CENTERITY

October 2020

Cyber AIOps – Cyber Observability Use Cases

merlin®

1 Manage the Cybersecurity Chaos

The Problem

The challenging cybersecurity landscape of today offers an over-abundance of cybersecurity tools. As the number of breaches proliferates, so have the solutions and technologies designed to stop them. The state of cybersecurity is not getting easier to manage, even though enterprises and organizations worldwide are spending more money than ever on new technologies and solutions.

The Solution

Centerity Cyber AIOps Observability Module provides a unified single-pane-of-glass solution that continuously monitors, analyzes, and displays the cybersecurity posture of the organization as well as provides proactive recommendations to improve. Designed especially for CISOs, IT Infrastructure Managers, SOC Managers, Risk Officers and other relevant stakeholders in the enterprise, Centerity delivers an end-to-end continuous Cybersecurity Management and Awareness solution, focusing on the following four layers

CYBER AND IT TOOLS HYGIENE STATUS

CYBERSECURITY POSTURE VIEWS

CYBER COVERAGE STATUS

IMMEDIATE ALERTS ON DEVIATIONS FROM NORMAL ACTIVITY

2 Line of Defense status

The Problem

Organizations need to implement dozens of different security tools from different vendors to secure their digital data and their network environments. It is extremely difficult and requires tremendous efforts to verify that the tools are well configured, are aligned with industry as well as the vendors best-practices and are implemented in a manner that maximizes their capabilities and features.

The Solution

Centerity Cyber AIOps Observability Module continuously verifies that the cybersecurity tools and cybersecurity related IT infrastructure tools are well configured, up and running and deliver the desired line of defense. This includes specific module issues, policy issues, agent statuses, scanning issues, licensing statuses and more.

3 Prioritize Cyber Security Defense efforts

The Problem

Organizations cannot protect all the digital data equally and they need to prioritize critical/high risks and protection of the organization's crown jewels/assets.

The Solution

With Centerity Cyber AIOps Observability Module you can create specific, customized views based on the organization's critical business assets, you can modify polling intervals, weights of criticality and thresholds per asset. Customizable asset views enable you to get an instant and comprehensive picture about your security status based on tech teams (that are in charge of specific tools),remote work, regions, domains, various services and specific applications that serve them (such as billing, production line, HRM, etc.) within your organization.

4 Understand if something went wrong ASAP

The Problem

A flood of data along with a very complex IT infrastructure to manage as well as siloed teams causes in most cases months to know that something went wrong and that the damage is severe.

The Solution

Centerity Cyber AIOps Observability Module engine continuously polls the various cyber and IT tools already deployed in the organization for highly valuable data and calculates the activities that represent normal behaviour. Then, Centerity alerts continuously about deviations from the normal behaviour. This enables the relevant stakeholders to easily identify cyber incidents, weaknesses and quickly manage their mitigation efforts, while reducing mean-time-to-detect (MTTD). This aids in the prevention of breaches and improves the organization's cybersecurity posture and maturity on a continuous basis.

5 Building on-going security program

The Problem

CISOs, Risk officers, CIOs, IT Infrastructure Managers and team leaders need to design and implement an on-going security program.

The Solution

Centerity Cyber AIOps Observability Module comes equipped with Industry Best Practices recommendations on Cyber Security capabilities needed (coverage) and through thousands of Critical Security Controls (CSCs) reflects vendors and industry best-practices. These capabilities and CSC's are continuously updated recommending actions that are needed in order to stay safe at all times. You can always plan ahead and build an ongoing security program and work plans based on the organizations needs and its risk appetite.

6 Reporting

The Problem

Organizations need to continuously report to C-level management, the board, auditors, risk officers and others about the cybersecurity status and posture of the organization over a period of time.

The Solution

AUTOMATIC REPORTING: Centerity Cyber AIOps Observability Module reporting engine provides updated information about the organization cybersecurity tools status and cyber posture views. The reporting engine enables you to view the reports in tabular and graphical formats, customize the reports with filters, schedule customized reports for delivery to specific email addresses and download the reports to your computer in PDF and Excel formats.

7 Compliance with standards, regulations and frameworks

The Problem

Organizations need to comply with industry security standards, regulations and frameworks (ISO, NIST, PCI, CIS and many others). It takes endless efforts to gather information from many various data sources and keep the information updated.

The Solution

To address the growing compliance needs and complexity, Centerity Cyber AIOps Observability Module delivers comprehensive awareness into your organization for international standards, such as NIST, ISO 27001, PCI-DSS and more by continuously retrieving data from various security tools. Out-of-the-box self-assessment sheets deliver an on-going compliance visibility that saves time and effort and most importantly – provides you with highly valuable ACTUAL cyber data, coming in directly from the relevant cyber and IT tools.

8 Cyber defense infrastructure documentation

The Problem

Ever-changing cybersecurity environment, IT Infrastructure architecture and configuration changes make documentation of updates practically impossible to maintain.

The Solution

Centerity Cyber AIOps Observability Module connectors continuously retrieve Critical Security Controls (CSCs) from the various tools already deployed in the organization and then save and store the raw data. You can then keep track on Admins activities, FW rule changes, policies changes, malware definitions updates, tool configuration changes and more.

merlin
August 2020
If Tools Could Talk...
Come clean with your cyber hygiene
"There's something you should know" -OUTDATED ANTI-VIRUS
"I don't have all the answers" -INACCURATE CMDB
"I'm not who you think I am" -UNRELIABLE IDAM

Read more on Merlin's `If tools Could Talk' Whitepaper

About CENTERITY

Centerity's Cyber AIOps Platform delivers Dynamic Business Service Views of the full technology stack to the executives responsible for technology-driven business services, ensuring the performance, availability and security of critical processes. Centerity displays real-time, consolidated business analytics for complex on-prem, cloud, and hybrid technology environments generating SLA Executive Dashboards that identify performance anomalies and isolate faults across applications, operating systems, infrastructure & cloud assets.