MyRISK HyperGRC

ORACLE | Partner

Continuous Control Monitoring Implementation Series

# #3 - CCM for Asset Management

## White Paper

Presented by David Vohradsky
CEO and Founder

### Introduction

Asset Management is the bedrock of any cybersecurity program. Without knowing what hardware, software, and data assets exist and where they reside, an organisation cannot effectively protect or monitor anything else. For this reason, our journey into domain-specific Continuous Controls Monitoring begins with assets. Part 3 of the series details how to implement CCM for Asset Management. We will examine how to maintain a continuously updated inventory of assets (including cloud and on-premises), how to monitor the asset lifecycle (from acquisition to disposal) for control compliance, and how this continuous asset awareness ties into compliance frameworks like ISO 27001, ASD Essential 8, and others. By the end of this part, you should have a clear strategy for ensuring that at any given moment, you have an accurate picture of your environment – a fundamental prerequisite to all other continuous controls.

### 1. Continuous Asset Inventory – "Always On" Asset Discovery

Traditional approach: Asset inventories were maintained manually or updated infrequently, leading to drift. Continuous approach: Implement systems to discover and catalog assets in real-time or near-real-time. Here's how:

- **Network and Endpoint Discovery:** Deploy automated discovery tools that regularly scan the network for connected devices (using protocols like ARP, SNMP, Nmap scans, etc.). Complement this with agents on known endpoints that report their presence. For example, an organisation might use an endpoint management solution (Microsoft Endpoint Manager, Tanium, etc.) to ensure every workstation and server checks in daily. If a device hasn't checked in within a threshold, it's flagged as missing (which might indicate it's been removed or turned off – further investigation needed). Conversely, if a new device appears on the network that's not in the inventory, that triggers an alert. This fulfills control objectives such as ASD Essential 8's first step (inventory management) and CIS Control 1. In fact, CIS Control 1 (Inventory of Devices) explicitly states to use active discovery tools to identify assets connected to the network.

- **Cloud Asset Discovery:** Use cloud provider APIs and services to list resources. Cloud providers often provide inventory services (e.g., AWS Config, Azure Resource Graph, Google Cloud Asset Inventory) that can be polled or even set to push updates. A good practice is to enable cloud asset change notifications – for instance, AWS CloudTrail coupled with AWS Config can generate an event whenever someone creates a new EC2 instance or S3 bucket. Your CCM can capture that event and verify that the new asset is accounted for (e.g., tagged properly, added to CMDB). If your organisation uses multiple cloud accounts or providers, consider a multi-cloud inventory aggregator (there are open-source and commercial CMP tools that unify this view). Continuous inventory is crucial for cloud compliance – misconfigurations often come from resources that were created outside the normal process.

- **Reconciling with CMDB:** Many enterprises maintain a formal CMDB or asset registry. The continuous discovery tools should feed into this registry automatically. A reconciliation job can run daily comparing discovered assets with CMDB records. Items found with no corresponding record can either be auto-added with a temporary status or flagged for someone to investigate and formally register. Items in CMDB that are not seen for X days could be candidates for removal if decommissioned (or might indicate an asset that is powered off or not currently reachable – which might be okay, but should be verified). The goal is a virtuous cycle: discovery finds stuff -> updates inventory -> inventory informs security controls.

- **Endpoint User Reporting:** Some organisations also crowdsource asset discovery by requiring users to log/label new devices. For example, if someone wants to plug in a new server, policy might require they inform IT. While not as reliable as technical controls, continuous monitoring can even check sources like Active Directory (for new computer objects) or DHCP server leases to catch devices early. The combination of sources (network, cloud, directory, etc.) ensures thorough coverage.

## 2. Monitoring Asset Lifecycle and Changes

Continuous asset management isn't only about initial discovery – it's about tracking changes to assets through their life and ensuring controls keep up:

- **New Assets:** When a new asset comes online, CCM should verify it meets baseline requirements. For example, is it immediately put under vulnerability scanning? Does it have the standard security agents (AV, vulnerability, monitoring) installed? A continuous control could be: "All new servers must have endpoint protection installed within 1 hour of creation." If your deployment process is automated, you can actually enforce that (through configuration management tools or cloud-init scripts). The CCM system can have a timer – if a new server appears and after an hour it's not reporting to the AV console, trigger an alert. This addresses the gap where sometimes new systems are spun up and security configurations lag (especially problematic in dynamic cloud environments). Many breaches start with a test system that was spun up without the usual hardening.

- **Moved/Repurposed Assets:** If an asset's role or location changes, ensure documentation and controls change accordingly. For instance, if a server moves from a test environment to production, it should inherit production security monitoring. Continuous monitoring might catch this by noticing its network segment changed or tags changed, and then verifying if all production controls (like more frequent vulnerability scans or inclusion in SIEM logs) now cover it. If not, it's a gap to fix.

- **Decommissioned Assets:** Orphaned assets lingering are a risk (e.g., an old VM left running unpatched). Continuous monitoring of assets can identify assets with no logins or activity for a long period, indicating they might not be in active use. At the same time, if an asset is marked as decommissioned in CMDB but still responding on the network, that's a serious discrepancy – perhaps someone forgot to actually turn it off, or the record-keeping was premature. Either way, CCM surfaces it. Ideally, you integrate asset decommission into the continuous process: when an asset is slated for removal, a checklist (wiping data, removing from monitoring, updating inventory) is executed, and CCM confirms the asset truly disappears from the environment after. Until it's gone, it might remain on a "watch list" of supposed-to-be-gone items.

- **Configuration Drift of Assets:** (Note: This overlaps with secure configuration management in Part 5, but at a high level, asset monitoring also means monitoring asset attributes over time.) An asset that was compliant yesterday might not be today if changes occurred. E.g., a server could be taken off the domain (removing it from certain controls) – that should be caught. Or encryption turned off on a laptop – continuous endpoint management alerts can catch that event. Essentially, any change in state that violates policy should trigger alarms.

A great example of lifecycle monitoring: Many organisations adopt the practice of "asset birth certificates" and "death certificates." When an asset is created, a birth record is logged with its baseline security posture. When it's decommissioned, a death record confirms removal. CCM ensures no asset exists without a birth record (catching shadow IT) and no asset "ghosts" after a death record. This concept keeps asset inventory auditable.

## 3. Monitoring Software Assets and Licenses (Continuous SAM)

Asset management isn't just physical devices – it includes software (Software Asset Management - SAM). CCM can extend to:

- **Licensed Software Tracking**: Continuously track installations of software to ensure you stay compliant with licenses and also to detect unauthorised or risky software. If a prohibited software (say, torrent client) appears on a company device, continuous monitoring should flag it within a day, not wait for a manual audit. This improves security (unapproved software often bypasses security controls).

- **Version Monitoring**: For major applications, you might continuously record versions installed and flag if any asset is running a very outdated version that is not allowed (which segues into vulnerability management, but from an asset lens, it's about what's installed where).

- **Open Ports/Services:** Knowing what services (by port or application) each asset runs is part of inventory. Continuous port scanning or agent data can feed this. For example, an inventory entry for a server might list "IIS web server running". If tomorrow it suddenly is also running an SQL service on a new port, CCM would catch that addition. It could be benign (admin installed something) or malicious (a backdoor opened a port).

All these aspects tie to frameworks: ISO 27001's asset management section expects not just hardware but also software to be tracked. Essential 8's Application Control essentially demands knowing what software is allowed and ensuring only that runs – continuous monitoring of software inventory supports that at scale.

## 4. Compliance and Reporting Benefits

By implementing continuous asset monitoring:

- During audits, you can provide evidence like "Here's our up-to-date asset list, and here are the automated discovery logs and discrepancy reports for the last 12 months." Auditors can sample and see that every time a new server was added, it was captured. This level of rigour can satisfy ISO 27001 control A.8.1 (inventory) fully, and also various IT audit requirements (many audit frameworks start by checking if inventory is accurate).

- Many regulations (like SOCI Act rules or APRA standards) might not explicitly say "thou shalt do continuous asset scanning," but they require effective risk management. Having this in place shows proactive risk management. Regulators tend to view unknown assets as a governance failure. In fact, APRA CPS 234 indirectly hints that asset changes and emerging vulnerabilities must be addressed promptly; without continuous asset awareness, that's impossible.

Reporting metrics might include: - Total number of assets (trended over time). - Assets added/removed in the last month (with verification that each addition/removal followed procedure). - % of assets with complete attribute information (owner, classification, etc.). - Timeliness metrics: e.g., median time from asset discovery to CMDB entry. These can be reported to management as part of security KPI. It demonstrates maturity in security operations.

## 5. Tools Spotlight

- **ServiceNow CMDB with Discovery:** Many organisations use ServiceNow's discovery module to continuously scan subnets and update the CMDB. When properly tuned, it's powerful for CCM.
- **Tanium or Similar Platforms**: Tanium in particular gives near-real-time visibility of all endpoints (it's often used by Australian government agencies for Essential 8 compliance). It can show all assets online and their state in seconds. That's very useful for CCM asset management and for feeding other control checks.
- **Open-Source Tools:** If budget is a concern, open-source network scanners (like OpenVAS, Masscan) can be scheduled frequently. For software inventory, tools like OSQuery (Facebook's tool) can continuously gather and report system info. Combining these with a scripting and dashboard layer can form a DIY continuous asset monitor.
- **Cloud-native:** For AWS, enabling AWS Config with rules that every resource must be tagged, and setting Amazon GuardDuty (which can detect unknown instances doing unusual things), helps cover asset detection and security in one go. Azure and GCP have analogous services.
- **MyRISK HyperGRC Platform:** MyRISK HyperGRC integrates seamlessly with leading asset discovery tools (e.g., Tanium, ServiceNow, AWS Config) via its workflow automation engine to ingest asset data into its unified control monitoring framework. AI agents within MyRISK can continuously assess asset telemetry against control baselines (e.g., Essential 8, NIST CSF) to detect anomalies, misconfigurations, or missing assets. MyRISK workflows can automatically trigger alerts, initiate investigation tasks, or escalate exceptions for review - ensuring timely remediation and audit readiness. This enables organisations to shift from static asset inventories to dynamic, intelligent, and auditable asset control monitoring.

## 6. Challenges and How to Manage Them

- **Handling Dynamic Environments:** In very dynamic or large environments, continuous scans might produce a lot of "churn" (assets appearing and disappearing). It's important to distinguish meaningful assets from ephemeral ones. One approach is to enforce tagging or naming conventions that indicate ephemeral resources; CCM can then ignore or separately track those to avoid alert fatigue.
- **Accuracy vs. Performance:** Scanning too frequently can strain networks or systems. Use incremental scanning where possible (only scan IP ranges where something changed, etc.). Cloud APIs are efficient but have rate limits – be mindful not to overload those either. A hybrid approach (real-time events + periodic full reconciliations) is effective.
- **Integration Overload**: Getting all data sources to talk to each other (e.g., network scans into CMDB, cloud into CMDB, etc.) can be complex. It might require scripting or middleware. Dedicate time in the program design to data integration efforts, possibly using a central database to collate and compare before updating official records.
- **False Positives**: Discovery might identify devices that are actually authorised but were not labeled properly, causing "false alarms" of unknown assets. The cure is improving the process so that new assets are properly registered (so the system doesn't falsely flag them). Over time, as people see CCM catches every forgotten registration, they'll be more diligent in updating the CMDB beforehand – a cultural shift that CCM incentivizes.

## Conclusion

Continuous monitoring for asset management ensures you maintain constant visibility into what your organisation owns and operates. This visibility is foundational for all subsequent security monitoring and controls. By having a living inventory that updates itself and alerts on anomalies, you reduce the likelihood of "unknown unknowns" – those forgotten servers or devices that attackers love to exploit. Moreover, you create an auditable trail that your asset governance is robust, satisfying auditors and regulators.

With your assets in check, you are ready to tackle continuous monitoring in more focused control areas.