Centerity's Cyber AIOps modules evaluate risk information from cyber-oriented layers that may impact your critical business services

These include extensive discovery capabilities, compliance and regulatory measurements and security configuration analysis. As your dynamic environment is in a constant state of change, these features along with Centerity's AIOps topology discovery engine enables you to identify changes in endpoints, networking and other elements in a contextual way. Configuration analysis coupled with performance analytics allows for the creation of dedicated executive dashboards and reports for accurate measurement of service level impact.

The complexity of today's IT environments coupled with security tool fragmentation and misconfiguration creates a major cyber hygiene challenge for companies of all sizes. Centerity helps by continuously monitoring and improving your cybersecurity posture, providing visibility and control over all IT assets connected your network and identifying external attack surface risks all with business context and impact analysis. Centerity's Cyber AIOps capabilities present a comprehensive way for organizations to implement and maintain proper cyber hygiene and business health across your critical applications and processes.

Centerity's Cyber AIOps offering provides the ability to align both security and IT metrics with business impact. Named a Gartner Cool Vendor, Centerity's dynamic service views eliminate 'unknown' IT zones while enabling total visibility into all technological layers to help reduce mean-time-to-repair (MTTR) and eliminate Cyber threats and risks which can impact your business.

- **Centerity's Cyber AIOps Observer** module provides continuous monitoring and actionable insights allow organizations to ensure compliance hygiene, compliance to frameworks, and fully optimized tool configuration across its security ecosystems. The customizable platform enables organizations to address fragmented tool ecosystems while providing timely metrics on overall security posture.
- **Centerity's Attack Surface Management** module identifies, manages and help defend an organization's entire global digital footprint. It locates and maps digital assets (Internet-connected devices) while providing real-time alerts about security issues such as unknown exposures, shadow IT risks, misconfigurations and vulnerabilities among other security issues, with related business context impact.

- **Centerity's Rogue Device Mitigation** module adds to your cyber hygiene arsenal with the ability to detect and mitigate the threat of rogue devices across the enterprise. Through our solutions, security teams gain full visibility of their organization's infrastructure.
- **Centerity's Autonomous Breach Protection XDR** module collects all activity signals from the environment and correlates these to understand the true context of each activity then executes precise breach protection actions. This module provides Next-Generation Antivirus, Endpoint Detection and Response, Network Analytics, Deception and User Behavioral Analytics.

All Centerity Cyber AIOps modules can be implemented quickly to produce immediate value and reduce organizational risk cost-effectively, providing a clear overall picture of your organization's cybersecurity posture, reducing your cybersecurity vulnerabilities, and helping ensure proper Cyber hygiene.

Visit the links below for more information:

https://www.centerity.com/
https://www.centerity.com/cyberops/