THE SOC'S BIGGEST PAIN: ASSET INVENTORY

CREST

SOC

Introduction

Today, Security Information and Event Management (SIEM) platforms and Security Operations Centers (SOC) are at the forefront of cybersecurity, tasked with continuously monitoring, detecting and responding to cyber threats.

Amid a wide range of challenges encountered by these entities, one obstacle persistently stands out: the effective management of asset inventory.

The importance of a comprehensive, up-to-date asset inventory might not be immediately apparent to all your stakeholders. Some may perceive it as a concern secondary to the core functions of a SOC, possibly relegating it to the realm of IT asset management.

But this underestimation misses the critical role that asset inventory plays in the cybersecurity ecosystem – and raises a pertinent question: If asset inventory management is not directly linked to the day-to-day operations of a SOC, why does it demand significant attention, strategy and resources?

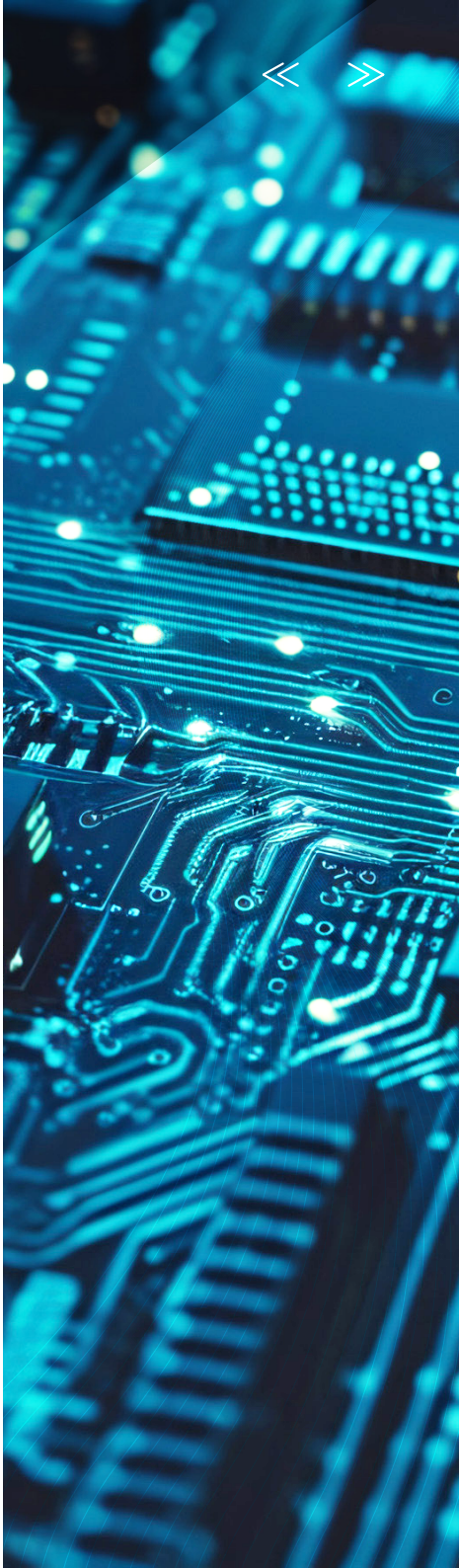
Asset inventory management actually forms the cornerstone of effective cybersecurity measures. It entails the detailed cataloguing and ongoing monitoring of an organisation's physical and digital assets, including hardware, software and network resources.

This foundational task is crucial for several reasons: it enables vulnerability management, informs risk assessments and guides deployment of protective measures tailored to the unique risk profiles of different assets.

Without a clear and comprehensive asset inventory, security teams are essentially navigating in the dark, unable to protect against or even recognise threats targeting unaccounted for - or improperly classified - assets.

The ongoing challenge of managing asset inventory highlights a fundamental truth in cybersecurity: knowledge is power. A detailed inventory of assets is not merely an administrative record; it is a strategic asset in its own right.

Without it, SOCs face significant handicaps with their capacity to monitor for threats, detect vulnerabilities and respond to incidents critically undermined.



Visability

Any SOC's effectiveness is intrinsically intertwined with the scope and quality of its monitoring capabilities.

That effectiveness largely depends on what it monitors, including the number and types of devices from which it collects logs, along with the sophistication of the correlation searches or rules applied to those logs.

SIEM platforms play a crucial role here by aggregating, analysing and correlating data from various sources to identify potential security incidents.

Usually, we find that the scope of monitoring starts small and expands over time. This incremental approach allows a SOC to scale its monitoring capabilities as it grows in maturity - and as the organisation's infrastructure evolves. Starting small also helps in fine-tuning the monitoring process and correlation rules to ensure efficiency and effectiveness before scaling up.

If we take a list of servers from the Configuration Management Database (CMDB), configure them for monitoring, and then add this configuration to the base images of the servers, so they automatically ("automagically") log to the SIEM, in theory we have 100% server coverage, and everyone is happy.

By integrating the SOC's monitoring setup with the CMDB, organisations ensure both existing and new servers are automatically configured to log their activities to the SIEM system.

This automation is crucial for maintaining continuous monitoring coverage without manual intervention, every time a new server is added to the network.

The objective is to achieve 100% server coverage, meaning every server in the organisation's infrastructure is monitored by the SIEM system. Achieving this goal is significant, as it ensures there are no blind spots in the monitoring coverage, thereby enhancing the SOC's ability to detect and respond to incidents across the entire infrastructure.

If we agree that complete monitoring coverage is a critical metric of success for a SOC, ensuring and enhancing its ability to detect, investigate and respond to potential security threats effectively, then we must underscore the importance of SIEM platforms and integration with CMDBs.

Security Alert!

Now, let's assume your SOC has complete coverage of servers, to the best of your knowledge, and we start seeing alerts. You may have some trick correlation rules[1], but also the basic hygiene ones[2] that make sure everyone plays by your security policies.

Then something out of the ordinary happens. You get an alert for the use of high privilege accounts (administrator or root) on a server that doesn't meet your naming convention and isn't in the CMDB. Obviously, this situation raises immediate concerns because any activity involving high-privilege accounts warrants scrutiny, and the lack of visibility into the server complicates the SOC's response.

After some hours of digging around, you discover it's an unofficial test server. This is yet another SOC Groundhog Day.

The point here is to highlight the repetitive and time-consuming nature of investigating alerts, especially those that turn out to be false alarms or related to undocumented assets. Such incidents consume valuable time and resources, detracting from the SOC's ability to focus on genuine threats.

Three takeaways here:

The Importance of Asset Management:

Accurate and comprehensive asset inventory is crucial for effective security monitoring. Undocumented assets pose significant challenges in incident response and risk management.

The Cost of False Positives and Unaccounted Assets:

Investigating alerts, especially those involving assets not in the CMDB, are a significant time sink, diverting resources from more critical security concerns.

The Need for Policy and Process Improvement:

Incidents such as the above highlight the need for better processes around asset registration and compliance, as well as the importance of maintaining an up-to-date CMDB.

[1] Advanced, sophisticated rules designed to detect complex patterns of behaviour or specific sequences of events that may indicate a security threat. Such rules go beyond basic threshold or single-event alerting to provide more nuanced detection capabilities, often involving multiple data sources, contextual analysis and temporal relationships. These rules might include the likes of sequential failed security controls or rare process execution, for example.

[2] Basic hygiene correlation rules are essential for maintaining a secure and compliant IT environment, forming the foundation of a strong security posture by addressing common vulnerabilities and enforcing good security practices. Such rules might include the likes of multiple login failures, unpatched vulnerabilities, excessive permissions or policy violations.

LEVEL UP - Add EDR & Cloud

As organisations mature, they face ever-evolving complexity and greater challenges in managing IT assets and security.

To face these challenges, you'll probably adopt more advanced technologies like Endpoint Detection and Response (EDR)[3] systems and cloud computing.

These technologies offer advanced capabilities but also introduce new challenges.

Many modern EDR systems include the ability to discover devices on the network that may not have been previously accounted for. This can reveal devices that are not in the CMDB and, critically, such devices may not be patched or secured, posing potential security risks. But discovery of these devices can be positively framed - because it brings unknown assets to light, allowing for their management and protection.

Now, you might add the flexibility the organisation and application managers want, via self-managed cloud subscriptions. You can simply spin up servers as you need them, without waiting for traditional IT provisioning processes.

While this approach offers agility and flexibility, it often lacks the disciplined management and security practices that IT departments typically enforce.

The decentralisation of IT management, especially with self-managed cloud resources, creates further significant challenges in maintaining visibility over the IT environment.

These challenges are exacerbated by discrepancies in how assets are identified (for example, instance names in the CMDB vs. hostnames used by security tools) and the lack of enforced tagging policies in cloud environments.

Proper tagging is crucial for managing resources effectively, especially in large cloud environments, as it helps in categorising and applying appropriate security measures based on the criticality and function of the asset.

A lack of enforced tagging and discrepancies between CMDB records and security tools' data can lead to critical information gaps. For instance, without proper tags, it becomes difficult to identify the environment (Production, QA, etc.) a resource belongs to, or the appropriate support group for escalation in case of security incidents. This situation complicates incident response and risk management efforts.

Adopting advanced IT and security technologies is something of a double-edged sword. While these technologies provide enhanced capabilities for detection and flexibility, they also introduce challenges in asset management, visibility and compliance.

Organisations must carefully navigate these challenges, ensuring technology adoption benefits do not come at the cost of weakened security posture and increased operational risks. The increased usage of cloud comes with the benefit of additional capabilities for Attack Surface Management that provide the SOC with enhanced information about risks and threats for the infrastructure, along with a complete inventory to compliment those of traditional CMDBs.

[3] Endpoint Detection and Response (EDR) technology provides continuous monitoring and collection of data from endpoints - devices that connect to your network, such as laptops, desktops, and servers. EDR solutions are designed to detect, investigate, and respond to potential security threats at the endpoint level in real-time.

Conclusion

You can create an effective SOC with good monitoring and security processes, but if the CMDB is flawed through poor coverage and insufficient data, then the SOC's visibility and ability to effectively respond is reduced.

A well-maintained CMDB ensures the SOC team has comprehensive visibility over all assets within the organisation's network. This visibility is essential for effective monitoring, allowing the SOC to accurately identify which assets may be affected by a security threat and to prioritise response based on the criticality of those assets.

Conversely, if the CMDB has poor coverage (such as missing information on some assets) or contains inaccurate or outdated information, the SOC's ability to effectively monitor the environment and respond to incidents is significantly compromised. This can lead to delays in detecting threats or even complete oversight of certain attacks, increasing the organisation's vulnerability.

While CMDB maintenance typically falls outside the direct responsibilities of the security team (it is often managed by IT operations), its quality directly impacts organisational security posture.

Organisations must evaluate the quality of their CMDB as a fundamental aspect of a good security posture. This is crucial because a comprehensive and accurate CMDB is foundational for effective threat detection and response strategies.

Since the CMDB provides the SOC with the necessary context for detecting and responding to threats, its integrity and completeness are essential for maintaining a robust security posture. Without a reliable CMDB, even the most sophisticated SOC operations can be hindered.

In summary, while the CMDB's maintenance may not directly fall under the security team's purview, its quality significantly influences the SOC's effectiveness. Ensuring your CMDB is comprehensive and accurate is therefore essential for helping your SOC properly protect, detect and respond to threats.


CREST