noetic

From Risk to Returns

Noetic Cyber Asset and Exposure Management

By Brad LaPorte

Table of Contents

Overview

ABOUT BRAD LAPORTE

Brad LaPorte is an Advisor at Lionfish Tech Advisors and Partner at High Tide Advisors—providing go-to-market consulting and advisory services to investment firms and cybersecurity startups.

Brad is a former top-rated Gartner Research Analyst for cybersecurity, veteran U.S. Cyber Intelligence, and product leader at Dell, IBM, as well as several other startups. He is credited with creating the first-ever Managed Detection and Response (MDR) service in 2014 and creating the Attack Surface Management category at Gartner in 2019. He has spent most of his career on the frontlines fighting cyber criminals and advising top C-level executives as well as other thought leaders on how to be as efficient and effective as possible.

He is a noted keynote speaker and strategic advisor for several leading cybersecurity solution providers. He has his MBA from Ithaca College and holds several industry leading professional certifications in cybersecurity and information technology. Brad's passion in life is to help others no matter what the challenge.

Executive Summary

In today's landscape of digital-first strategies, the role of IT and security teams has evolved into critical strategic pillars rather than mere support functions. But as the spotlight shines brighter, these teams continue to face multifaceted challenges in comprehending and securing their cyber estates.

From the complex nuances of shadow IT to the intricacies of dynamic cloud infrastructures, today's attack surfaces extend far beyond the scope of conventional threat and vulnerability management (TVM) programs. Most conventional strategies focus solely on infrastructure and software vulnerabilities, leaving the 'nontraditional', 'unpatchable' attack surface exposed.

According to the Gartner® Implement a Continuous Threat Exposure Management (CTEM) program report, "Enterprises fail at reducing their exposure to threats through self-assessment of risks because of unrealistic, siloed and tool-centric approaches."

"A forward-looking defense strategy requires modernization of the assessment tool portfolio. These tools must not only inventory patchable and unpatchable exposures, but also prioritize findings based on what an attacker could really do."

Gartner®, Top Strategic Technology Trends for 2024

Therefore, while a seemingly endless supply of IT and security tools exist today, they address only fragmented pieces of today's complex attack surface management puzzle.

Rather than continue to invest more in siloed security solutions, progressive security leaders are consequently prioritizing the recording and reporting of potential impact to effectively reduce risk and demonstrate organizational value and establish a resilient security architecture. Today's teams are encouraged to integrate cybersecurity validation techniques into exposure management processes through the evaluation of techniques such as asset visibility and classification, attack path mapping, and cybersecurity control automation.

Visibility is the Foundation of Cyber Asset and Exposure Management

Fortunately, the necessary data to enable such processes already resides within existing tools, systems, and databases. The crux lies then in effectively gathering, correlating, and acting on this information before the adversary can act—the basis for a continuous threat exposure management (CTEM) program.

This is a where the new approach to cybersecurity asset management provided by Noetic Cyber proves to be invaluable. It enables IT and security teams to implement a proactive CTEM strategy through operating from a single, correlated view of their environment—leveraging documented APIs to automate the continuous discovery of new and updated assets and vulnerabilities, and mapping that together with their current security posture and interdependencies.

By implementing the Noetic Cyber Asset and Exposure Management platform, organizations can achieve considerable operational cost savings and potential risk reduction, delivering a significant return on investment (ROI).

This report is designed to explore these benefits, breaking down the efficiency gains into six core security use cases: Business Process Interruptions; Material Breach Risk Mitigation; Security Hygiene and Posture Management' Security Operations and Incident Response; Governance, Risk and Compliance; and IT Operations and Management.

Challenges Addressed

UNDERSTANDING THE NEED FOR CYBERSECURITY ASSET AND EXPOSURE MANAGEMENT

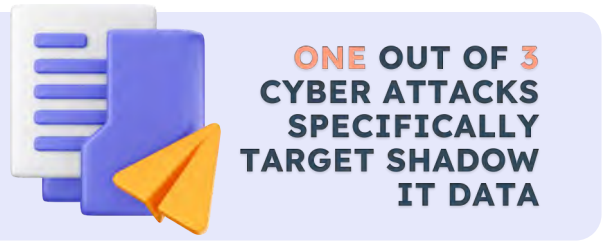
When presenting a business case for cybersecurity asset management, IT and security leaders can emphasize numerous areas that surpass traditional asset management considerations.

To effectively calculate and communicate the potential return, teams should consider:

- **Shadow IT**
- **Impact of a Data Breach**
- **The Human Element**
- **GRC Requirements**
- **Team & Tooling Efficacy**

1. The growing Shadow IT problem

Shadow IT–also called gray IT– refers to assets including SaaS applications that are used within an organization 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. Shadow IT presents a significant risk to the business as it bypasses security controls and best practices.

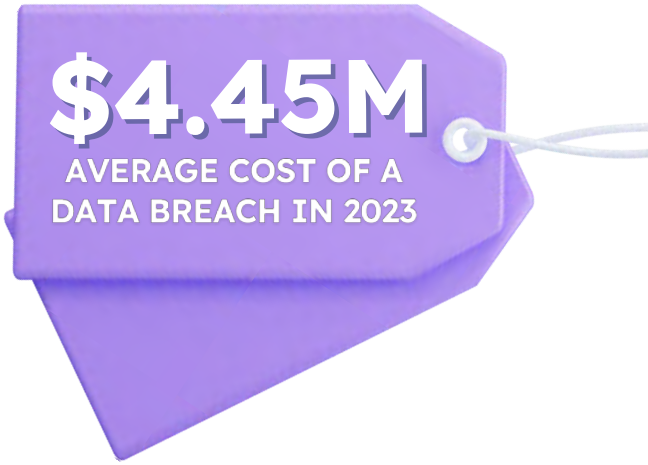


- Shadow IT accounts for a substantial portion of IT spending, ranging from 30-50%. (Gartner).
- SaaS Sprawl is a significant issue, with 59% of professionals struggling to manage SaaS applications, and 65% of these applications being unapproved by IT (BetterCloud).
- One-third of successful cyber attacks specifically target data stored in shadow IT infrastructure (Gartner).

2. The Impact of a Data Breach

Significant data breaches can have a major direct and indirect impact on organizations. They run the risk of regulatory fines, reputational damage resulting in lost business or fall in market value. Indirect costs can include consumer notifications in some markets, as well as considerable organizational disruption.

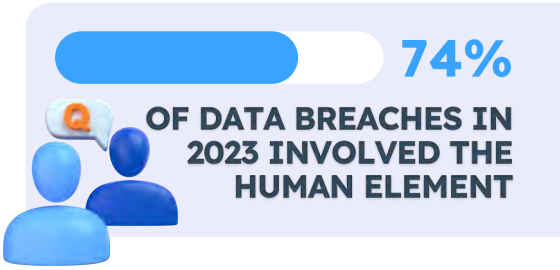
- The average cost of a data breach stands at around $4.45 million.
- 83% of organizations have experienced multiple data breaches, with 45% of these breaches occurring in the cloud. (IBM)



3. The Human Element

Users are often an overlooked component of a Threat & Exposure Management program. Whether through spear phishing, BEC attacks or stolen credentials, the need to help employees securely manage their access to data and critical business applications is a vital part of any cybersecurity program.

- 74% of all reported breaches in 2023 involved human element as either the total or part reason for the breach. (Verizon)
- 83% of IT teams find it impossible to enforce cybersecurity policies, particularly in the context of remote work. (HP)
- 42% of employees use email accounts not approved by IT, while 58% of IT managers also employ unapproved tools for collaboration. (Statista)



4. Stringent Governance, Risk and Compliance (GRC) Requirements

The number of different cyber regulations and frameworks that organizations must comply with due to industry or geography continues to grow. These regulations, such as PCI DSS 4.0, the EU's NIS 2.0, and the revised SEC cybersecurity regulations have become more technically specific and rigorous.

- 74% of organizations agree that compliance is a burden (Drata)
- Most compliance costs come from indirect sources, such as administrative fees. One-third of compliance costs are direct, such as payments to auditors. (GlobalScape)
- 60% of GRC professionals still manage compliance manually with spreadsheets (Coalfire)

5. Security Team & Tooling Efficacy

A lack of visibility into the whole cyber estate creates more work for security teams. Without understanding the whole attack surface, it is impossible to know whether existing solutions are deployed effectively to deliver the best value.

According to the 2023 ESG Security Hygiene and Posture Management report:

- Over half (58%) of organizations lack a centralized approach to security hygiene and posture management.
- 42% of teams take more than 80 hours to complete a comprehensive asset inventory.
- Security and IT tool integration is the top priority for improving security asset management programs.

Addressing these multifaceted challenges requires a proactive and comprehensive approach to cybersecurity asset management. By navigating these complexities, organizations can significantly enhance their cybersecurity posture, mitigate risks, and streamline operations, aligning their security initiatives with evolving digital landscapes for sustained resilience and efficiency.

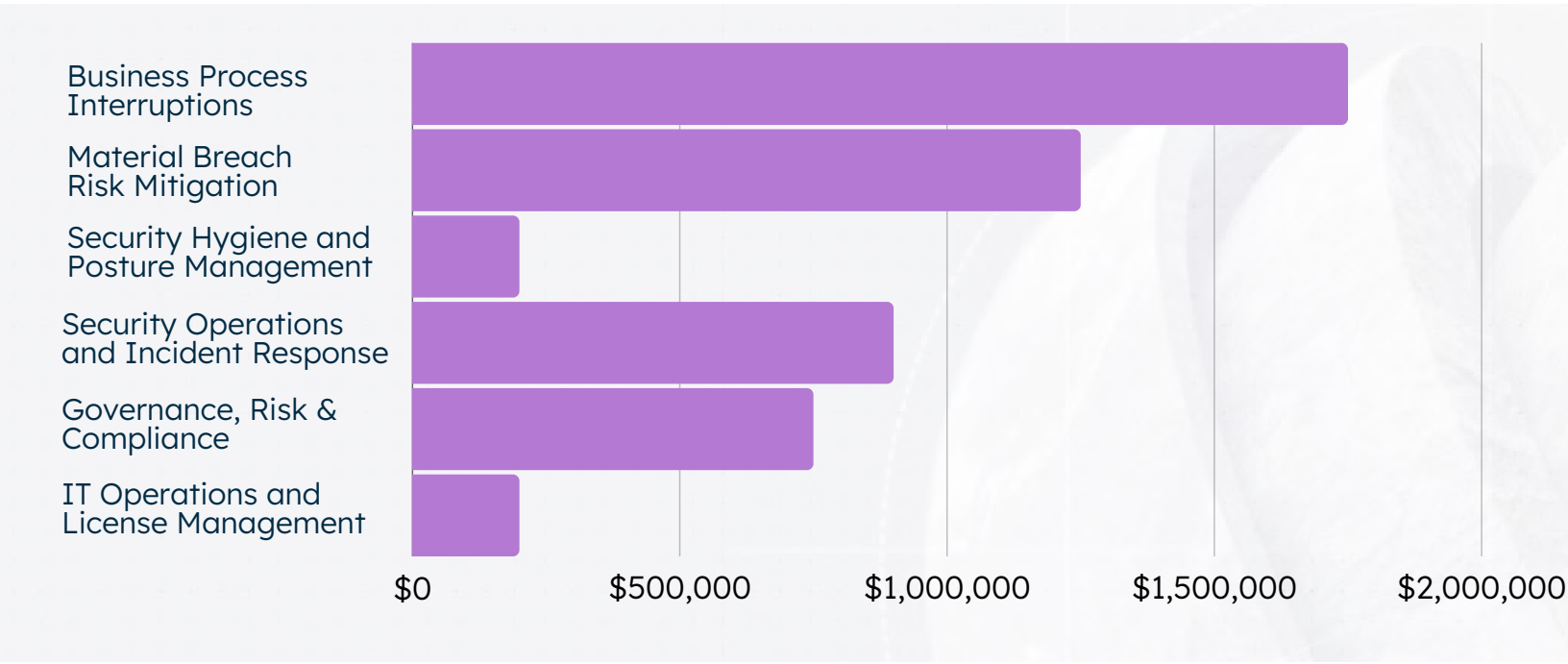
Quantifying the Value of Noetic

AN IN-DEPTH ANALYSIS OF COST SAVINGS AND EFFICIENCY GAINS FOR SECURITY TEAMS

An investment in the Noetic platform yields numerous advantages, delivering a significant return of investment (ROI) for security leaders through reduction in business interruptions, mitigated material breach risks, improved asset management efficiency, reduced attack surface, streamlined security operations, cost-effective governance, risk, and compliance management, and boosted productivity in IT operations.

These benefits collectively enhance operational efficiency, trim costs, fortify security posture, and foster increased customer trust and loyalty. Leveraging Noetic empowers organizations to redefine their risk-centric programs, safeguard critical business processes, and navigate the dynamic cybersecurity landscape with unwavering confidence.

Projected Cost Savings with the Noetic Platform



*The illustrative cost savings are based an analysis of real-world customer environments and industry benchmarks. These figures represent composite organizations with more than 10,000 employees and the estimated savings are calculated over a 3-year period.

Business Process Interruptions

Noetic enables the integration of data from existing tools and databases, providing organizations with a centralized platform that streamlines work for infrastructure, applications, cybersecurity, and remediation teams. This centralized approach ensures better coordination and collaboration among teams, leading to quicker identification and resolution of potentially high-impact vulnerabilities. Consequently, critical business processes face fewer disruptions, preserving valuable time and resources.

Beyond streamlining workflows, Noetic drives cost savings by enabling users to:

- **Mitigate the potential financial losses and business disruption associated with unplanned downtime.**
- **Efficiently allocate resources, focusing on securing and patching high-value assets and minimizing the potential impact of security incidents.**
- **Reduce costs and maximize operational efficiency by improving collaboration between IT, DevOps, and security teams.**

Potential Cost Savings*

$1.5M-$1.75M

Effective use of the Noetic platform can result in a 20-40% reduction in business process interruptions from security patching. Over three years, organizations with 20,000 or more assets can save up to $1.75M.

Material Breach Risk Reduction

Noetic plays an instrumental role in the pursuit of eliminating the financial consequences of material breaches. By effectively managing assets and maintaining an accurate inventory, organizations can reduce the risk of major reportable security breaches which could result in regulatory fines, audit costs, legal expenses, and security compliance costs. The proactive management of security risks also serves to minimize expenses related to incident response and notification to affected parties. By avoiding these costs, organizations can prevent customer churn, saving them the expenses involved in acquiring new customers and the revenue lost due to customer attrition.

By improving their overall security posture and getting better control of their attack surface, users can achieve:

- **Up to 50% boost in employee efficiency and productivity in through enhanced visibility across the cyber estate.**
- **Up to a 30% reduction in major data breach incidents by uncovering unprotected assets and high-risk vulnerabilities.**

Potential Cost Savings*

$1M-$1.25M

Research indicates the average organization with 20,000+ assets experiences 2.5 material data breaches per year. With Noetic, users can save $1-$1.25M over a 3-year period with Noetic based on the average costs associated with a breach (regulatory fines, customer compensation, loss of revenue, etc.)

Security Hygiene & Posture Management

With Noetic, organizations can achieve remarkable improvements in reducing their attack surface and improving their overall security posture. By gaining vastly improved visibility into managed and unmanaged assets across the organization, security teams can reduce the use of shadow IT and ungoverned assets. This is made possible through enhanced visibility, policy control, and cyber asset awareness. By gaining better insights into their asset landscape, organizations can mitigate the risk of unauthorized access and potential security breaches.

Another critical benefit is in the Noetic platform's support for cloud security use cases. Cloud platforms offer tremendous flexibility and scalability, but misconfigurations can inadvertently expose sensitive data or systems to security risks. By providing visibility and control over cloud configurations, particularly across complex hybrid public and private cloud environments, Noetic helps organizations avoid costly misconfigurations that could compromise their security posture. This reduction in the attack surface not only decreases the likelihood of security incidents and reduces the current burden on the security team to do this work manually or using a range of different tools.

Users can maximize the efficacy of their existing security hygiene and posture management initiatives by leveraging Noetic to achieve:

- **Up to 90% improvement in their current asset inventory process through automated identification and collection of asset data from existing systems.**
- **Reducing the exposed attack surface by over 50% through decommissioning obsolete assets and bringing shadow IT under security control.**

Potential Cost Savings*

$150,000-$200,000

Data was taken from interviews with Noetic customers who quantified and stated the benefits and efficiencies they realized with their security posture and hygiene management. The savings equate to $0.15 to $0.2M over a 3-year period.

Security Operations (SecOps) & Incident Response (IR) efficiencies

The use of Noetic triggers a profound transformation in the efficiency of Security Operations processes. Without a robust asset management solution, SecOps teams often invest substantial time triaging incidents and assessing criticality.

With the automation capabilities of Noetic, organizations streamline the cyber asset identification process, reducing the time and effort required for incident response and remediation. This automation not only accelerates response times but also minimizes the impact on business operations.

Enhanced operational efficiency in security operations yields substantial cost savings, including:

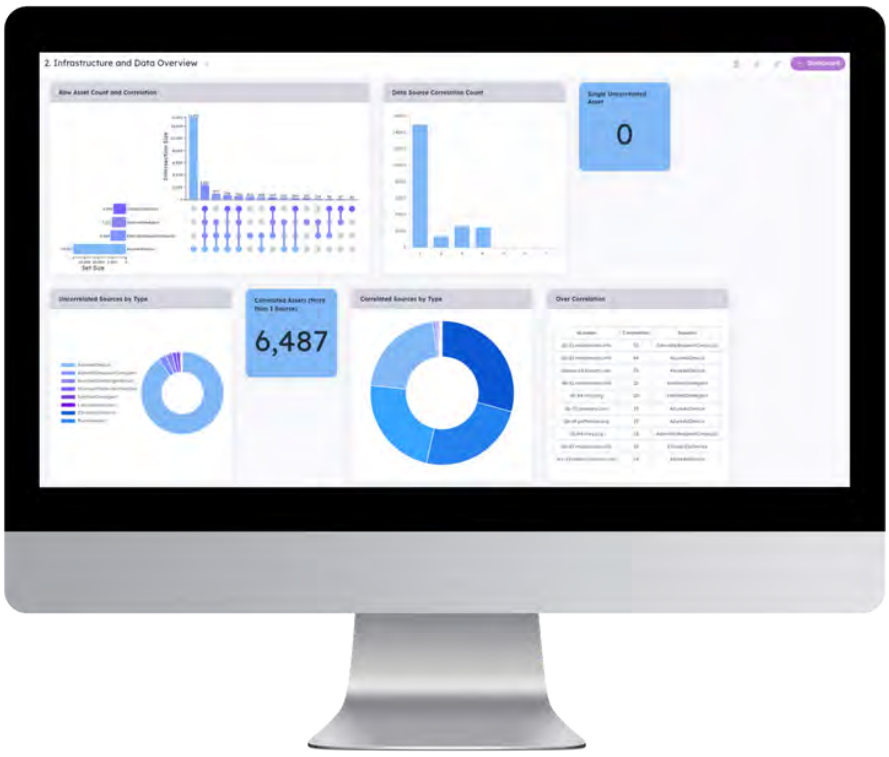
- **Optimized resource allocation enabling handling a higher volume of incidents with existing resources, resulting in substantial human capital savings.**
- **Up to 70% reduction in cyber asset investigation time, significantly expediting the security triage process.**

Potential Cost Savings*

$700,000-$900,000

SecOps and IR efficiencies from improved cyber asset visibility worth $0.7-$0.9M over three years. With Noetic, the composite experiences a 90% reduction in the number of SecOps resource hours devoted to manual investigation and identification of cyber assets.

This assumes 200+ security incidents requiring manual investigation of cyber assets per year, an average of (3-5) full-time SecOps employees dedicated to incident response, an average of 8 hours per resource to remediate each incident, and an average rate of $60 per hour.



Increased efficiency in Governance, Risk & Compliance (GRC)

Efficiency gains in governance, risk, and compliance (GRC) management are another notable outcome of implementing Noetic. Leveraging the features and capabilities of Noetic, organizations can consolidate their GRC efforts around a smaller number of essential tools, reducing complexity and streamlining their compliance processes. Noetic's unique understanding of security posture and technical control status enables organizations to automate much of the evidence collection process and compliance assessments, generate comprehensive reports, and demonstrate adherence to regulatory requirements. This automation not only saves time but also reduces the costs associated with manual compliance efforts, such as conducting audits and engaging with external assessors.

Integrating seamlessly with existing GRC tools like ServiceNow or Archer, Noetic drives efficiencies by:

- **Preventing costly non-compliance fines by continuously monitoring key technical controls associated with required frameworks.**
- **Reducing manual GRC workload by >60% through automating the evidence collection to support audit and reporting requirements.**

Moreover, Noetic provides organizations with continuous visibility into their security posture, enabling them to identify and address compliance gaps promptly. By proactively managing their cyber asset attack surface, organizations can ensure continuous compliance, avoiding penalties, fines, and other financial repercussions resulting from non-compliance.

Potential Cost Savings*

$600,000-$700,000

*Noetic users experience up to to 80% labor savings from reducing costs associated with GRC management, reporting, and assessments. This equates to $.6-$.75M over a 3-year period and includes license and professional service fees and hours that can be reallocated to other priorities.

Improvements in IT Operations and Software License Management

Although not primarily a security benefit, Noetic also enables organizations to enhance the efficiency of their Configuration Management Database (CMDB), ensuring the accuracy and currency of asset information. This empowers organizations to make informed decisions, allocate resources effectively, and streamline their IT management processes.

By aggregating and correlating insights from many different IT and Security tools across the organization, Noetic is also able to help identify where investments are underutilized or duplicated, helping to drive additional cost reduction processes.

Noetic's unique visibility across the entire cyber estate also helps to drive better alignment across the different functions, helping to optimize collaboration between Security and IT.

With Noetic, IT Operations and Management teams:

- **Reduce risk and software licensing costs by decommissioning end-of-life and unused software.**
- **Improve productivity between DevOps, IT, and security teams by ensuring consistency of information.**

Potential Cost Savings*

$150,000-$200,000

*This assumes automation of 30-50% of IT Operations and a reduction of 20% of unused and misused software that has led to unnecessary increases in license costs. This yields savings of $.15-$.2M over three years.

The Noetic Difference

In today's dynamic digital landscape, organizations grapple with multifaceted challenges in comprehending and safeguarding their cyber estate. Yet, armed with the right approach and tools, these challenges transform into opportunities for fortified security posture, risk reduction, and amplified operational efficiency.

Enter the Noetic platform—

A comprehensive cybersecurity asset management solution. It offers a unique blend of top-down and bottom-up visibility, empowering IT and security teams with a holistic view of assets, applications, and their interconnected cyber landscape. This pivotal visibility facilitates informed decision-making, priority setting, and effective risk mitigation.

Comprehensive 360-Degree 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 across the entire cyber estate for public, private cloud, and on-premises systems.

Out-of-the-Box Security Dashboards

With immediate access to out-of-the-box dashboards, customers swiftly gain access to critical insights that accelerate security strategies immediately.

Seamless Integration with Existing Investments

Noetic features agentless connectors that seamlessly integrate with existing security and IT management tools, ensuring rapid deployment.

Unified Metrics and Compliance Reporting

Noetic continuously monitors the cyber estate for changes to the environment, automatically detecting new control gaps, validating successful remediation, and collecting evidence to demonstrate compliance with relevant internal policies and external controls such as ISO 27001 and NIST CSF. Customizable dashboards and reports can be automatically generated and distributed, reducing the manual workload for the security team.

Advanced No-Code Automation

At the heart of the Noetic platform is a fully comprehensive automation workflow engine, empowering security analysts to swiftly establish new automated processes. Leveraging a wide range of deployed connectors, users are better positioned to enrich, update, or remediate their security posture coverage.

Streamlines Vulnerability Prioritization

Gartner's 2024 Strategic Roadmap for Managing Threat Exposure (November 2023) emphasizes the need for organizations to transition from traditional vulnerability management to a more dynamic continuous threat and exposure management practice. Security leaders are recognizing the growing issue of expanding attack surfaces and are seeking better approaches to evaluate and address these risks.

As part of this, Noetic leverages external open-source and commercial threat and vulnerability intelligence data from trusted sources such as NIST, CISA, FIRST, MITRE, Noetic empowers users to accurately assess vulnerability severity and exploitability together with asset exposure and criticality. This drives prioritization, empowering users to focus on critical areas.

In conclusion, Noetic Cyber presents a transformative solution to fortify cyber defenses, streamline operations, and achieve operational excellence. With its comprehensive visibility, risk-driven prioritization, and automated compliance, it equips organizations to navigate the evolving cybersecurity landscape with confidence, ensuring robust protection for critical assets.

ON-DEMAND DEMO

See the power of the Noetic platform.

Elevate your defenses beyond conventional solutions and empower your organization to navigate the ever-changing landscape of cyber threats with confidence.

Watch Now

noetic

Empowering teams to trust, understand and act on security & risk data.

www.noeticcyber.com hello@noeticcyber.com linkedin.com/noeticcyber