

A Random walk through (a few) 1,000,000 Things

A Story of Millions Interrogated Devices

Chris Rouland

Founder and CEO, Phosphorus Cybersecurity





Printers



Cameras



UPS



PDU



Phones



Robotics

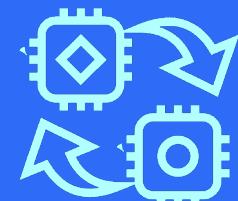


Wireless router

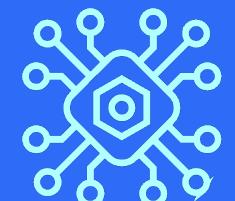


Door controller

What is xIoT?



Purpose-built
firmware/HW



Network-connected



Can't run
Endpoint security

Cloud Security



**10 Million servers
world-wide**





Endpoint Security

.57 desktops per person

World-wide desktops or laptops per person.

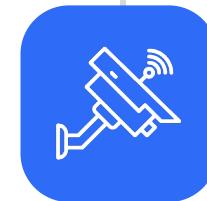


5 Billion desktops WW

Total computers with keyboards world-wide.



xIoT Security



**50 Billion xIoT
devices world-wide**

Spanning IoT, OT, and
Network Devices.

State of xIoT Security

The need to Find, Fix, and Monitor
xIoT devices automatically.

78%

of Enterprise IoT
devices have a CVE of
8+

26%

of Enterprise IoT devices
are end-of-life by their
manufacturer

7
years

Average firmware age
of an embedded device



50%

Of enterprise IoT/OT
devices use default
credentials

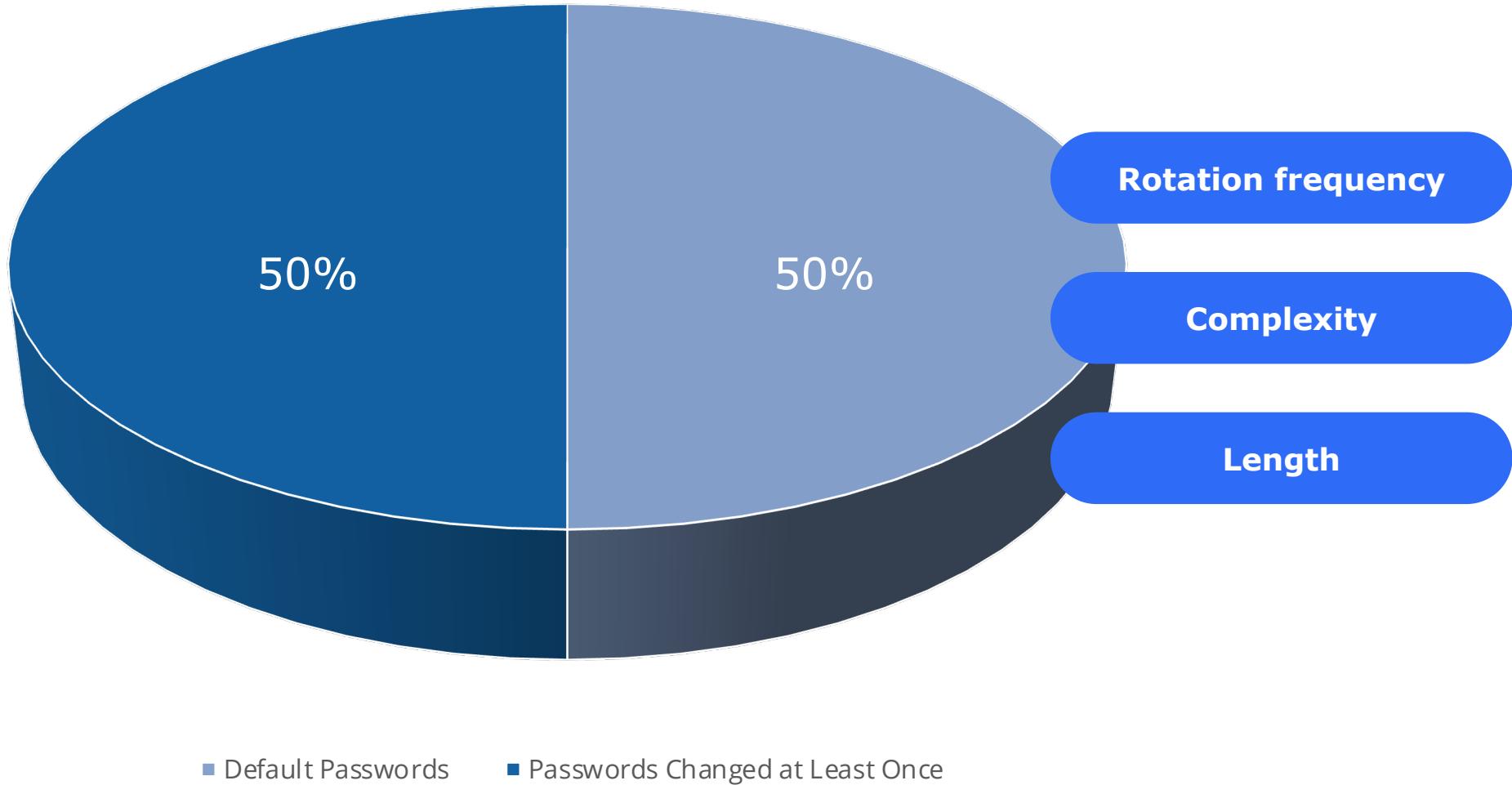


3-5

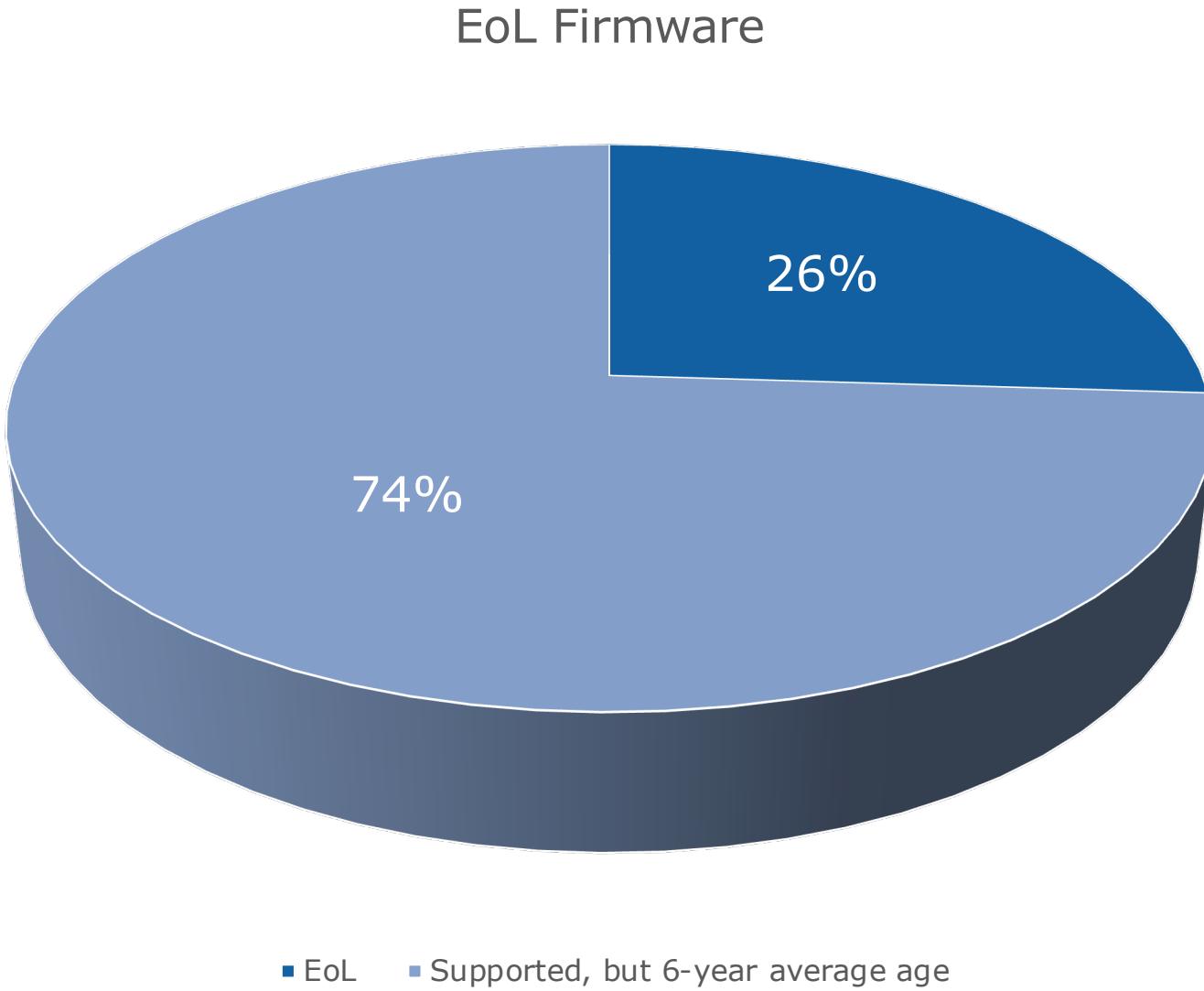
IoT devices per
enterprise employee

Phosphorus Research Stats

Default Passwords



Phosphorus Research Stats



SHODAN Explore Pricing camera **camera**

TOTAL RESULTS
4,921,561

TOP COUNTRIES

COUNTRY	RESULTS
United States	818,867
Viet Nam	300,636
United Kingdom	280,577
Germany	271,019
Korea, Republic of	191,256

View Report **Browse Images** **View on Map**

New Service: Keep track of what you have connected to the Internet.

301 Moved Permanently [View Report](#)

18.157.207.232
ec2-18-157-207-232.eu-central-1.compute.amazonaws.com
A100 ROW GmbH
Germany, Frankfurt am Main

SSL Certificate
Issued By:
- Common Name: R3
- Organization: Let's Encrypt
Issued To:
- Common Name: www.welovecycling.com
Supported SSL Versions: TLSv1.2, TLSv1.3

AGRANA | Россия | AGRANA [View Report](#)

104.22.22.189

SSL Certificate

SHODAN Explore Pricing **VoIP** **VoIP**

TOTAL RESULTS
259,462

TOP COUNTRIES

COUNTRY	RESULTS
Italy	246,902
Germany	3,855
Taiwan	2,131
United States	958
France	584

View Report **View on Map**

New Service: Keep track of what you have connected to the Internet.

151.66.16.89 [View Report](#)

WIND TRE S.P.A.
Italy, Monza

```
SIP/2.0 404 Not Found
From: <sip:nn@nm>;tag=rc
To: <sip:nn@nm2>;tag=rc
Call-ID: 50000
CSeq: 42 OPTIONS
User-Agent: DLINK VoIP E
Supported: replaces,time
Via: SIP/2.0/UDP nm;rece...
Content-L...
```

151.29.252.53 [View Report](#)

ppp-53-252-29-151.wind.it
WIND Telecomunicazioni S.p.A.
Italy, Pisa

```
SIP/2.0 404 Not Found
From: <sip:nn@nm>;tag=rc
To: <sip:nn@nm2>;tag=bc
Call-ID: 50000
Content-L...
```

SHODAN Explore Pricing **printer** **printer**

TOTAL RESULTS
83,349

TOP COUNTRIES

COUNTRY	RESULTS
United States	15,426
Korea, Republic of	13,473
France	7,338
Germany	5,047
Taiwan	3,023

View Report **Browse Images** **View on Map**

New Service: Keep track of what you have connected to the Internet.

P Home page [View Report](#)

89.22.118.5
dogado GmbH
Germany, Leipzig

SSL Certificate
Issued By:
- Common Name: R3
- Organization: Let's Encrypt
Issued To:
- Common Name: printer-v6demo-ek414.your-prin...

Diffie-Hellman Fingerprint: RFC3526/Oakley Group 14

SHODAN Explore Pricing **UPS** **UPS**

TOTAL RESULTS
13,668

TOP COUNTRIES

COUNTRY	RESULTS
Singapore	7,514
Thailand	2,698
China	1,733
United States	455
Indonesia	152

View Report **Browse Images** **View on Map**

New Service: Keep track of what you have connected to the Internet.

125.137.118.66 [View Report](#)

Korea Telecom
Korea, Republic of, Mungyeong

```
<<<< UPS SNMP Agent II
Copyright(c) 200...
```

Mega System Tech...

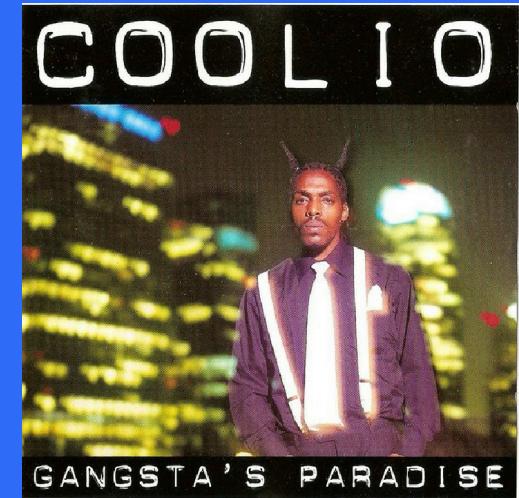
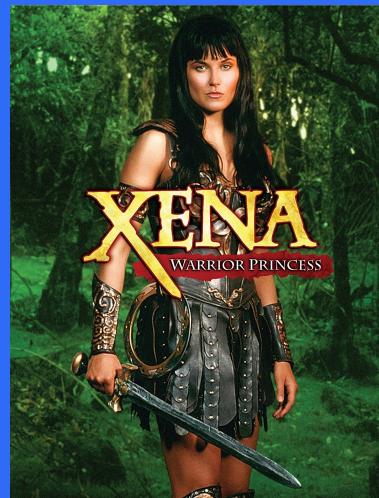
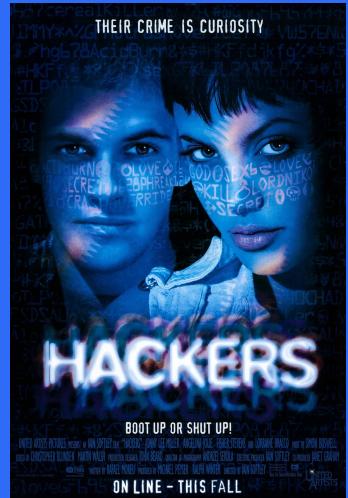
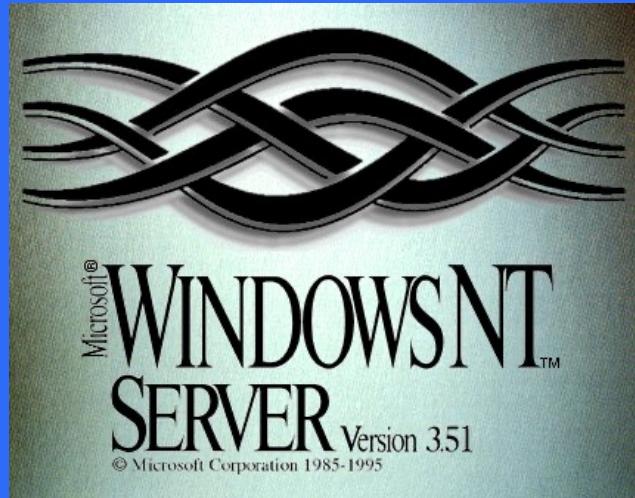
Press any key to...

302 Found [View Report](#)

HTTP/1.1 302 Found
5.181.216.42
srv104.niaahostler.com

xIoT Security Today = IT Security In 1995

Phosphorus[®]



Phosphorus[■]

Banned Chinese xIoT Devices



U.S. House of Representatives passed H.R.5515 - prohibits federal agencies from using xIoT devices from certain China-based firms including Huawei, ZTE, Hikvision, Dahua & Hytera.

The screenshot displays the user interface of the Russian xIoT Hacking Tool. It includes:

- A document header (Приложение № 1 к Договору № ИДГ-12-0-1) with sections for УЧЕБНО-ЗАДАНИЕ (Contractor: ООО "ФСБ", Date: 2017 год) and СОБСТАВЛЯЮ (Contractor: ООО "ЦДР", Date: 2017 год).
- A network diagram titled "Структура связи изолята" (Network Structure of the Isolated System) showing a central "Сеть изолята" (Isolated Network) connected to "Локальная сеть" (Local Network) via a "Сетевое оборудование" (Networking Equipment) node.
- A table titled "Список устройств" (List of Devices) showing a table of IoT devices with columns: IP, Название устройства (Device Name), Операционная система (Operating System), WiFi, and Управление (Management). Most devices are listed as "general purpose" with "Linux" OS and "No" WiFi.
- A configuration screen titled "Настройка" (Configuration) with fields for "Программа" (Program), "Порт" (Port), "IP-адрес" (IP Address), "Пароль" (Password), and "Ключ" (Key).
- A file structure view showing files: .codelite, project-fronton, .tern-project, add_user.sh, scanner, scanner-develop, scanner-stuff, stand, stand-keys, thc-hydra, uploadable, build.bash, create_tunnel.sh, hydra-deps.bash, and install.bash.
- Code snippets from the scanner module, including logic for port scanning, connection handling, and exploit delivery.



- › “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

Russian State Hackers Target xIoT

Internet-accessible xIoT



Two default passwords
One unpatched vulnerability

Internal Enterprise Environment



Sniff traffic with tcpdump Scan
& expand Enumerate
administrative groups



Strontium APT28 - aka Fancy
Bear aka SoFancy - Linked to
Russian Intelligence GRU



Microsoft
Threat
Intelligence

Discovered by the
Microsoft Threat
Intelligence Center

Russian State Hackers Target Routers

VPNFilter Malware



Compromised through
extraneous services like remote
management that were running
with default passwords



Traffic capture



Firmware wiping –
destroying router



Post reboot malware
persistence

500,000

infected business & home routers: Linksys, MikroTik,
Netgear, QNAP, & TP-Link

Discovered by Cisco

Russian State Hackers Target Net. Devices

A separate attack

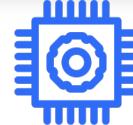
- Remote login with default username & password
- Initial boot credentials
- Undocumented user account with privilege level 15
- Full access to all commands & changes



Russian Dragonfly Cyber Unit targets millions of Cisco network devices with port TCP 4786 (Smart Install) open



Exfiltrate configurations over TFTP, execute commands, replace the IOS images, and set up accounts



Patch the firmware, turn off extraneous services & manage credentials correctly...& eat your vegetables

Mirai Botnet



Actual brand not pictured

Default & eight common passwords



PayPal, Twitter, Reddit, Sony, Netflix, GitHub

Russian xIoT Botnet Takedown

Phosphorus⁺

RSOCKS Botnet



Industrial Control Systems (OT), Network Gear, Enterprise xIoT...



Millions of compromised devices operated by Russian cybercriminals & leased ~\$30/day



Law enforcement from the US, UK, Germany & Netherlands participated in the takedown

APTs Achieving Persistence with xIoT: QuietExit

Phosphorus[®]



UNC3524 was published by Mandiant on May 2nd, 2022 & labeled "QuietExit"



Associated with Russian Espionage Threat Actors: APT 28 Fancy Bear & APT 29 Cozy Bear



It exfiltrates executive, corporate development, M&A, and security staff data – 18 month+ dwell time

General PLC Exploits

Phosphorus⁺

- Real Time OS (RTOS)
- VxWorks & OS-9
- C++ & Python
- (1) Runtime on embedded device
- (2) Editor – laptop for writing programs
- (3) SCADA GUI – monitor



- Critical
- Hyper-connected
- Modern & legacy protocols
- Poor user documentation
- Proprietary encryption
- Depreciation over decades
- Unmaintained
- Mostly no authentication
- No integrity (tamper aware)
- No confidentiality (plain text)

Interruption

blast messages, it's simple so you can easily DoS a PLC (flood w/ 1,000 msg./sec.)

Interception

read the message, there is no encryption across the network

Modification

change the message, like a bump in the wire, modify the content and resend

Injection

make your own message (Modbus/TCP frame), all messages are welcome

KVM Switches

Phosphorus[®]



Running Ubuntu Linux v10 from
~October 2010 (current release is
v21.1 as of October 2021)



Totally unpatched with
hundreds of vulnerabilities

Lights Out Management Controls

Phosphorus[®]



Three common types of lights out
management controllers including
HP, Dell, & Supermicro



They are IoT devices running
their own OS and applications
(Linux or VxWorks)

Server Cabinets & Racks

Phosphorus[®]



UPS backup, cooling, cable
management & tamper sensors



Passwords are usually default;
old firmware with critical CVEs

Physical Access Controllers

Phosphorus[®]



During a POV we could lock and unlock 6,400 doors at a FS company



Nortek Security & Control systems had several CVSS scores of 9.8/10 & 10/10



Allowing remote, unauthenticated, and low-skill exploitation for full control

Printers

Phosphorus[®]



Black Hat 2019: critical level vulnerabilities were discovered in 10,000 printer brands/types/versions



Promiscuous & multi-vector access with everything on by default and default credentials



Some of the most targeted assets by state sponsored attackers

VoIP Phones & Video Conf. Systems

Phosphorus[®]



Some run Android OS and have undocumented SSH with default credentials



A beacon of hope: one customer had 31,000 phones and “only” 700 had critical CVEs

15 Stock Exchange Atomic Clocks

Phosphorus⁺



Knew about six of them
No CVEs

WHICH xIoT DEVICE TYPE IS THE #1 BIGGEST OFFENDER?

Security Cameras

Phosphorus[®]



The #1 worst offender; running Linux such as BusyBox; some ship with malware preloaded



Everyone has them; nobody knows who's responsible: IT, IT Sec., Facilities, Corp. Sec., Network Ops...

Beyond Enterprise xIoT

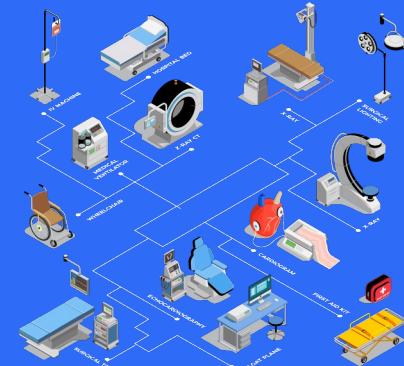
Phosphorus[®]



Internet of Battlefield Things (IoBT)



Industrial Internet of Things (IIoT)



Internet of Healthcare Things (IoHT)



Smart Ships



Smart Buildings & Cities



Network Gear

Phosphorus[■]

Summary

Organizations don't know what things they have.

So, they don't know what things to fix.

They don't have the ability to fix things at scale.

They aren't monitoring things to keep them fixed.

This is leaving **xIoT** and IT/cloud assets at risk.

It's resulting in data theft, destruction, spying, ransomware...

Thank you!

Chris Rouland

Founder and CEO, Phosphorus Cybersecurity

 chris@phosphorus.io

 <https://www.linkedin.com/chrisrouland/>