Asset Intelligence, Dirty Secrets, Dangerous Lies & Hacking Demos

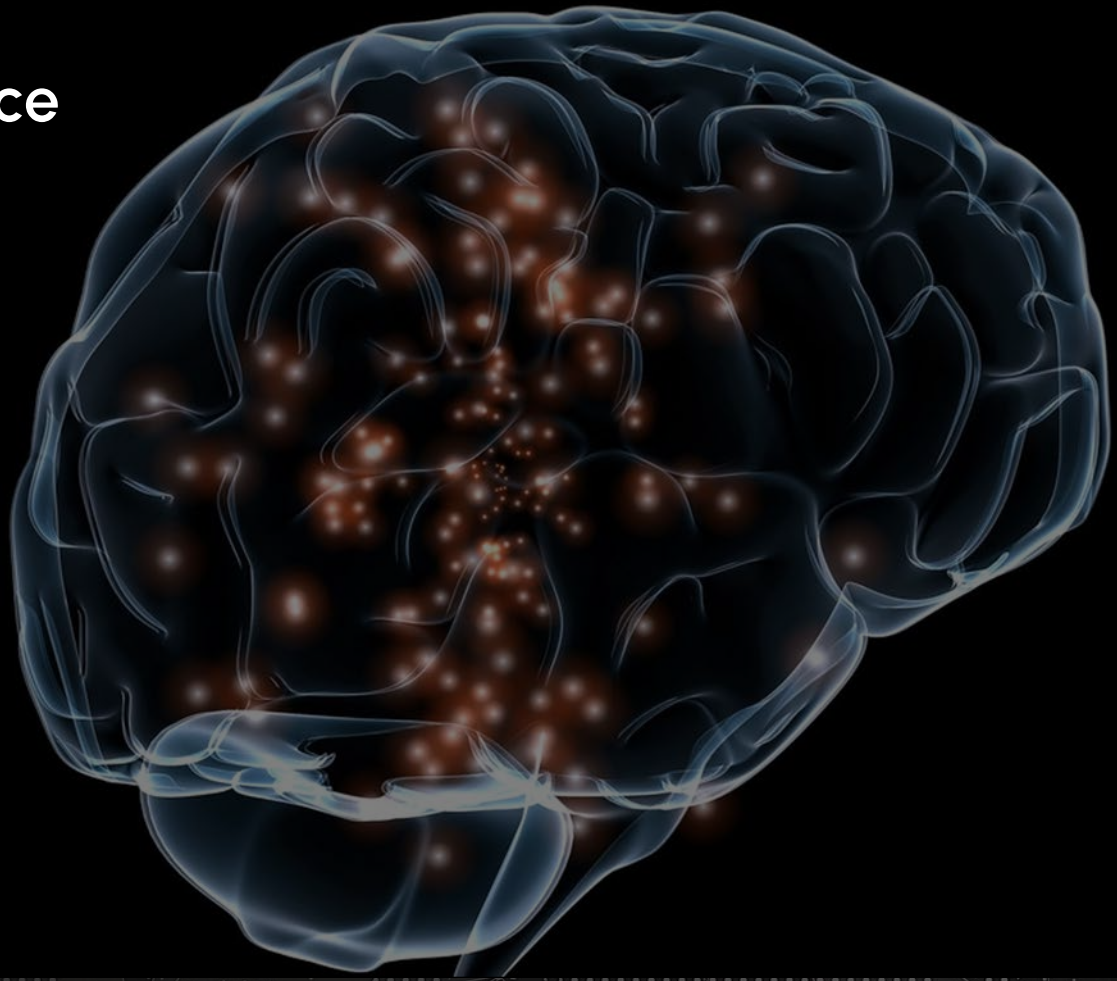
Brian Contos

Chief Strategy Officer, Sevco

brian@sevco.io

https://www.linkedin.com/in/briancontos/

Asset Intelligence



Four Dimensions of Asset Intelligence

LENGTH	BREADTH	HEIGHT	TIME
Asset Types	Asset Locations	Asset Details	Real-time & Historical

Dirty Secrets

xIoT

- Purpose-built firmware/HW
- Network-connected
- Can't run endpoint security


Printers


Phones


Cameras


Robotics

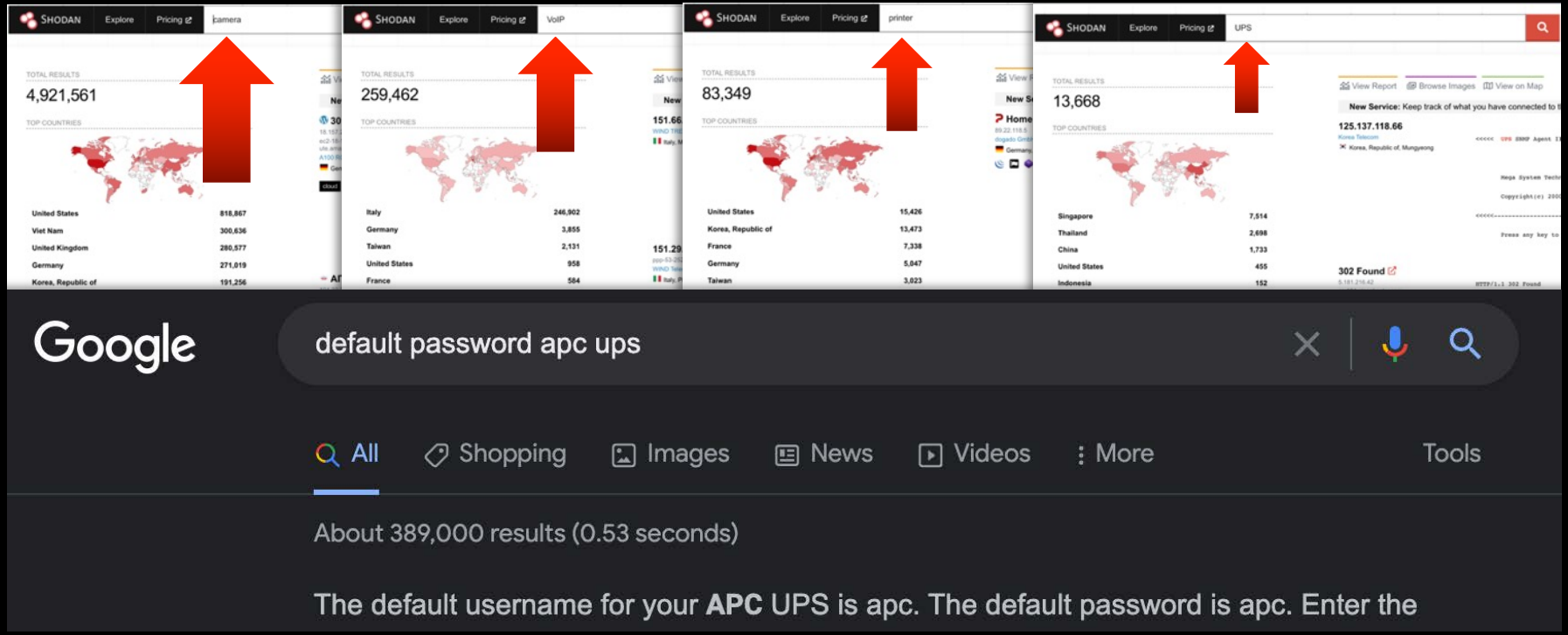

UPS systems


Wireless routers

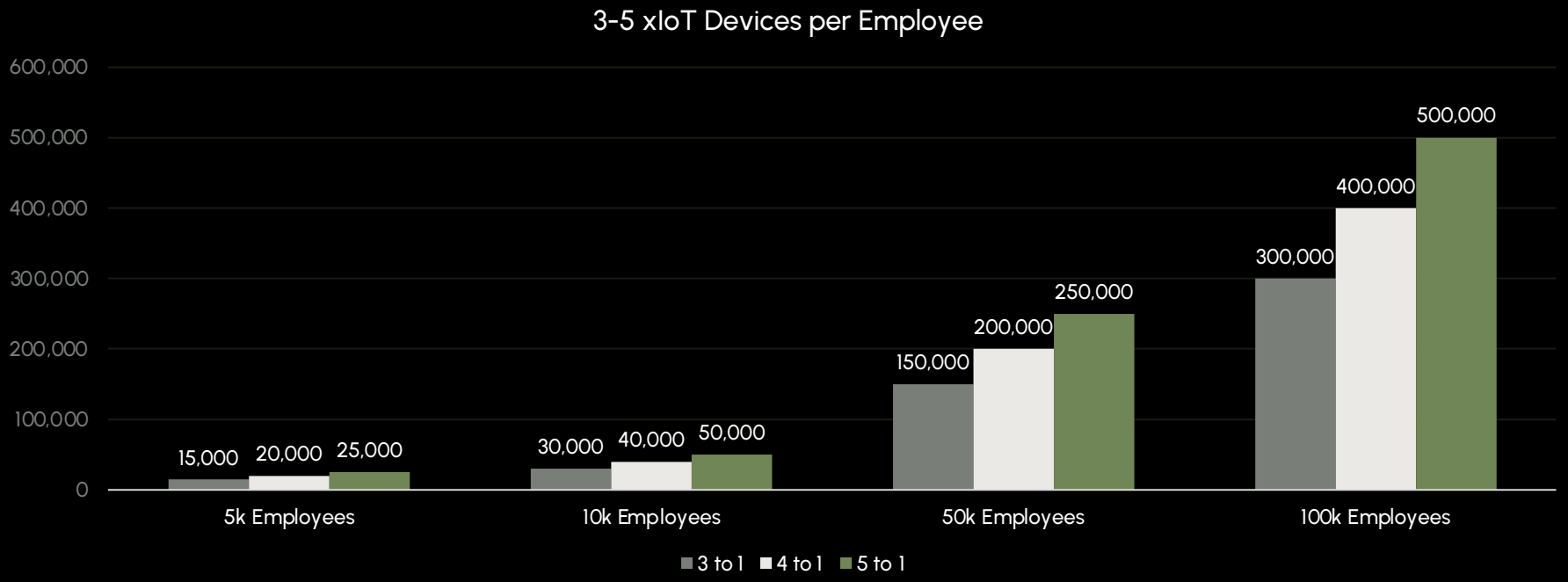

Smart cities


Door controllers

Internet-accessible xIoT

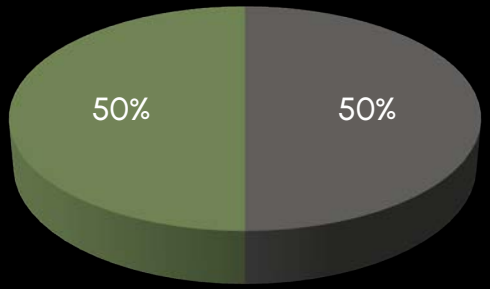


Research Stats



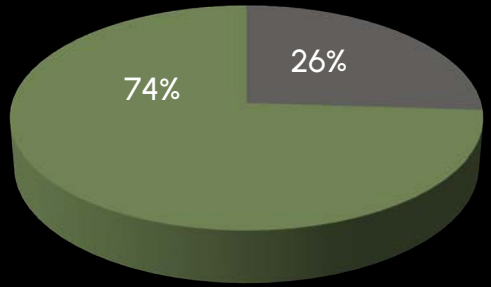
Research Stats

Default Passwords



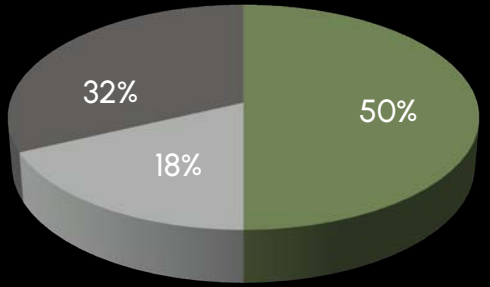
- Default Passwords
- Passwords Changed at Least Once (Usually Only Once)

EoL Firmware



- EoL
- Supported, but 6-year average age

CVSS Scores



- CVSS = 8
- CVSS = 9 or 10
- CVSS <= 7

Dangerous Lies

Common xIoT Attack Types

Legacy attacks

Attacks on xIoT assets for the sake of the xIoT assets & opportunistic attacks like botnets monetized by cybercriminals (RSOCKS)

RSOCKS

Common xIoT Attack Types

Legacy attacks

Physical attacks

Spying, attacks on power, unlocking doors, & devices that control physics - often associated with nation-states (FRONTON)

Fronton

- Fronton, designed by contractors for Russian FSB
- Targets xIoT devices for C&C
- Digital Revolution hacking group discovered & released it
- Now available on torrents & the usual places

Common xIoT Attack Types

Legacy attacks

Physical attacks

OEM attacks

Malicious xIoT assets out of the box
(Huawei, ZTE, Hikvision, Dahua & Hytera)

Illegal xIoT Devices

- China-based firms, including Huawei, ZTE, Hikvision, Dahua & Hytera
- NOW illegal to import or sell in the USA as of November 2022

Common xIoT Attack Types

Legacy attacks

Physical attacks

OEM attacks

Pivot attacks

Gain access through an IT asset, hide on multiple xIoT assets, attack IT assets, & exfiltrate data through the xIoT assets (QUIETEXIT)

QUIETEXIT

Compromise & C2 Tunnel

Dropbear SSH client-server software

API calls on-prem & in the cloud

Exchange

Office 365

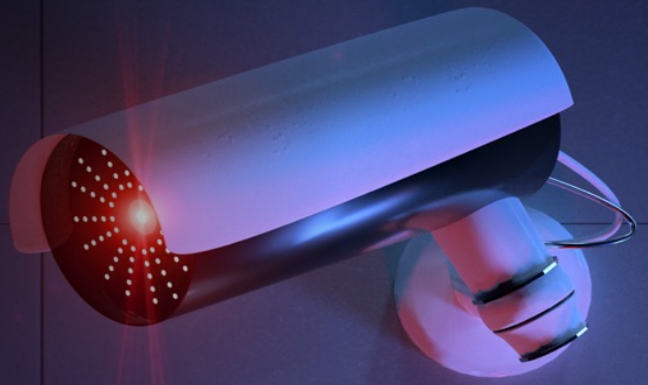
Data retrieval

Data exfiltration

Hacking Demonstrations

HACKING

Security Cameras

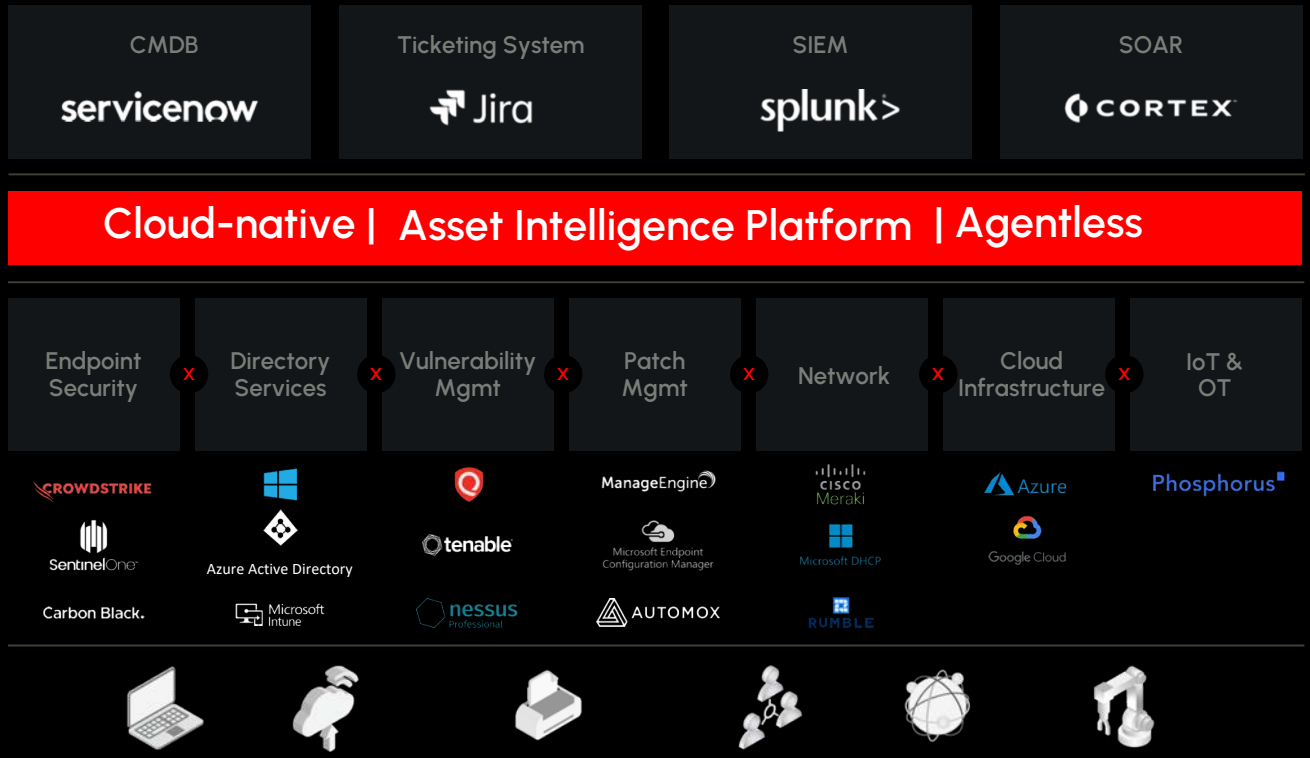


HACKING

Industrial Robots

Remediation

Visibility with an Asset Intelligence Platform



Try It. A Free POC Only Takes 60 Minutes!

Next Week

POC

- (3) Sources
- (1) Point of Contact
- (1) Hour

Next Month

Configure

- Devices
- Identities
- Applications & VA

Next Quarter

Integrate

- CMDB
- Ticketing
- SOAR, SIEM...

https://www.sevcosecurity.com/book-a-demo/

Asset Intelligence, Dirty Secrets, Dangerous Lies & Hacking Demos

Brian Contos

Chief Strategy Officer, Sevco

brian@sevco.io

https://www.linkedin.com/in/briancontos/