noetic

# The Noetic Continuous Cyber Asset Management and Controls Platform

Improve. Continuously

noetic

# Market Challenge

## The Asset Management problem – protecting unknown devices.

Security teams have a problem in identifying all the assets in the business and the security risk that they represent. Organizations now have millions of different assets, not just traditional compute devices but also networks, virtual machines, containers, mobile devices, code repositories, personal data, and people. In recent guidance on establishing an asset management program, the UK's National Cyber Security Centre defined an asset as '*anything that can be used to produce value for your organization.'*[1]

Security teams have struggled to create and run effective cybersecurity asset management programs for many reasons, and these include:

- **Ownership**. Traditionally, IT Asset Management (ITAM) has been the domain of the IT organization, but the information they collect and maintain is not optimized or suitable for cybersecurity use cases.
- **Technology innovation and adoption**. The way we buy and deploy technology has changed. With the growth of cloud services and SaaS applications, traditional IT procurement processes can be bypassed. This has led to the growth of 'Shadow IT' outside of regular security controls**.**
- **Complex digital infrastructure**. There are many IT management and security tools that have a partial view of assets, but only from their own perspective and domain expertise. This fragmentation of IT management, DevOps and security tools means that, although the relevant insights are potentially available, this data is siloed and difficult to extract.

This growing technology sprawl across cloud services, virtual machines, and SaaS applications, together with the huge volume in the number of managed and unmanaged assets in an organization, also means that many of these assets are 'ephemeral' in nature. They might only be available for a short amount of time, but can still represent security risk to the business, depending on the access they have and the data they link to. All these factors have created the need for a new kind of cybersecurity asset management. In a recent report, Gartner has defined this as Cyber Asset Attack Surface Management (CAASM), stating that "*CAASM is an emerging technology focused on enabling security teams to solve persistent asset visibility and vulnerability challenges. It enables organizations to see all assets (both internal and external) through API integrations with existing tools, query against the consolidated data, identify the scope of vulnerabilities and gaps in security controls, and remediate issues."*[2]

---

[1] NCSC, Implementing asset management for good cyber security, May 2021

[2] Gartner, Hype Cycle for Security Operations, July 2021

# The Noetic Solution

The Noetic solution is a cloud-based cyber asset management and controls platform that provides teams with unified visibility and security insights into all assets across their cloud and on-premises systems, and delivers continuous, automated remediation to close coverage gaps and enforce security policy.

By building a map of the cyber relationship between all assets in the organization, Noetic delivers:

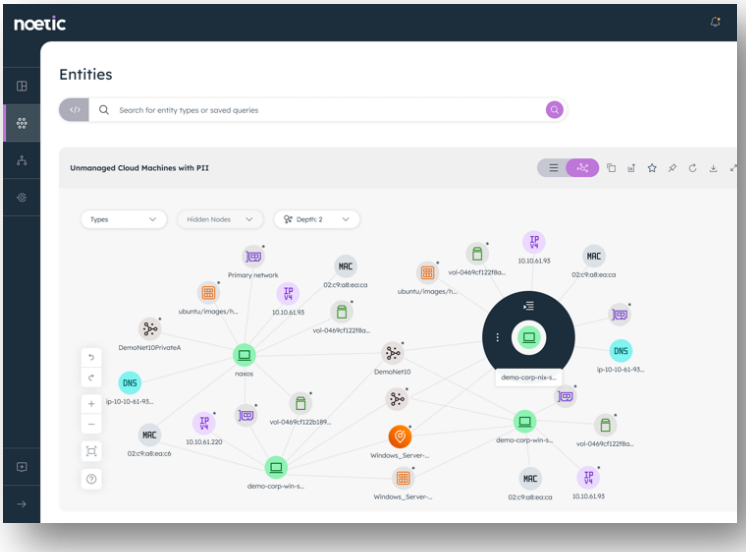
- **Unparalleled Visibility:** Noetic breaks down the silos of existing security tools with pre-built agent-less connectors, creating a unified view across cloud and on-premises of all assets and their current state, highlighting coverage gaps and policy violations.
- **Real-time Insights:** By understanding the cyber relationship between all assets across the enterprise, Noetic's dashboards provide immediate operational insights and gives security teams with an uptodate understanding of the state of their network now.
- **Continuous Security Posture Improvement**: With Noetic, teams can create and schedule powerful queries that identify policy and configuration drift. By running continuous queries, teams can not only identify this drift, but can remediate changes through the automation workflow engine, restoring assets to an approved state, in line with internal security policies.

Key capabilities of the Noetic platform include:

## Operational Visibility

Noetic provides unprecedented visibility into all assets in the organization and the cyber relationships between them. Noetic leverages existing IT and security investments with agentless, API-based connectors to mine them for all assets and entities of interest, building out a graph of the entire cyber estate.

Through continuous discovery, correlation and enrichment of these assets, Noetic helps teams identify common security gaps, such as cloud misconfiguration, shadow IT deployments outside of endpoint security coverage and vulnerability scanning processes

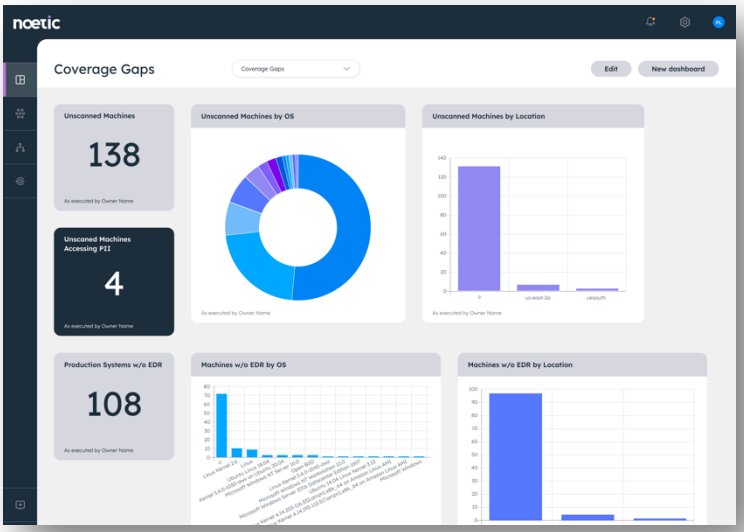


noetic

# Continuous Controls Monitoring (CCM)

Noetic provides automated assessment and evidence collection on internal and external control effectiveness and compliance status.

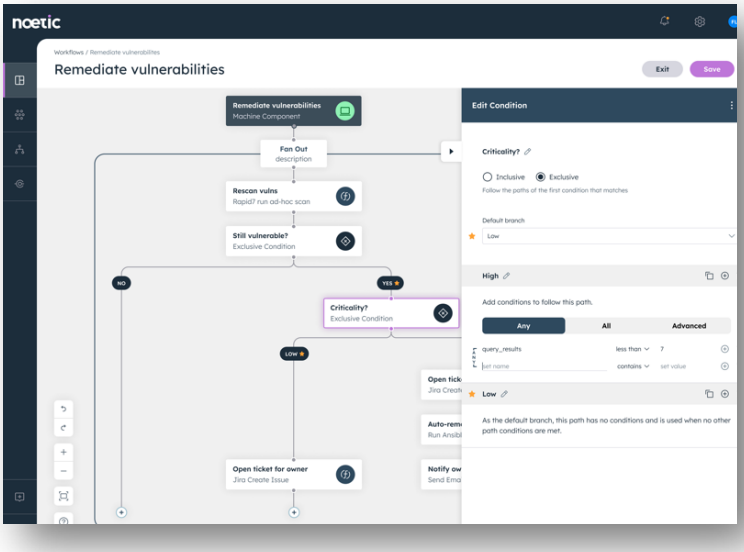
As teams build out internal security policies or need to track compliance with external security controls and policies, they can build out recurring queries to track their status, report to different stakeholders with rich, customizable dashboards and use automated workflows to ensure that new and non-compliant assets are returned to an approved state.




# Automation at the Core

Noetic is built to deliver security outcomes, not just insights and dashboards. At the heart of the Noetic platform is a rich Automation workflow engine that enables security teams to build out enrichment and remediation processes using a simple drag & drop visual editor to create comprehensive and precise workflows.

Security automation requires confidence. By leveraging the high-fidelity, correlated data delivered in the Noetic graph, teams can build repeatable processes to reduce manual workload. Find a problem once, fix it continuously.




Noetic Cyber enables security teams to make faster, more accurate decisions to detect coverage gaps and reduce cyber risk. Noetic is based in Boston and London. For more information, visit www.noeticcyber.com, or follow us on LinkedIn or Twitter.

You can request a demo of the Noetic platform here.