Before bounties: know your assets

BY ELEANOR BARLOW · AUGUST 13, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **Why maintaining a complete and up to date asset inventory is essential for successful bug bounty programs**, ensuring all potential attack surfaces are visible and testable.
- **What types of assets should be tracked, including hardware, software, cloud resources, and shadow IT, and how to categorize them effectively** to improve vulnerability discovery and risk management.
- **How practical asset management tools and workflows can simplify visibility and support a stronger security posture and meaningful bug bounty results** by reducing blind spots and helping prioritize remediation.

If you are unaware of what's running in your environment, you can't patch, monitor, or secure it. The simple fact is, you can't defend what you don't know exists. If your team is unsure of an asset, such as a subdomain or an unpatched staging server, it will not be included in your security controls. If left undetected, eventually a threat actor will find and exploit it.

As one of Intigriti's leading bug bounty hunters discusses in '[Top Hacker in Q2]'

> **"You could always find that forgotten server. There can always be a DNS entry pointing to a private address space; that's something you can use later if you find a Server-Side Request Forgery (SSRF). Maybe that staging server is not pointing to Cloudflare like the production servers."**
>
> JCA

A lack of asset management can lead to insecure devices, which, in turn, can lead to breaches and data leakage. Effective asset management is a cornerstone of cyber security maturity and is essential for meaningful bug bounty results.

Meeting cybersecurity compliance

Because an up-to-date asset inventory is the bedrock of risk management, as well as incident response and vulnerability scanning, multiple cybersecurity frameworks, including ISO27001, SOC2, NIS2, NIST, and CIS, highlight its importance.

The **Network and Information Security Directive (NIS 2**), for instance, is a legal framework designed to improve cybersecurity and critical infrastructure throughout the European Union (EU). The first step toward being NIS2-compliant is to showcase the status of all your IT assets. This includes being able to identify all hardware and software in use and then being able to assess the associated risk levels.

ISO27001 guarantees the safe management and security of assets such as financial information, intellectual property, employee details, or information entrusted by third parties. It also requires

companies to identify and document their assets, identify associated risks, and put in place steps to protect said assets.

> **"Providing the highest levels of security is at the core of what we do. ISO/IEC 27001 is the best-known and most sought-after certification by our customers. By achieving this certification, we've taken another step in ensuring our customers can have absolute confidence in the security and privacy of what we do."**
>
> **Niels Hofmans, Head of Security at Intigriti.**

SOC2 (System and Organization Controls) SOC 2 is a compliance standard that requires businesses to manage and secure sensitive data according to five key trust criteria. These are Security, Availability, Processing Integrity, Confidentiality, and Privacy. In the context of asset management, SOC 2 emphasizes maintaining an accurate inventory of physical and digital assets, enforcing access controls, ensuring system availability, securing sensitive and personal data, and managing the full asset lifecycle. Read more about SOC2 here.

The **NIST Cybersecurity Framework** includes asset management as the first step within its 'Identity' section.

'The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistently with their relative importance to business objectives and the organization's risk strategy' – NIST, Cybersecurity Framework, Identify

And the **Center for Internet Security (CIS)** Controls focuses on inventorying hardware and software assets. Control 1 specifies the control of enterprise assets:

'Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.' - Inventory and Control of Enterprise Assets.

While Control 2 specifies maintaining comprehensive inventories of software assets:

'Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.'- Inventory and Control of Software Assets

What to include in your asset inventory

A respectable asset inventory should include everything within your company's domain, including hardware, software, cloud assets, network devices, domains, and subdomains.

Hardware should include elements such as mobiles, laptops, IoT devices, and servers. Software should include all apps, licenses, and firmware.

Many obscure or less-used elements can be missed. Printers, for instance, or charging poles connected to the electricity network by Distribution Network Operators (DNOs), might be missed.

For your cloud assets, make sure to include storage accounts, as well as serverless functions, cloud, virtual machines, and S3 buckets.

'AWS S3 (Simple Storage Service) buckets are a popular storage service used by software companies and organizations to store public as well as sensitive data. However, the implementation of this service is not always correctly done. A single missing access policy can often introduce security risks, data leaks, or other unintended consequences.' – Hacking misconfigured AWS S3 buckets

Under the network devices list, catalogue all switches, routers, and firewalls. Domains and subdomains should include all active as well as parked domains and DNS records.

'Domains are managed centrally as company-level assets. Previously, duplicate domains with identical names and types have been automatically merged into single, unique asset entries. External APIs and existing integrations are not affected by this update.' - Asset Management

Another element to provide is Shadow IT, such as rogue devices, developer instances, and unofficial SaaS tools.

'Shadow IT refers to assets that were created without formal IT or security approval. This can include developer environments, rogue APIs, and unregistered cloud instances. These elements can bypass inventory controls and, therefore, not be included in scanning or bug bounty scopes.' - Security Maturity Complexity

The visibility challenge

Despite the clear importance of having an up-to-date asset list and many available guides on what to include, it begs the question, 'Why does asset management remain a challenge for most companies?'.

Well, many on-prem environments still rely on manual processes and, often, outdated CMDBs.

'Due to the dynamic nature of modern environments, Configuration Management Databases (CMDBs) are becoming more difficult to maintain. Elements such as cloud instances and containers need to be factored in. Manual updates are time-intensive, and poor integration and a lack of tools can lead to incomplete entries. Alongside this, a lack of direction and, with it, a lack of ownership, instills a blame culture where responsibilities are not clear.' – Security Maturity Complexity

For cloud-based customers, the challenge is then the use of siloed cloud solutions, which might not end up in the central asset management list.

Tools to simplify asset visibility

There's no one-size-fits-all solution, but there is a mix of tools you can use to get started, depending on your environment.

- For both hybrid and cloud-centric environments, you can use tools such as Asset Panda, which can be applied for asset tracking and reporting on both hardware and software inventories. It comes with mobile support, custom workflows, and barcode scanning.
- BlueTally is useful for asset management with integrations to other platforms such as Azure AD, Intune, and JAMF, which can be used for tracking assignments as well as lifecycle.

- Microsoft Intune can be used for managing endpoint security, inventory, and compliance across mobile devices, OS, and Windows machines. As well as Mobile Device Management (MDM) solutions, such as Intune and JAMF.
- For a traditional on-prem service, Active Directory (AD) can be used to track domain-joined devices, users, and groups, and provide policy enforcement.
- ServiceNow IT Asset Management (ITAM) is an enterprise-level asset and configuration management platform with automation capabilities for processes.
- For hybrid environments, tools such as Lansweeper can provide an agentless network for asset discovery and inventory.
- And Snipe-IT is an open-source IT asset management system designed for small to medium-sized companies that require on-prem deployment.

Next steps

Before jumping to the next thing on your cybersecurity to-do list, pause, and ask yourself, your team, and your company, “Do we know what we own?”

If the answer is anything less than 100% yes, then start looking into your asset management. This is where the real cybersecurity begins. Accurate asset management will be the foundation to build your security maturity on and will be the basis for fruitful bug bounty hunting.

For proactive steps to asset management, read this blog.

Or, if you are unsure about anything discussed in this article, or for any bug bounty-related questions, contact the team here.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years’ experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.