allows user to provide follow-up corrections

Trained to decline inappropriate requests

Limitations

May occasionally generate incorrect information

May occasionally produce harmful instructions or biased content

Limited knowledge of world and events after 2021

INNOVATION OR DISRUPTION?

MANAGING ALL RISKS ALL THE TIME

- Hackers are faster than laws, regulation, standards, norms
- You can not possibly know every zero day in advance
- You can not possibly know every new adversary tactic in advance
- If you bought/implemented every security tool available, would you be secure?
- If you were compliant to every regulation and standard, would you be secure?
- How much better would your security be if you had enough well-trained security professionals?

ADAPTABLE PROTECTION

- Culture eats security controls for breakfast
- IDS and “APS”
- Creativity - use existing tools in new and creative ways
- You are protecting against a skilled human (or many) with powerful tools; respond with the same
- OT technology span has both a time spectrum and innovation spectrum; train for both

THE BEST SECURITY YOU CAN BUY

CONTACT ME

@PATRICKCMILLER

LINKEDIN.COM/IN/MILLERPATRICKC

PMILLER@AMPERESEC.COM

WWW.AMPERESEC.COM

+15032721414

All images sourced through Creative Commons and Pixabay