noetic

Cyber Asset Attack Surface Management (CAASM) Solutions for Energy Companies

THE CHALLENGE

Due to its complex nature and importance to our society, securing the world's critical infrastructure is one of the biggest and most challenging responsibilities for the security community. Gartner® estimates that by 2025, 30% of critical infrastructure organizations will experience a breach resulting in the halting of a mission-critical system.

The energy sector worldwide is at the center of a digital transformation, shifting from legacy technology to internet-connected smart grid infrastructure, supporting solar parks, wind farms and smart meters. This also creates an expanded attack surface to manage and protect.

Energy companies are also experiencing changing geopolitical trends. The need to secure critical infrastructure from nation state actors as well as highly motivated ransomware gangs is clear. Recent, well-publicized incidents, such as the Colonial Pipeline ransomware attack, the 3CX breach of US energy companies as well as the compromise of the Ukrainian power grid in 2015 each highlight the different critical challenges that security teams face in safeguarding energy systems.

MAJOR CHALLENGES THAT SECURITY LEADERS IN THE ENERGY SECTOR MUST ADDRESS INCLUDE:

- Attack surface sprawl across the organization: The need to track software and hardware vulnerabilities, shadow IT and other potential exposures across complex IT and OT environments.
- Growing regulatory pressure: Government and industry regulators worldwide are introducing new cyber requirements for critical infrastructure with specific technical reporting requirements.
- Complex supply chain dynamics: Third-party suppliers are now a common attack vector for energy companies. Security teams need to understand and manage the potential exposure created by partners and customers.

SIMPLIFY COMPLIANCE WITH NOETIC.

NIST CYBERSECURITY FRAMEWORK (CSF)

Currently updating to 2.0 and is required for US energy companies. A comprehensive framework that includes need for asset discovery & management across IT & OT estates.

NERC CRITICAL INFRASTRUCTURE PROTECTION (CIP)

Ensures consistent security controls such as identifying & managing critical assets.

DHS TSA SECURITY DIRECTIVE 2

Requires pipeline operators to report cyber incidents and have a clear plan to identify and remediate vulnerabilities.

EU NETWORK & INFORMATION SYSTEMS DIRECTIVE (NIS2)

Europe-wide reporting & oversight requirements including critical assets and vulnerabilities.

SOLUTION BENEFITS

- Maintain 360-Degree Visibility
- Simplify Compliance Reporting
- Experience Immediate Time to Value
- Risk-Based Vulnerability Prioritization

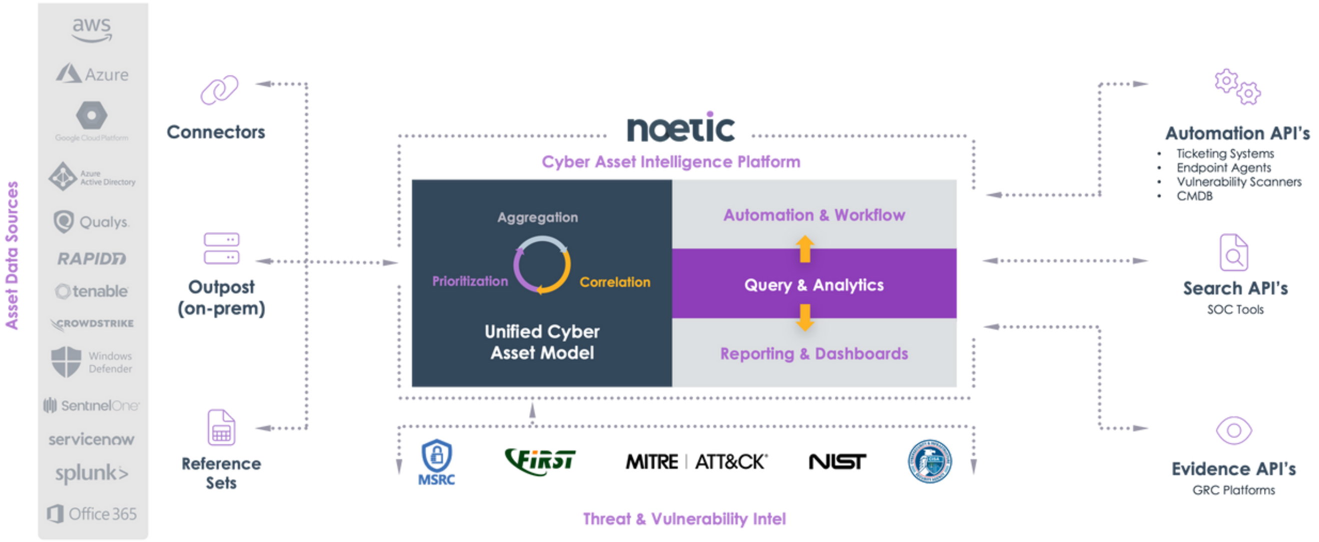
© NOETIC CYBER 2023

THE NOETIC SOLUTION

Powering Cyber Resilience for Energy Providers

Noetic's market-leading, innovative Cyber Asset Attack Surface Management (CAASM) solution helps security leaders manage their attack surface and reduce cyber risk by giving teams the visibility they need into critical assets, high-risk vulnerabilities and other potential exposures that could cause costly security incidents.

By leveraging data from existing security, IT management and networking tools, Noetic builds a multi-dimensional map of all assets in the organization, across the cloud and on-premises, to highlight their current security posture and how they are connected. Our no-code automation & workflow engine allows security teams to create simple automated processes to streamline enrichment and remediation.



KEY BENEFITS FOR SECURITY, RISK AND COMPLIANCE LEADERS

- **360° VISIBILITY**
  Noetic ingests and correlates data from existing tools, data sets, and third parties to provide a cohesive, contextual view of your entire attack surface from both the IT and OT environments.

- **IMMEDIATE TIME TO VALUE**
  Noetic's agent-less connectors work with deployed tools to use existing security data. Out-of-the-box dashboards and reporting for common use cases mean that customers gain critical insights quickly.

- **RISK-BASED VULNERABILITY PRIORITIZATION**
  Noetic enables teams to focus their vulnerability remediation efforts where they matter most by highlighting critical areas of risk based on asset risk & exposure, as well as leveraging vulnerability intelligence data from NIST, CISA, FIRST and more to measure severity and exploitability.

- **SIMPLIFIED COMPLIANCE REPORTING**
  Noetic's continuous controls monitoring automatically monitors your environment for control gaps, validates remediation, and collects evidence to demonstrate compliance with relevant controls.

About Noetic Cyber

Noetic provides a proactive approach to cyber asset and controls management, empowering security teams to see, understand, fix and improve their security posture and control drift. Our goal is to improve security tools and control efficacy by breaking down existing siloes and improving the entire security ecosystem. Founded in 2019, Noetic is based in Boston and London.

noetic

noeticcyber.com
hello@noeticcyber.com

© NOETIC CYBER 2023