Definitive Guide™

to

Enterprise xIoT Security

How to protect offices, factories, cities, and the world by finding, fixing, and monitoring **x**IoT devices

Jon Friedman

FOREWORD BY:

Richard Stiennon

Compliments of:

Phosphorus

About Phosphorus

Phosphorus Cybersecurity® is the leading **x**IoT Breach Prevention platform for the eXtended Internet of Things. Designed to secure the rapidly growing and often unmonitored world of Things across the enterprise **x**IoT landscape, our Enterprise **x**IoT Security Management Platform delivers attack surface management across every industry vertical, providing active discovery and risk assessment, hardening and remediation, and detection and response. It brings enterprise **x**IoT security to every cyber-physical system in your enterprise environment. With unrivaled **x**IoT Intelligent Active Discovery and risk assessment, Phosphorus automates the remediation of the most significant IoT, OT, IoMT, and IIoT device vulnerabilities—including unknown and inaccurate asset inventory, out-of-date firmware, default credentials, risky configurations, and out-of- date certificates. Founded in 2017 by Chris Rouland, Rebecca Rouland, and Earle Ady, previously of Bastille, Endgame, and other successful Internet companies, Phosphorus is a trusted partner of Fortune 500 and Global 2000 companies and government agencies. Phosphorus is a privately held company headquartered in Nashville, TN.

Definitive Guide™

to

Enterprise xIoT Security

How to protect offices, factories, cities, and the world by finding, fixing, and monitoring **x**IoT devices

Jon Friedman

Foreword by Richard Stiennon

IT industry analyst, author, and columnist

CYBEREDGE PRESS

Definitive Guide™ to Enterprise xIoT Security

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at 800-327-8711 or info@cyber-edge.com.

ISBN: 978-1-948939-36-2 (Paperback)
ISBN: 978-1-948939-37-9 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Phosphorus Contributors: John Vecchi, Thomas King, Sonu Shankar, and Daniel Craig

Table of Contents

Foreword

A large percent of the organizations I talk to can't tell you how many smart devices attach to their networks. Typically, they can't even find 30% or more. Most of the unknown and unmanaged systems are **x**IoT (eXtended Internet of Things) devices – or things like IoT (Internet of Things), OT (Operational Technology), IoMT (Internet of Medical Things), and IIoT (Industrial Internet of Things) devices. Many of them pose serious risks, not only to operational processes and networks, but to core IT systems as well.

What does a threat actor see when looking at your attack surface? Probably:

- ☑ Thousands of insecure, connected devices that you aren't monitoring…
- ☑ A high number of devices that are easy to hack, and likely deployed with default passwords and old firmware…
- ☑ An unprotected attack surface which can threaten your enterprise with business disruption, data exfiltration, or worse.

But you are not alone, and not without opportunities to apply proactive security technologies and best practices to your **x**IoT devices.

This *Definitive Guide™ to Enterprise **x**IoT Security* explains the challenges of protecting **x**IoT devices, including the vast array of device types, the vendors that short-change security issues, the proliferation of protocols and standards, and the simple fact that security agents cannot be installed on most of these systems.

It will also help you understand the processes and technologies needed for defense.

Discovery has always been a core requirement for any kind of IT security. First, discover your assets. Only then can you figure out what to defend and how. This guide summarizes

the requirements for finding and assessing the multitude of strange and wonderful **x**IoT devices attached to your networks.

Remediation at scale is an equally critical topic. Most organizations have thousands of **x**IoT devices, some in offices, but many in remote, industrial, and inaccessible locations. Manually patching vulnerabilities and fixing misconfigurations is a losing proposition (and the reason many organizations have devices with firmware and settings that are years out of date). Here you will find suggestions on how to automate remediation and device hardening.

This guide also contains useful information on how to monitor devices, combat "environmental drift" with better change management, and integrate **x**IoT security solutions with the rest of your IT security infrastructure to improve discovery, remediation, and incident response.

xIoT security is a topic that is only going to increase in importance as more devices are connected to more networks, offering more and richer targets to threat actors. Now is the time to master the basics of this field and get a head start on implementing solutions.

Richard Stiennon
Chief Research Analyst, IT-Harvest; Author; Columnist

Introduction

"It was the best of times, it was the worst of times…" That, of course, is the opening of Charles Dickens' *A Tale of Two Cities*. But it is also an accurate summary of the state of information technology as the Internet of Things begins to mature.

We are already at a point where a vast variety of new devices with computing power and networking capabilities are being added to our offices, our buildings, our factories, our hospitals, our transportation and distribution networks, our cities and towns, and our homes. They have the potential to make our lives dramatically easier, safer, more productive, and more fulfilling.

Unfortunately, many of these devices lack safeguards and security controls that we would consider elementary and essential for conventional IT systems. If compromised, they can become vehicles for information theft, extortion, business disruption, and in extreme cases, physical harm.

This guide aims to help you understand the why's and how's of **x**IoT (eXtended Internet of Things) security, so you can move forward deploying **x**IoT devices with confidence.

Chapters at a Glance

Chapter 1, "The xIoT Security Journey," defines **x**IoT and describes why threat actors target **x**IoT devices and how **x**IoT security needs to improve.

Chapter 2, "Why Is xIoT Security So Hard?," explains the lack of security controls in many **x**IoT devices and why you can't use traditional IT tools to protect them.

Chapter 3, "Decisive Points of Attack and Defense," identifies the four areas that threat actors attack to compromise **x**IoT devices.

Chapter 4, "Visibility and Assessment," discusses how to discover rogue and "shadow **x**IoT" devices, flag security issues, and prioritize remediation.

Chapter 5, "Remediation and Hardening," explores methods for remediating vulnerabilities in **x**IoT devices and hardening them against potential attacks.

Chapter 6, "Monitoring Devices and Managing Change," describes how monitoring and response can fight "environmental drift" and can keep devices secure.

Chapter 7, "Sharing the Load; Integrations," outlines the advantages of integrating an **x**IoT security solution with a variety of IT security tools.

Chapter 8, "Criteria for Selecting an xIoT Security Solution," reviews seven capabilities you should look for in an **x**IoT security solution.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Want to learn more? Follow the corresponding URL to discover additional content available on the web.

Chapter 1

The xIoT Security Journey

In this chapter

- Define "Internet of Things" and "xIoT"
- Learn why threat actors target xIoT devices
- Understand the "xIoT security journey"

"The Internet of Things devoid of comprehensive security management is tantamount to the Internet of Threats."

— Stephane Nappo, CISO and technology strategist

The World of xIoT Devices

The Internet of Things

The *Internet of Things (IoT)* can be defined as the network of devices that have firmware and computing power, can be networked, don't include a keyboard, and are unable to run traditional endpoint security software.

IoT devices include printers, phones, cameras, sensors, monitors, controllers, and thousands of gadgets, gizmos, and thingamajigs that contain chips and a wired or wireless network interface. They are found in offices, homes, smart buildings, smart cities, factories, and vehicles, not to mention on and inside people.

There are a lot of them. According to industry analyst firm IoT Analytics, there will be 17.2 billion global IoT connections by the end of 2023.

What's *not* on the list of IoT devices? Computer workstations, laptops, servers, and smartphones. Why not? Because they are traditional computing devices with keyboards.

What are "xIoT" devices?

xIoT refers to the *eXtended Internet of Things*. It comprises three categories of devices that appear in a wide range of settings: **enterprise IoT devices + network devices + operational technology (OT) devices**.

Enterprise IoT devices include printers, VoIP phones, cameras, network attached storage, smart lighting, and door controllers.

Network devices include routers, wireless connection points, network gateways, load balancers, uninterruptible power supplies, KVM switches, and other appliances.

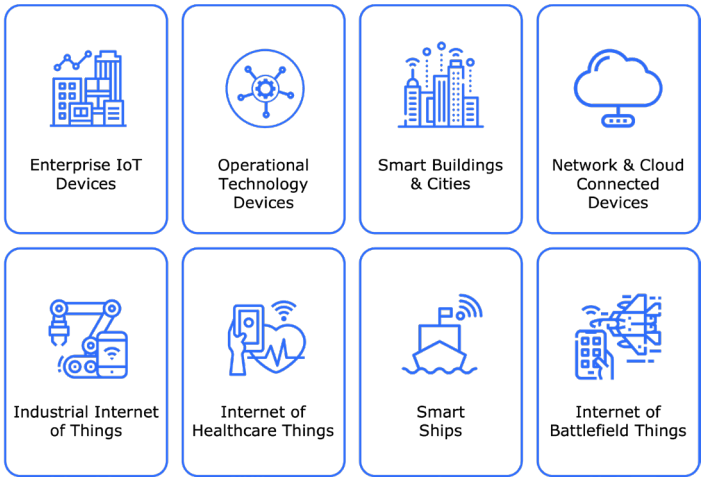

Figure 1-1: xIoT devices are found in a wide range of settings.

OT devices include industrial control systems (ICS), robots, supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), and other acronym-worthy apparatuses that control the operations of factories, pipelines, warehouses, transportation networks, and similar environments.

Network and OT devices share many characteristics with IoT devices, most notably an inability to host conventional IT security tools. If your organization is seeking to protect enterprise IoT devices, it makes sense to provide security for other **x**IoT devices at the same time.

A Profusion of Threats

Cybercriminals, state-sponsored hackers, and other bad actors are increasingly seeking to exploit **x**IoT devices for three reasons:

1. Their numbers are growing by billions every year.
2. They are less protected and monitored than traditional IT systems (see the text box below).
3. They can be incorporated into an incredibly wide range of attacks, including attacks on traditional IT systems and applications.

Why xIoT devices make easy targets

Generally, **x**IoT devices have far less built-in security than laptops, servers, smartphones, and other IT systems, and are unable to host anti-malware and endpoint monitoring software. Many of them can be accessed with a default or weak password, and the majority operate with high-risk or critical vulnerabilities. Large numbers are unknown to security teams ("shadow **x**IoT"). Still more are known but are not monitored for vulnerabilities or suspicious activity. In many organizations, it is not even clear who is responsible for **x**IoT security: IT teams, IT security teams, the operational groups deploying the devices, or nobody at all.

Threats to business continuity

Disabling **x**IoT devices or causing them to function improperly can interrupt business processes, halt data collection, shut down production lines, stop deliveries, paralyze digital and physical infrastructures, and otherwise prevent organizations from producing goods, serving customers, or managing processes.

Threats to safety and the environment

Attacks on traditional IT systems typically affect productivity, revenue, and reputation. Attacks on **x**IoT devices can do the same, but may also result in injury, death, and potentially large-scale environmental disasters.

Extortion and espionage

Because they can wreak havoc in so many ways, **x**IoT devices are excellent tools (from a malicious actor's perspective) for ransomware attacks and other types of extortion. In addition, compromised cameras, sensors, and printers can be used to collect and exfiltrate images and data. For example, images captured by cameras and printers might include intellectual property and other confidential information.

Botnets and crypto mining

Unmonitored **x**IoT devices can be commandeered to attack or benefit third parties. They have been used to host botnets and "mine" bitcoins and other cryptocurrencies. By degrading the performance of devices, these activities can affect their owners' business and potentially create legal liabilities.

Data breaches of IT systems

xIoT devices typically store less data than traditional IT systems. So how could they be involved in massive data breaches?

Simple. They can be compromised and used to stage attacks against an organization's core IT systems. For example, an attacker might be able to plant malicious software on a VoIP phone or networked printer. That malware might be able to capture information from internal databases and cloud-based applications, copy sensitive data to the device, establish a tunnel to the attacker's external server, and then exfiltrate customer data or company and government secrets.

xIoT devices are part of the attack surface for IT systems and data. CISOs and members of IT security teams should be very concerned about **x**IoT security, whether or not they have explicit responsibility for it.

Here is a short article about how **x**IoT devices can be used to stage attacks against IT systems: How APTs Are Achieving Persistence Through IoT, OT, and Network Devices, Dark Reading, June 2022.

New classes of attackers?

In most industries, cybersecurity teams focus on cyber criminals as the primary risk to IT systems. However, when it comes to **x**IoT devices, they need to think carefully about a wider range of threat actors. In particular:

- Is there a chance that state-sponsored hackers would want to take down operations as part of an international conflict?
- Are there ideology-driven "hacktivists" who might try to embarrass the organization or draw attention to controversial corporate policies and environmental risks?
- Might competitors want to spy on the organization or interfere with a critical operational process?

While these risks might seem remote, many global enterprises operate in parts of the world where they need to be taken seriously.

The xIoT Security Journey

Let's turn now to the task facing the teams responsible for protecting **x**IoT devices. They need to move from a state where most **x**IoT devices are vulnerable and unmonitored to one where the vast majority are known, assessed, protected as much as possible, and continuously monitored.

The state of xIoT security today

Facts about **x**IoT security today are shown in Figure 1-2.

80% of organizations can't identify the majority of their **x**IoT devices
The firmware on most **x**IoT devices is old, often past end-of-life and no longer supported by their manufacturers
68% of enterprise **x**IoT devices have high or critical vulnerabilities (CVSS scores of 8 or above)
Most **x**IoT devices are not monitored for vulnerabilities or suspicious activity

Figure 1-2: Facts about **x**IoT security. (source: Phosphorous)

This situation can be visualized as the left side of Figure 1-3. Of all the **x**IoT devices in the typical organization, the vast majority are in one of these conditions fall into one of these categories:

- ☑ Unknown to security teams in the organization ("shadow **x**IoT")
- ☑ Known, but not fully assessed
- ☑ Known and assessed, but not managed (i.e., there is no process to identify and remediate vulnerabilities or harden the devices)
- ☑ Fully managed, but not continuously monitored

Only a fraction of **x**IoT devices are managed and continuously monitored.

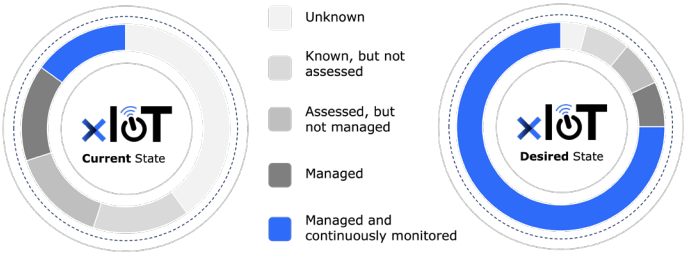

Figure 1-3: The xIoT security journey: current and desired states.

Taking the journey

The goal of the **x**IoT security journey is to dramatically reduce the number of unknown, unassessed, and unmanaged devices, and to increase the number of managed and continuously monitored devices (illustrated on the right side of Figure 1-3).

The rest of this guide describes how to reach that goal.

Chapter 2

Why Is xIoT Security So Hard?

In this chapter

- Understand why vendors don't build many security controls into xIoT devices
- Learn why you can't use traditional IT security tools to protect xIoT devices

"Adversity is the first path to truth."

— George Gordon, Lord Byron, Romantic poet

Several factors make **x**IoT devices harder to protect than traditional IT systems. Let's review them.

Vendors' Lack of Security Focus

Typically, security is not a design point for **x**IoT devices. Most device vendors focus on providing great features for sensing, measuring, controlling, viewing, printing, manufacturing, or whatever else is the main function of the device. Security is an afterthought. Many **x**IoT devices don't protect firmware from tampering or store credentials securely. Others have only very basic access control, such as four-character PINs. Many devices are shipped with default credentials that can be found with a simple web search, and don't require credentials to be changed during setup.

Also, **x**IoT device vendors usually don't follow secure coding practices or operate with secure software development life-cycles. Examples of bad practices:

- ☑ Credentials hardcoded on the device
- ☑ Shared software libraries that contain multiple vulnerabilities (allowing malicious actors who discover a vulnerability on one device to exploit it across many brands and device types)

Who would publish default credentials on the web? Try doing a few web searches like "Password for XYZ," where XYZ is the model of one of the devices in your environment. Or use an **x**IoT security solution to identify all your devices still accessible through default and weak passwords.

Constraints on Single-purpose Devices

Single-purpose **x**IoT devices, such as sensors, monitors, controllers, and cameras, are often deployed in offices, homes, factories, warehouses, pipelines, and other settings where:

- ☑ Space is at a premium
- ☑ Power is limited
- ☑ Real-time or near-real time performance is required
- ☑ Designers are pressured to use low-cost components to keep unit costs down

These constraints often discourage **x**IoT device vendors from building in security features that might require significant power and computing resources.

Vulnerabilities in Multi-purpose Devices

Different issues arise when vendors build their devices around standard IT technologies – without taking security risks into account. Some people still think of **x**IoT devices as single-purpose gadgets with no capabilities beyond their core functions. However, many run full commercial operating systems such as Linux, Android, and Windows, and real-time

operating systems like VxWorks. **x**IoT vendors often neglect to harden their devices, leaving them vulnerable to the same types of malware and ransomware that afflict IT systems.

Long Replacement Cycles

Most enterprises "refresh" desktop computers, laptops, and servers every three to five years. Part of the reason is that older models lack hardware features for security introduced on newer systems and may not support new software releases with critical security updates.

In contrast, the planned replacement cycle of **x**IoT devices often exceeds 10 years, because of the cost and physical challenges involved in replacing old models with new ones.

The average age of enterprise **x**IoT devices is **seven years**. Approximately one-quarter (26%) have been designated "end of life" by their manufacturer. You need to find a way to protect them despite their age and status.

Massive Scale

A recent study found that the average enterprise has between two and three **x**IoT devices per employee. As Figure 2-1 shows, that means an organization with 5,000 employees probably has 10,000-15,000 devices to manage, and an enterprise with 100,000 employees is dealing with 200,000 to 300,000 devices. Clearly, at that scale **x**IoT devices cannot be managed by walking around and touching each one; a high degree of automation is required to monitor and remediate them.

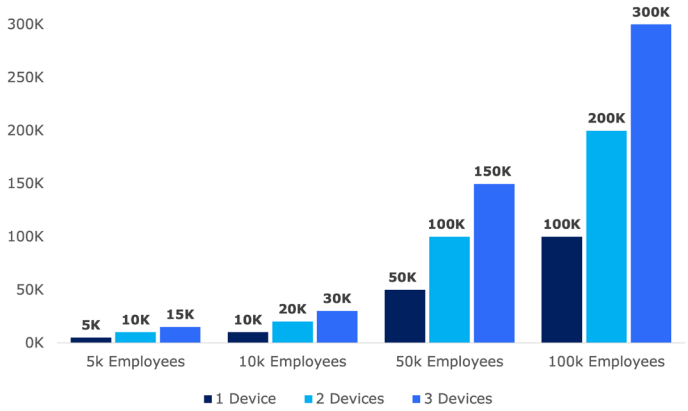

Figure 2-1: xIoT devices in an enterprise, assuming one, two, or three devices per employee.

Inability to Use Traditional IT Security Tools

The vast majority of security tools used by IT teams today are designed to work on systems that can host security agents and communicate via standard protocols. Most xIoT devices don't meet one or both of these conditions, so traditional IT security tools can't communicate with or protect them.

No place for security agents

Most xIoT devices cannot run the local agents used by anti-malware packages, endpoint detection and response (EDR) tools, and other security products used to monitor and protect IT systems and smartphones.

Protocol salad

Many xIoT devices in operational settings use specialized network protocols. Only tools that employ the right protocols can safely be used to interrogate and remediate them. Do you speak BACnet, S7, ENIP, Fieldbus, Totalflow, and Modbus?

Standards soup

IoT and OT security standards and frameworks have proliferated. While they contain useful recommendations for device vendors and security teams, they are too diverse to provide much consistency across networks of **x**IoT devices.

Lotsa gotchas

Diverse operational processes also make it hard to manage enterprise IT security tools on **x**IoT devices. Manufacturer- and device-specific nuances include varied firmware upgrade paths, assorted password complexities, and differing prerequisites and steps for modifying credentials.

IoT security standards and frameworks

Here is a small sample of current standards and frameworks for IoT security: NIST NISTIR 8259 Series and SP 800-213 Series; European Union Agency for Cybersecurity (ENISA) Baseline Security Recommendations for IoT, IoT Secure Software Development Lifecycle, and Guidelines for Securing the Internet of Things; IoT Security Foundation IoT Security Assurance Framework and Secure Design Best Practice Guides; GSMA IoT Security Guidelines; and ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements.

Chapter 3

Decisive Points of Attack and Defense

In this chapter

- Identify four areas that threat actors target to compromise xIoT devices
- Explore methods for defending these areas

"The talent of the strategist is to identify the decisive point and to concentrate everything on it."

— Carl von Clausewitz, general and military theorist

Was the previous chapter a bit depressing? Take heart! One important factor works in favor of **x**IoT security. There are relatively few ways that most **x**IoT devices can be compromised. If we understand these decisive points of attack, we can concentrate our defenses on those areas.

In this chapter we examine the decisive points of attack and outline strategies to defend them. In subsequent chapters we will go into detail about how the battles can be fought.

Firmware and Operating Systems

Unlike IT systems, most **x**IoT devices cannot download and run random application software modules, so security teams do not need to worry about vulnerabilities in those. However, malicious actors can, and do, frequently target firmware and operating systems on devices. And because many **x**IoT device vendors do not perform rigorous security testing, their firmware is rife with vulnerabilities (see Figure 3-1). Also, because of long replacement cycles and irregular patching, many **x**IoT

devices run on out-of-date firmware and operating systems with known weaknesses.

Security and operations teams can prevent attackers from exploiting these vulnerabilities by keeping firmware and operating systems patched and upgraded. However, in practice that is not a simple matter. You must be able to:

- ☑ Safely discover all the devices
- ☑ Know exactly what version to install on each device (installing wrong versions can cause devices to crash or behave unpredictably)
- ☑ Implement processes to store, retrieve, and apply the correct versions to hundreds or thousands of devices

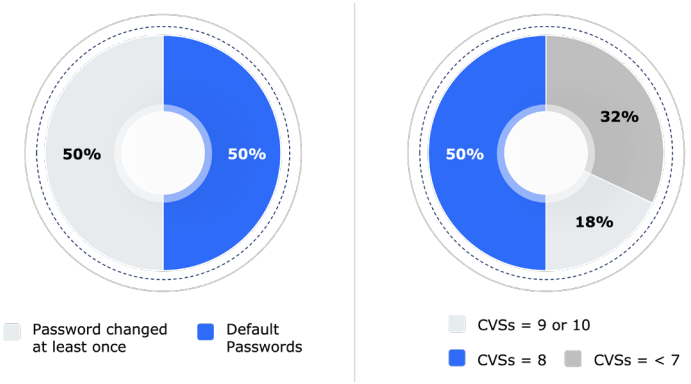

Figure 3-1: Security weaknesses in **x**IoT devices are surprisingly common. (Source: Phosphorus)

We will discuss these challenges in upcoming chapters.

Credentials

While access control and secure authentication have long been top priorities for IT teams, many OT and **x**IoT vendors and operations management groups retain a mindset from an era when **x**IoT networks were isolated from the internet and nobody worried about sharing passwords. As a result, a shocking percentage of **x**IoT devices in use still have original,

default passwords, common passwords like "123456," "admin," and "abc123," or weak passwords that can easily be cracked by a brute force attack.

Of course, once a threat actor has credentials, it's simple to disable or reconfigure a device or plant malware on it.

To prevent these events, security teams should be able to:

- ☑ Detect default, common, and weak passwords
- ☑ Replace them with credentials that meet the organization's security policies
- ☑ Rotate passwords on a regular schedule

Again, these activities involve challenges such as keeping track of the types of credentials allowed or required on each device.

Certificates

Digital certificates are used to prove the authenticity and ownership of servers and devices that have IP addresses. Some applications only permit communication with systems that have a valid, unexpired certificate issued by either the enterprise itself or a public certification authority (CA).

Threat actors can effectively disable **x**IoT devices by deleting or altering their certificates so they will not be authenticated by applications.

This type of attack can be counteracted by checking devices for missing or expired certificates and replacing them with valid ones.

Ports, Protocols, and Services

Many **x**IoT devices ship with open ports and with unnecessary and obsolete protocols like SSH and Telnet enabled. These give attackers many opportunities to compromise the devices.

Once threat actors have a foothold on devices, they can change configurations and parameters, potentially causing the devices to shut down, behave unpredictably, or even produce results

that are the opposite of what is expected (e.g., blow hot air when cold air is needed and vice versa).

Preventing these outcomes requires:

- ☑ Hardening devices by disabling ports and unneeded protocols
- ☑ Monitoring devices and reversing unauthorized changes to configurations and parameters

An example would be disabling WiFi, 5G, and Bluetooth connections for a device that only needs a wired Ethernet connection.

Have you seen these protocols?

Many xIoT devices ship with old, insecure protocols enabled. You really don't want them accepting traffic via Telnet, SNMPv1 (or v2), LLMNR, or for that matter, SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0, or TLS 1.1.

Speed and Scale

Speed and scale are not points of attack, but they are requirements for defense. Attackers can succeed by finding one vulnerable device, while security teams must protect all of them.

For example, if a vulnerability is found in a version of firmware, or a vendor alert reveals that a type of device accepts weak passwords, security teams need to be able to patch the firmware or upgrade the passwords on hundreds or thousands of devices before attackers locate one vulnerable unit.

Chapter 4

Visibility and Assessment

In this chapter

- Learn about discovering rogue, shadow xIoT, and other unknown devices
- Review the types of data that can be collected from devices
- Examine ways to prioritize and communicate remediation actions

"We shall not cease from exploration/And the end of all our exploring/Will be to arrive where we started/And know the place for the first time"

— T.S. Eliot, Modernist poet

The first step in managing the security of **x**IoT devices is to locate, inventory, and assess all of them.

Discovery

As we mentioned in Chapter 1, 80% of organizations report that they can't identify a majority of their **x**IoT devices. The unknown systems are comprised of:

- ☑ **Rogue devices**, connected to the organization's network by employees or contractors without authorization
- ☑ **Shadow xIoT devices**, purchased and deployed by a department without notifying the security team
- ☑ **Forgotten devices**, deployed for a project but no longer listed in any inventory
- ☑ **Unrecognized devices**, new gadgets not perceived as **x**IoT devices but creating the same security risks

A further complication is that IT security teams, network groups, and operations, facilities, building management, and device management teams often keep separate records of the **x**IoT devices in their domains, making it difficult to track, much less manage, the complete set of systems.

You could try to persuade every group in the enterprise to find and report on the **x**IoT devices in their areas. Good luck with that! ☺ Instead, you can use an **x**IoT security tool to traverse the entire environment and safely assess all **x**IoT devices in it. Alternately, if you already have discovery tools and asset inventories, you can pull data from those and maintain a central database with all the information needed for **x**IoT security.

A Hippocratic Oath for device discovery and assessment

xIoT security tools are never asked to swear by Apollo and Aesculapius to "first, do no harm." But they are required to discover and assess devices without breaking them. A malformed packet or an incorrectly structured query can disable a device, with potentially serious consequences. That means an **x**IoT discovery or security management product needs to be very good at safely identifying a wide range of device types and knowing the precise protocols and API calls associated with each of them.

Data Collection

Before you can assess, remediate, and monitor **x**IoT devices, you must know a lot about them. You need information about the devices themselves, and about the status of their security features.

Device fingerprints

It is essential to collect information about each device such as:

- ☑ Manufacturer and model
- ☑ Part number and serial number

- ☑ Static or dynamic IP address and MAC address
- ☑ Firmware and operating system versions

You can't rely on static IP addresses or MAC addresses alone to identify **x**IoT devices. Some use static IP addresses, but others don't. Moving an **x**IoT device with multiple NICs can change the MAC address. An **x**IoT security tool needs to collect enough pieces of data about each device to create a unique fingerprint.

Security posture

It is also important to collect information that can be used to assess the security posture of each device. This might include:

- ☑ Credentials such as a password
- ☑ Firmware and digital certificates
- ☑ Open ports and active services
- ☑ Protocols enabled
- ☑ Unpatched vulnerabilities

90% doesn't cut it

IoT If you want to ensure that remediation and hardening steps (discussed in the next chapter) are reliable and effective, it is important to collect 100% of the relevant information from your **x**IoT devices. And that information has to be 100% accurate. Making a mistake about the model or the firmware level could cause firmware upgrades to fail, potentially disabling the device. Failing to detect a single default or weak password or one insecure protocol could enable attackers to compromise the device.

Assessment

After discovering and collecting data from **x**IoT devices, the next step is to assess them and determine those that need to be remediated first.

Classifying devices

It is a good idea to classify the **x**IoT devices you have discovered both at the level of device type and down to specific manufacturers and models. The types will vary greatly depending on the industry and setting, but in an office, high-level categories would likely include:

- ☑ Printers
- ☑ Phones and video conferencing systems
- ☑ Security cameras
- ☑ Network switches and routers
- ☑ Physical access controllers (locks, biometric entry scanners, etc.)
- ☑ Environmental controls (thermostats, airflow controllers, etc.)
- ☑ Industrial control systems and SCADA systems

These can then be broken down into sub-types and models. These classifications can point you toward particularly vulnerable devices.

Frequent offenders

Some of the devices in office settings merit special attention:

VoIP phones – Often deployed with default credentials and insecure protocols like SSH.

Printers – Widely distributed in vast numbers, they run multiple services and protocols that can be exploited by attackers.

Servers with **lights out management controllers** – Allow attackers to shut down the host computers, run shells, and upload malware.

Security cameras – Some models ship with malware already installed, giving attackers the opportunity to spy, disable surveillance, and attack IT devices.

Flagging security issues

Figure 4-1 shows the types of security issues you can look for with data collected from your **x**IoT devices.

Data	Security issues
Manufacturer/ model/part number	• Devices unsupported or discontinued by the manufacturer • Devices barred by the government for certain industries or locations
Firmware and operating system versions	• Devices with unsupported firmware and operating systems • Known vulnerabilities in firmware and operating systems
Security posture	• Default and weak passwords • Devices with expired and invalid digital certificates • Unnecessary open ports, active services, and enabled protocols

Figure 4-1: Examples of issues that can be identified from **x**IoT data.

Prioritizing remediation actions

After discovering and assessing known and previously unknown devices, most organizations will have a very long list of devices that need remediation to mitigate vulnerabilities or hardening to protect against potential attacks. It therefore becomes very important to prioritize remediation actions and communicate with the groups that can perform them.

While prioritization will vary greatly among organizations, the most important factors tend to be:

- ☑ Likelihood of attack
- ☑ Potential costs and impact of a successful attack
- ☑ Number of vulnerable devices
- ☑ Difficulty of remediation

When prioritizing remediation actions, don't get sucked into a numbers game. Sure, it looks good to report that you upgraded the firmware on 2,000 devices this week, but that may be less important than eliminating vulnerabilities on 20 key controllers. Make sure your decisions are based on actual reduction of risk.

Communicating priority remediation actions

The saying "There's many a slip 'twixt the cup and the lip" goes all the way back to the third century BCE. In many organizations, it's surprising how often the slip is between the people who know what should be done and the people who need to do it. That's especially true when responsibilities are split across various IT, operations, and related groups.

Ideally, critical remediation requests should be communicated as alerts through email, a SIEM, team collaboration tools like Slack, and service management ticketing tools. Remediation actions that are not quite as time sensitive can be communicated via the same channels (with information on their relative priority), or through a trouble ticketing or problem remediation system.

In all cases, the requests should include as much information as possible about the vulnerable devices, their security posture, and the actions to be taken.

Ideally, the alerts and the trouble tickets should be:

- ☑ Generated automatically
- ☑ Communicated via direct integration or API, without manual intervention
- ☑ Recorded in a central database for future review and analysis

Chapter 5

Remediation and Hardening

In this chapter

- Examine the pros and cons of network segmentation
- Explore other remediation options such as patching firmware, managing credentials, and updating digital certificates
- Understand how to harden xIoT devices by disabling or enabling services and features

"The time to repair the roof is when the sun is shining."

— John F. Kennedy, 35th president of the United States

After **x**IoT devices have been discovered and fully assessed, security and OT teams can develop strategies and a roadmap for remediation and hardening. In a few cases, organizations can isolate devices, but more often the best options involve removing vulnerabilities and strengthening defenses at the four decisive points of attack we discussed in Chapter 3.

Segment Networks

You can't "air gap" most **x**IoT devices. Ordinarily, they must be connected to a network to fulfill their mission. However, you can restrict access by segmenting networks into multiple virtual local area networks (VLANs) and tightly controlling access to the VLANs that contain **x**IoT devices. Network segmentation forces attackers to overcome additional access controls before they can reach and compromise **x**IoT devices.

However, a segmentation strategy has several drawbacks. The switching infrastructure needed to create VLANs is expensive. Management of the VLANs adds administrative overhead. Misconfigurations can cause operational problems (e.g., blocking necessary communication with devices) and undermine security effectiveness. Finally, segmentation doesn't help with rogue and shadow **x**IoT devices.

Consider segmentation where the extra expense and effort are justified, but don't rely on segmentation alone. Instead, make sure all **x**IoT devices are fundamentally secure, whether or not they are on specially protected VLANs.

Manage Firmware

Patching and upgrading firmware

As we discussed in Chapter 3, malicious actors like to exploit vulnerabilities in the firmware of **x**IoT devices. They target **x**IoT firmware because:

- ☑ Many device vendors use shared software libraries and fail to thoroughly test firmware (see the Vendor Lack of Awareness section in Chapter 2).
- ☑ Long replacement cycles and irregular patching mean that many devices run out-of-date firmware with known vulnerabilities.

The solution, obviously, is to patch and upgrade firmware frequently. But that can be very challenging. After you detect out-of-date firmware, you need to send exactly the right version for the right model, across hundreds or thousands of units. Trying to install the firmware for SuperDuperJet 595 printers on SuperDuperJet 597 models could make them unusable.

To handle the task at scale, you must:

- ☑ Maintain a central, secure repository of validated firmware for all the **x**IoT devices in your environment

- ☑ Automate the process with an **x**IoT security tool that can recognize the firmware needed for each device, retrieve it from the repository, and distribute it to the targets with little or no human intervention

Knowledge of upgrade paths

There is a nuance to firmware management that most people don't appreciate until it bites them. Sometimes, you can't upgrade directly to the latest version. For example, if a device has firmware version 2.0 and the latest version is 4.0, you may need to install version 2.1, then version 3.0, and only then version 4.0. Your automated tool needs to know this fact and be able to handle the correct step-by-step process.

When to step backward

There are times when you will want to *downgrade* firmware. Say you get an alert from a vendor: they have just discovered that the latest firmware version has a vulnerability that can be exploited to disable the device. They are working on a fix and will have it to you in a month.

Can you tolerate hundreds of at-risk devices for 30 days? If not, the best course of action may be to downgrade to an earlier release of the firmware that does not have the vulnerability, until the fix is ready. Of course, this will be much easier if you have an automated tool that can perform firmware downgrades with a click.

Manage Credentials

Detecting and replacing default and weak passwords

Default credentials are a huge issue for **x**IoT devices. If you refer to Figure 3-1, you will see that fully half of the devices in use today still have the credentials that were on them when they shipped. Only recently has it become a recognized best practice for **x**IoT device manufacturers to ship their products without default passwords.

Among the recommendations to device vendors in the IoT Security Foundation's Secure Design Best Practice Guides: "Never hard-code credentials into an application" and "Remove all default user accounts and passwords." But don't hold your breath waiting for widespread implementation.

Even on devices where credentials have been changed, common and weak passwords are serious problems that make many of these systems vulnerable to dictionary and brute force attacks.

To defend against these threats, security and OT teams need to be able to identify devices with default and weak passwords and work with the devices (and with users) to replace them with unique, strong passwords that conform to the organization's policies.

Rotating passwords

Another important capability for security and OT teams is password rotation. Rotation ensures that compromised passwords are only usable for a limited time. Ideally, the organization will have an automated tool to schedule rotations and change passwords with minimal human interaction.

Know your devices (or make sure your **x**IoT security tool does)! Some devices may accept passwords with only a few characters, or only alphanumeric ones. Others may require a long string, including special characters.

Integrating xIoT security with PAM

Credential management is a complex field that includes aspects of identity management, encryption key management, and other security technologies. Often, many of these capabilities are included in privileged access management (PAM) products. It therefore makes sense for **x**IoT security tools to be integrated with those PAM products. Here are some examples of how that integration can save time and effort (and improve security).

Device discovery and enrollment. The **x**IoT security tool discovers devices, verifies that their credentials can be managed over the network, and enrolls them with the PAM product, which stores their credentials in a secure repository. Without this integration, the PAM product might have no visibility into many of the **x**IoT devices in the enterprise.

Credential management. When the **x**IoT security tool needs to interrogate devices, upgrade their firmware, or take other actions, it obtains the most recent credentials from the PAM product's repository.

Credential rotation. The PAM product keeps track of the organization's credential policies (perhaps with variations based on factors like device types and locations), including policies and schedules for verifying and rotating credentials. When a policy triggers an action, the PAM product notifies the **x**IoT security tool, which performs the action on the devices.

Manage Certificates

In Chapter 3 we mentioned that some applications only permit communication with systems that have a valid, unexpired certificate. Threat actors can effectively disable **x**IoT devices by deleting or altering those certificates.

To protect the devices, you need to be able to detect and update expired certificates.

It is also desirable to be able to check certificates against the organization's policies. For example, certificates should use a relatively recent version of TLS and have the right type of signing status. Certificates that do not conform to these policies should be replaced by ones that do.

Harden Devices

We are using "hardening" here to mean proactively changing device configurations to make them more resistant to attacks.

Hardening typically includes disabling:

- ☑ Unneeded ports and interfaces
- ☑ Unneeded and insecure protocols
- ☑ Unneeded services running on the device

Hardening can also involve making sure that helpful security and management features are enabled, for example:

- ☑ Data encryption on the device
- ☑ Authentication services and access control lists
- ☑ Activity logging

Don't forget to reboot! Configuration changes on many **x**IoT devices (and IT systems) require a reboot. Whether you are hardening devices manually or (ideally) with an automated tool, make sure that rebooting is part of the process.

Device intelligence

Detailed knowledge about security threats = threat intelligence.

Detailed knowledge about **x**IoT devices = device intelligence.

Effective device hardening requires in-depth information about the configuration options of all the **x**IoT devices in your environment. You, or the supplier of your **x**IoT security solution, need to be able to keep up with the latest devices and their configuration choices.

That can be quite a challenge, because of the enormous variety of **x**IoT devices and their vast range of capabilities and features.

Chapter 6

Monitoring Devices and Managing Change

In this chapter

- Learn how xIoT devices fall out of compliance because of "environmental drift"
- See what kind of monitoring and response processes can keep xIoT devices secure for the long term

"Let the eye of vigilance never be closed."

— Thomas Jefferson, third president of the United States

Non-compliance Creeps In

Let's imagine that every **x**IoT device in our environment has been discovered and assessed. Let's say that all of them have been hardened based on the organization's security policies, and every vulnerability and security weakness has been remediated. Are we finished with **x**IoT security? Can we go home and take a nap?

Of course not.

Environmental drift

One of the biggest challenges for **x**IoT security in the long run is "environmental drift": actions that inadvertently diminish security. Typical causes include:

☑ End users who change strong passwords to weak ones

- ☑ Operations team members and IT administrators who modify device configurations without considering security
- ☑ People who reset devices to factory settings using the "paper clip reset" or some other method (see text box)

The curse of the paper clip reset

The classic paper clip reset occurs when someone in an office or factory decides that a device isn't performing properly and, following the common wisdom "when in doubt, reboot," inserts the end of a bent paper clip into the little hole on the side. This causes the device to perform a factory reset. It comes up with the default password, open ports, a full set of enabled protocols (Telnet, anyone?), and other insecure settings. The perpetrator returns to work happy, with no one any the wiser (except for the bad guy scanning the network).

Of course, a bent paper clip isn't the only way to initiate a factory reset. Depending on the device, turning the power on or off or entering the right command might do just as well.

Additional devices

Organizations are constantly adding new systems to their networks. Many of these are known to the security team, but others are rogue or shadow **x**IoT devices that are not.

New models and device types

Among additional devices, new models and new device types are special cases. Not only do these need to be discovered, but the organization also needs to take several steps to be able to assess and remediate them.

In short, **x**IoT security can never stand still. Processes for ongoing monitoring and remediation need to be in place. In addition, **x**IoT security tools must be "extensible"; that is, they must be able to promptly adapt to and address new device types.

Monitoring and Alerting

Ongoing discovery and assessment

Not surprisingly, effective **x**IoT security requires ongoing discovery and assessment of devices across the organization's environment. This process includes discovering new rogue and shadow **x**IoT devices and collecting data about each device and its security posture. It also involves flagging security issues such as unsupported devices, old firmware versions, known vulnerabilities, default and weak passwords, expired and invalid certificates, and unnecessary ports, protocols, and services.

Alerting and response

The organization should have a process in place to alert relevant parties to **x**IoT security issues and manage remediation.

Figure 6-1 illustrates this type of process. An **x**IoT security solution discovers a group of new devices and determines that they have weak passwords. It then:

1. Generates an email alerting the person responsible for the devices
2. Interfaces with the organization's trouble ticketing system and creates a ticket listing the devices, describing the issue, and recommending remediation actions
3. Interfaces with the PAM system to register the devices and assign them strong passwords consistent with the organization's security policies
4. Logs onto the devices using the old, weak passwords and replaces them with the new, strong passwords
5. Returns to the ticketing system and marks the ticket as resolved

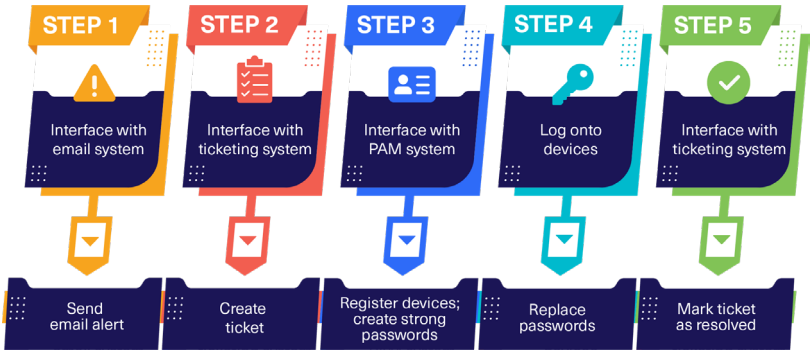

Figure 6-1: Illustration of remediating an **x**IoT security issue with an automated response process

Managing New Device Types

Over time, any organization will add new models of existing devices and introduce new device types. To be ready to manage these devices, the organization or its **x**IoT security solution provider needs to take actions like:

- ☑ Acquiring the latest firmware and knowledge of firmware upgrade paths
- ☑ Obtaining "device intelligence": details about the features and configuration options of the devices
- ☑ Defining policies on how to manage the new models and device types when security issues are detected
- ☑ Creating alerting and response processes to manage remediation

Ideally, the organization or its solution provider can take these actions quickly to minimize the window of opportunity that threat actors have to exploit vulnerabilities in the new devices.

Chapter 7

Sharing the Load: Integrations

In this chapter

- Learn what tasks are best handled by a purpose-built xIoT security solution
- Review other security products that should be integrated with an xIoT security solution

"When spider webs unite, they can tie up a lion."

— African Proverb

Cybersecurity has so many facets that multiple tools need to work together to manage and protect information assets. That is certainly true for **x**IoT security. We mentioned some desirable integrations in previous chapters. Here, we compare tasks that are typically performed by specialized **x**IoT products with others that are usually handled by other security tools integrated with them.

Tasks for xIoT Security Solutions

Security teams have many choices of tools that manage and protect conventional IT systems such as computer workstations, laptops, servers, and smartphones. However, the vast majority of these tools lack one or more capabilities needed to safeguard **x**IoT devices, such as:

☑ The ability to discover devices that use non-standard (for conventional IT) networks and protocols

- ☑ The ability to discover and interact with **x**IoT devices safely (i.e., without a significant risk of disabling the devices or causing unexpected behaviors)
- ☑ Access to information about all recent models of **x**IoT devices, including details such as features, firmware versions, protocols, and system services needed to assess their security posture
- ☑ Knowledge of firmware upgrade paths, minimum and maximum requirements for passwords, and "gotchas" specific to **x**IoT devices
- ☑ The ability to discover, assess, remediate, harden, and monitor devices without installing software on them (i.e., an agentless architecture)

Only security tools purpose-built for **x**IoT security have all these capabilities.

Advantageous Integrations

Figure 7-1 shows some of the IT security tools that can be integrated with an **x**IoT security solution to streamline and strengthen overall security in an enterprise.

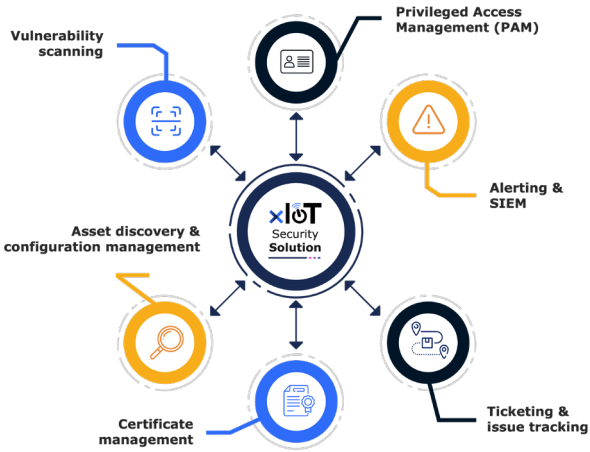

Figure 7-1: Typical integrations between an **x**IoT security solution and existing IT security tools.

Vulnerability scanning

xIoT security solutions and IT vulnerability scanning and management tools can work together to provide a comprehensive view of vulnerabilities across all the systems and devices in the enterprise.

This integration enables security teams to prioritize remediation tasks and allocate remediation resources to maximize risk reduction.

Asset discovery and configuration management

Because **x**IoT security solutions can discover and collect detailed data from **x**IoT devices, their integration with asset discovery and configuration management database (CMDB) products enables organizations to create a single database of all types of information assets and their characteristics.

This integration allows security teams to uncover and begin monitoring rogue and shadow **x**IoT devices, create complete lists of devices that are out of compliance with security policies, and better prioritize and organize remediation activities. It also speeds up the creation of reports for auditors with information about compliance, unsupported devices, critical vulnerabilities, and remediation activities.

PAM and identity management

A PAM product or identity management platform can work with an **x**IoT security solution in several ways. It can create and securely store credentials for newly discovered **x**IoT devices, provide information on user roles and permissions, supply up-to-date credentials when the **x**IoT solution needs access to devices for interrogation or remediation, and work jointly to rotate passwords and other credentials. (See Integrating **x**IoT security with PAM on page 29).

Certificate management

An **x**IoT security solutions can identify **x**IoT devices with invalid and expired certificates and replace them with valid certificates issued by a certificate management system.

Log management, SIEM alerting, and ticketing

An **x**IoT security solution can generate activity messages for log management products. It can create alerts for SIEMs, IT security groups, and OT teams with information about vulnerabilities and security issues. It can also interact with ticketing and issue tracking systems to initiate remediation tasks.

For examples of how an **x**IoT security solution can integrate with other security tools, read the Phosphorus integration briefs for Tanium and Sevco, or watch the CyberArk and Phosphorus integration video.

Collaboration Among IT Security, OT, and Other Teams

While we are on the topic of integration, it is important to acknowledge that in many organizations there is little or no integration among IT security, network, OT, facilities, security operations center (SOC), and other teams responsible for managing and protecting **x**IoT devices. Often, they live in separate worlds and rarely talk, much less work together.

An **x**IoT security solution that is integrated with existing IT management and security tools enables these teams to collaborate on eliminating vulnerabilities and responding to threats. It gives all the relevant parties an opportunity to see the same data, utilize the same workflows for response and remediation, and exchange information and insights.

When you deploy an **x**IoT security solution, one team may be driving the effort, but make sure that all relevant groups are involved and can influence the implementation. You want to get everyone's insights and buy-in.

Chapter 8

Criteria for Selecting an xIoT Security Solution

In this chapter

- Explore seven criteria for selecting the xIoT security solution that best meets the needs of your enterprise
- Revisit the starting point and end goal of your xIoT security journey

"There's no wrong time to make the right decision."

— Dalton McGuinty, Canadian political leader

How can you select an **x**IoT security solution that is right for your enterprise? Let's consider some of the criteria you should keep in mind.

Remediation and Hardening

It is important to recognize at the outset that some **x**IoT security products only handle device discovery, or discovery and assessment. Others were originally designed for discovery and had limited remediation features such as firmware patching bolted on later.

These products don't provide much help with the herculean task of remediating and hardening hundreds or thousands of **x**IoT devices. Unless your enterprise already has tools that provide excellent automated remediation and hardening, you should look for solutions that provide a rich set of features for the end-to-end capabilities described in this guide:

- ☑ Discovery
- ☑ Assessment
- ☑ Remediation and hardening
- ☑ Monitoring
- ☑ Reporting

Breadth and Depth of Coverage

IoT + network + OT devices

Quite a few security products manage only IoT devices, or IoT plus OT devices. Some have an even narrower focus, such as devices for smart buildings, factories, utilities, or healthcare facilities.

As we discussed in Chapter 1, IoT, network, and OT devices share many characteristics, so it makes sense to find a solution that can manage all of these at the same time.

Avoid the trap of selecting a solution that addresses one pressing problem quickly, without considering other needs for **x**IoT security. Organizations that yield to that temptation usually end up with multiple, overlapping products, fragmented data, and higher costs.

Using a single security solution for IoT, network, and OT devices also helps IT, OT, facilities, physical security, and device management teams work together. They all see the same data and can track progress toward remediating devices and addressing issues across the enterprise.

Device coverage

Most enterprises have hundreds or thousands of **x**IoT device types and models they need to protect and manage.

In Chapters 4 and 5 we examined how much information must be known about *each one* of those devices to interrogate, assess, and remediate it. That information includes physical characteristics, network protocols, firmware levels and

upgrade paths, default passwords, minimum and maximum requirements for credentials, use of digital certificates, and all the details needed to harden the device.

You should look for an **x**IoT security solution that captures all this information for *all* the **x**IoT devices in your enterprise.

Ask potential **x**IoT security solution providers to confirm that they cover the devices in your environment. Don't be afraid to give them a long list.

Scalability

We haven't addressed scalability yet in this guide, but there are two aspects that are particularly important.

Performance for many devices

If your enterprise contains thousands or tens of thousands of **x**IoT devices, you need to make sure that your **x**IoT security solution can perform critical tasks in acceptable time frames. These tasks include discovering devices, identifying vulnerabilities, and quickly remediating all similar devices across the enterprise when a vulnerability is discovered.

Impact on networks

xIoT security solutions vary widely in the amount of network traffic they create. Some solutions can have a noticeable impact on the performance of networks and applications.

Ask solution providers for examples of customers that successfully used their solution for the same number of devices you have in your enterprise.

Deployment Options

Deployment is another topic we haven't discussed, but it can be an important one for some organizations. We're talking about options to run an **x**IoT security solution on different platforms, principally:

- ☑ As a virtual machine (VM) on a server in a data center

- ☑ On a hardware appliance
- ☑ On a cloud platform

You might only be interested in one or two of these. However, to ensure maximum flexibility for the future, you might favor solutions that offer all three options.

Out-of-the-Box Integrations

In the previous chapter, we reviewed the advantages of integrating security products with your **x**IoT security solution, including:

- ☑ Vulnerability scanners
- ☑ IT asset discovery and management tools
- ☑ PAM and identity management products
- ☑ Certificate management systems
- ☑ Log management, SIEM, and ticketing systems

You should look for **x**IoT security solutions that provide out-of-the-box integration with tools of these types that you are already using or plan to use.

Unless there is no alternative, avoid integrating these types of tools with an **x**IoT solution yourself. Integrations performed internally can seem simple in the short term, but tend to be costly in the long run because of the time and effort needed to keep up with changes in the products on both sides of the interface.

Safe Interaction with Devices

We've said this before (see *A Hippocratic Oath for device discovery and assessment* on page 18), and we'll say it again: an **x**IoT security solution must know enough about the devices it is interrogating and remediating to "do no harm." Make sure

the solution providers you are considering have a good safety record in this area.

Why? Here are a couple of scenarios to consider.

The building management system in your corporate headquarters uses the Building Automation and Control Network (BACnet) protocol to communicate with the controllers that handle heating, ventilation, air conditioning, lighting, fire detection, and elevator operation. If your **x**IoT security solution interrogates these controllers with malformed BACnet packets, it could cause the controllers to reboot, shut down, or behave erratically. You really don't want any of those things to happen when the CEO (or anyone else) is in an elevator.

A food processing plant relies on a series of sensors and controllers to provide continuous and accurate temperature control across its production lines. Any unplanned interruption in the functioning of those devices could shut down processes. A shutdown would force the plant to discard large batches of in-process materials, raising costs, reducing productivity, and causing some people to lose their year-end bonus.

Vendor Vision

You want an **x**IoT security solution that meets your requirements today and will evolve to meet different requirements tomorrow. You should feel comfortable that the vendor's vision aligns with yours.

You also want a partner that will respond quickly to your questions and needs. For example, if you start deploying a new type of **x**IoT device, the vendor should be ready and willing to add it quickly to their list of supported devices.

CPS protection platforms: the future of enterprise xIoT security?

Speaking of vision…

One of the services that analyst firms provide to the IT industry is conceptualizing and naming new product categories. Three analysts at Gartner, Katell Thielemann, Ruggero Contu, and Wam Voster, have taken a shot at defining a concept that can be seen as a blueprint for comprehensive **x**IoT security solutions. They call it the "cyber-physical systems" (CPS) protection platform.

It's too soon to tell if this term will be widely accepted, but it is worth examining how the Gartner analysts describe this category and how it relates to the ideas we have been discussing in this guide.

According to Thielemann, Contu, and Voster, there has been an evolution from isolated OT systems, to converging IT and OT systems, to emerging cyber-physical systems where IT and OT systems share networks, exchange information, and perform a wide variety of new functions in office, industrial, and civic settings.

But these emerging cyber-physical systems pose unique security challenges. The first is discovering and identifying assets that are too numerous and varied to be found and assessed by manual methods or discovery tools built for conventional IT systems. The second is the work required to wrap additional security features around the assets discovered by the CPS protection platform.

Some of the security features of a CPS protection platform highlighted by the analysts are:

- Real-time visibility and categorization of assets
- Support for a wide range of protocols used by IoT and related devices
- Real-time flagging of "rogue" devices
- Prioritized patching
- Detailed logs of device configuration changes
- Integration with SIEMs, ticketing systems, and SOAR tools

Clearly, the analysts' vision of a CPS protection platform overlaps a great deal with the capabilities of the **x**IoT security solutions we have been discussing. We will be watching closely to see how they elaborate on the concept, and whether CPS protection platform (or an alternative term) will be adopted as the name of a major new technology product category.

The Gartner research note *Innovation Insight for Cyber-Physical Systems Protection Platforms* is available at: https://www.gartner.com/en/documents/4017995 (subscription required).

The Destination of Your xIoT Security Journey

At the end of Chapter 1, we briefly outlined the state of **x**IoT security today, where the large majority of **x**IoT devices are unknown, or known but not assessed, or assessed but not managed, or managed but not continuously monitored. We said that the goal of **x**IoT security was to reduce the number of devices in all those categories, as illustrated in Figure 1-3 on page 6.

Figure 8-1 recaps the result we want to achieve.

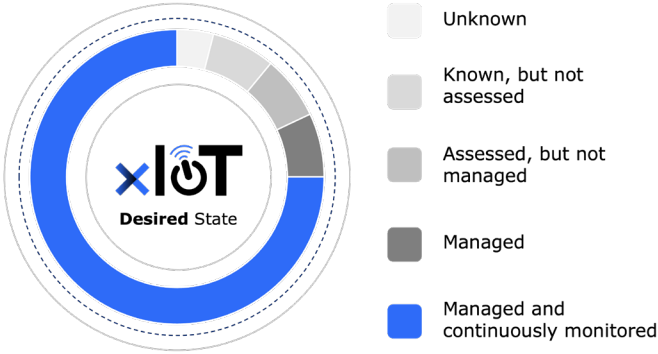

Figure 8-1: Desired state of devices at the end of the **x**IoT journey.

In short, the right **x**IoT security solution for your enterprise is the one that gives you the most confidence that you will be able to complete your **x**IoT security journey. It should enable you to reach the point where the large majority of your **x**IoT devices are efficiently, accurately, and continuously discovered, assessed, managed, and monitored

Phosphorus

xIoT Breach Prevention for the xTended Internet of Things

xIoT Discovery & Assessment

xIoT Hardening & Remediation

xIoT Detection & Response

www.Phosphorus.io

Do you know how why eXtended Internet of Things (xIoT) devices are easy to attack? Do you know how yours can be protected?

"**x**IoT" devices are being deployed in our offices, buildings, factories, cities, and homes. They will make our lives easier, safer, and more productive. But most lack security controls we would consider essential for conventional IT systems. They put us at risk for business disruption, extortion, information theft, and sometimes physical harm.

- IoT and **x**IoT devices — understand what they are and aren't
- Decisive points of attack and defense — learn the four ways threat actors compromise **x**IoT devices
- Visibility and assessment — find out how you can discover thousands of unknown and unmanaged devices and assess their risk
- Remediation and hardening — review how you can fix vulnerabilities automatically, at scale, and prevent future compromises
- Managing change — explore ways to defeat "environmental drift" and exchange information with asset management, PAM, and SIEM systems
- Requirements for **x**IoT security — explore seven criteria for finding the solution you need

About the Author

Jon Friedman has over 25 years experience in industry analysis and marketing roles at software and IT services companies. He has described cutting-edge technologies and their business benefits for more than 50 technology firms. Jon has a BA from Yale and an MBA from Harvard.

CYBEREDGE PRESS

Not for resale

ISBN 978-1-948939-37-9