Asset management

Implementing asset management for good cyber security.

Introduction

If you want to apply effective security controls, knowing what assets you have within your environment is fundamental. It's far easier to protect things that you know about.

This guidance explains the importance of asset management for cyber security and outlines the properties and practices needed to achieve good cyber security outcomes.

Below we give a working definition of what counts as an asset, point to some useful data sources and detail the ways in which asset management and cyber security can be mutually beneficial.

The asset management challenge

The diversity of asset types and their sheer volume, even in small organisations, can make asset management a challenging task. Hardware, software, virtual infrastructure, information, and online accounts must all be considered.

The effort is worthwhile, because asset management can help to avert many security incidents. Having the right visibility of your assets where it's needed gives you the chance to take remedial action, before an incident can develop.

What is an asset?

Assets can be thought of as, anything that can be used to produce value for your organisation.

This includes information, such as intellectual property or customer data. It encompasses many types of technology too, both IT and OT, hardware and software, physical locations and financial capital. And, of course, it includes your people, their knowledge and skills.

From a cyber security perspective, we are primarily interested in two types of asset:

- **Assets that must be configured or managed to achieve security outcomes.**
  For IT assets, IT Service Management standards (e.g. ITIL 4 and ISO 20000) refer to this type of asset as *Configuration Items*.
- **Assets that may be impacted as a result of a cyber incident.**
  These are often the things you are trying to protect.

Shadow IT

Also called grey IT, 'shadow IT' refers to IT assets that are used within an organisation for business purposes, but are not accounted for as part of the asset and risk management processes, or are not integrated with corporate IT processes.

Such devices are concerning because they are unlikely to align with the organisation's security or data governance policies and therefore constitute an unknown risk.

The importance of asset management

Asset management is not about making lists or databases that never get used. Good asset management means creating, establishing and maintaining authoritative and accurate information about your assets that enable both day-to-day operations and efficient decision making when you need them most.

Asset management provides the foundation for most other areas of cyber security:

- **Risk management**. Understanding and managing cyber risk depends on assets being accounted for. If assets are allowed to slip under the radar, it

will not be apparent if appropriate security controls are missing, resulting in unmanaged risks.

- **Managing legacy**. All software and hardware eventually becomes out of date. Continuing to use products beyond that point involves increased risk, or increased costs to mitigate those risks. Asset management can help organisations identify when systems will reach *end of support* and plan ahead. Our Obsolete products guidance can help further with managing legacy assets.
- **Identity and access management**. Being able to identify users and devices is necessary in order to implement an effective identity and access management system. Asset management can help ensure all users and devices have unique identities, and can also help identify resources that need access controls applied. See our Introduction to identity and access management for more detail.
- **Vulnerability and patch management**. One of the best defences possible for cyber systems is to ensure they don't contain known vulnerabilities, as these are easy attack points. Having accurate information on hardware and software assets provides the basis for ensuring available updates are applied and knowing where to scan for vulnerabilities. It's also useful to be able to quickly answer questions such as "does vulnerability X affect us?" whenever high impact vulnerabilities are announced. Please see our Vulnerability management and Vulnerability Scanning Tools and Services guidance for more information on this topic.
- **Monitoring**. Some threats cannot be prevented, so it's important that you have the ability to detect and investigate potential compromises, subsequently mitigating any threats. An effective monitoring capability depends on having access to the right data. Asset management can help you identify relevant data sources and enrichment information that may be needed for your monitoring capability. Our Introduction to logging for security purposes and Logging and protective monitoring guidance can help further.
- **Incident management, response and recovery**. Knowing your assets and determining which are most critical to your organisation helps you plan for, respond to, and recover from incidents. By ensuring nothing important is

missed and having the right information available, you will be able to act quickly and minimise disruption.

- **It's not just cyber security**. Most business operations depend on some aspect of asset management. This includes IT operations, financial accounting, managing software licences, procurement and logistics. While they may not all need the same information, there will be some overlap and dependencies between the respective requirements. The security aspect should not be considered in isolation or as the primary consumer of asset information, so integrating and coordinating asset management across your organisation will help reduce or manage any conflicts between these functions.

Integrating asset management into your organisation

Asset management is challenging to implement, it involves a level of coordination throughout the organisation. Proper asset management is not just

about the technology. Non-technology functions, such as procurement, must also be involved in the asset management life cycle.

Given these complexities, it's very important to have the buy-in of senior management. It's also essential have an ‘owner’ for the whole asset management system. Without an owner, coordination throughout the organisation will be difficult and assets may not be effective.

Asset management should form part of enterprise architecture, or cyber security process, with the current status of the asset management process being regularly presented to senior management.

What should be included in a good asset management approach

An asset management system will have a number of features that could add value from a cyber security perspective.

Your environment may already have the tools in place to leverage some or all of theses properties. But all environments are different, so you should assess the need for each function.

The list below details the cyber security considerations which should be taken into account when designing an asset management system. The list is unordered.

- **Asset discovery**. Use tools to scan your environment for new, modified or removed assets on a regular or continuous basis. This helps to maintain an accurate inventory of your assets and could be used to detect unauthorised changes to your environment.
- **Authoritative source of information**. Maintain a record of assets that everyone agrees reflects the environment. Consider normalising and consolidating asset information to avoid duplication and make it more

accessible. This ensures that collected information can be used effectively by all stakeholders, and does not require additional effort to validate.

- **Accurate source of information**. Asset information should be collected regularly to ensure it is kept up to date and a 'confidence' score or 'last seen' timestamp recorded, to reflect how stale or uncertain the information is. It may be appropriate to collect server information once a week because changes are infrequent, but desktop information may be needed once a day for configuration accounting or vulnerability management
- **Availability of asset information**. Ensure asset information is made accessible to support the relevant use cases in your organisation. A Configuration Management Database (CMDB) could be a significant component in your asset management solution, however this may need to be supported by a range of tools to facilitate the collection, processing, storage and use of asset data across your organisation. This ensures that collected asset information can be used productively.
- **Human factors**. The asset management process should accommodate the needs of users across your organisation and account for human factors such as usability and accessibility. A pragmatic approach may be necessary to avoid excessive bureaucracy. Using asset information to streamline business processes may help incentivise users to fully engage in the asset management process. This helps ensure that the accuracy of asset information is not diminished as a result of users finding workarounds and resorting to shadow IT.
- **Automation**. Automated mechanisms should be used to update asset records wherever practical. Ideally, tools should record asset information in response to changes in the environment, instead of detecting changes after they've happened. New projects should be encouraged to incorporate automated asset management from the start, to avoid technical debt as systems develop or get abandoned over time. This helps ensure accurate records are maintained and updates are less likely to be missed or forgotten, while also reducing the ongoing cost and effort required.
- **Completeness**. Ensure all assets are accounted for by the asset management process. This should include physical, virtual and cloud resources, along with your organisation's Internet presence, in the form of

social media accounts, domain name registrations, IP address spaces and digital certificates. This helps avoid any assets not being configured with the appropriate security controls and is required for compliance and vulnerability scanning.

- **Comprehensive visibility**. Identify how your organisation will use asset information and ensure sufficient details about your assets are collected to support these use cases. For example, knowing versions for all the software installed on your machines helps identify a much wider range of vulnerabilities than just knowing the operating system version. Where certain details may be difficult or costly to capture, consider whether these could be captured less frequently or retrospectively, alongside other mitigations such as network separation. This helps ensure that asset data can be used effectively and does not become unusable as a result of gaps in collection.
- **Change detection**. Ensure changes in asset information are recorded and use multiple data sources to identify inconsistencies. For example, a new spotted device on the network with no corresponding device management enrolment. This helps to identify unauthorised changes to your environment and helps in the investigation of security incidents.
- **Confidentiality**. Consider the sensitivity of asset data collected. Apply appropriate protections and access restrictions, while ensuring relevant use cases are supported. For example, all users should be able to look up the assets they are responsible for, but arbitrary bulk queries should be prevented. Consider monitoring access to asset data for possible signs of reconnaissance. This ensures that asset data can be used effectively for a range of use cases while making it hard for potential attackers to find useful information.
- **Registration before use**. Asset information should be collected before, or at the time of, first use. This may be enforced through process and detection capabilities. For example, certificate identities should only be issued for registered assets, preventing unregistered devices from authenticating to other systems. This reduces the risk of shadow IT being created by making it hard for unregistered assets to enter and persist in your environment.
- **Asset classification**. Consider defining and using categories to classify assets. This should be aligned with your risk management approach. For

example, classifying systems based on the sensitivity of information they process, or whether they support critical business functions. This can help identify relevant security controls for each asset and monitoring for compliance with security policies.

Data sources

The data needed by an asset management system with a cyber security focus can come from a number of sources. The information you need may not necessary come from a typical asset management tool - it could be the output of a procedure. Note also, that one tool may be able to provide more then one data source.

Active and passive data sources

A combination of active and passive data sources should be considered, to ensure comprehensive visibility across your environment.

You should use active scanning techniques where safe and appropriate. Where active scanning is an issue, use passive scanning tools. Active sources such as host-based agents and network scanning can generate deep insights into assets. However, active sources may be limited in their ability to detect new assets, or they may not be suitable for some environments, such as OT networks, due to network limitations or potential device instability.

Passive data sources can provide additional visibility by looking for side effects instead of interrogating assets directly. This could include network sources (DNS and DHCP logs or traffic captures) or application access and authentication logs, which may identify devices attempting to communicate with other systems. These sources will not generate as much detail as active sources, but can be used to validate existing asset data, or detect changes to the environment.

Example data sources

Some example data sources include:

- **Procurement records**. Knowing what has been purchased gives you a source to cross reference with your asset management database. This may not identify assets obtained freely, or through non-standard procurement routes. Free cloud services are a particular example where data could be stored with little oversight.
- **Mobile device manager or system/device management tools**. A number of system configuration or mobile device managers capture information that would be needed by an asset management system. However, these systems may only capture information for general purpose IT and may not support legacy IT.
- **Logging and monitoring platforms**. These can be used to validate a configuration database or detect new or updated assets, including the use of cloud services. This may include sources such as host or network logs (switches, DHCP, DNS, proxy, etc). A logging and monitoring platform can be used as part of the continuous discovery phase.
- **Vulnerability management platforms**. Like a monitoring and logging tool, this could either be used as part of your continuous discovery, or for validating a 'single source' of configuration management information. This type of platform could also add richer information, such as operating system and patch level.
- **Manual entry**. Sometimes, tools and automation are not suitable or are impractical. For example, when you only have a handful of assets to manage, or for unusual assets. Manual entries for these cases should still be kept up to date through regular review.
- **Information from development and engineering teams**. People that design, build and maintain systems will have the most in-depth knowledge of the ground truth. Documents like architecture diagrams or design patterns can help you understand the types of assets to expect with in a system.
- **Public key infrastructure**. Audit records could be used to identify users and systems that have been issued certificates, from both internal and public certificate authorities. This can be used to determine associated roles based on the types of certificates issued. For example, network infrastructure devices should not have the same type of certificate as a public web server.

Validating the Asset Management system

How do you know there's something you don't know? Validating your asset management process can provide confidence that you are not inadvertently overlooking any assets.

You should consider a range of scenarios, including whether assets could be added or changed without being detected. For example, if a user connects a new laptop to your network, would you have the ability to detect this device and its configuration? Or, if a new piece of software was installed on a device, would it be checked for vulnerabilities?

There are a range of ways you can help validate your asset management process:

- **Consider the identification, addition and modification of devices within the scope of penetration tests**. This may identify gaps or weaknesses in your asset management process for both internal and public facing assets.
- **Look for anomalies in log data, such as network traffic from unidentified devices**. This may indicate the presence of unmanaged devices.
- **Identify stale asset records**. These may indicate a device that hasn't been updated, or has been repurposed.
- **Reconcile procurement records and cloud billing with asset records**. Look for assets that have been purchased, but not captured by the asset management process.

PUBLISHED

28 May 2021

REVIEWED

28 May 2021

VERSION

1.0

WRITTEN FOR

Small & medium sized organisations

Public sector

Large organisations

Cyber security professionals