CYBER OBSERVER

Witz Cybersecurity
Australia & New Zealand Partner

Cyber Observer's Exciting New Features

The release of version 3.5

The challenging cybersecurity landscape of today offers an over-abundance of cybersecurity tools and services both on-premises and in the cloud. 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 problem: Your organization already has dozens of security tools in place, now you must maintain that security posture but with budget cuts, manpower reductions, requirements to maintain compliance with standards, building an ongoing security program, reporting to management, managing ever-changing infrastructure, etc. How can you know if something went wrong ASAP?

Designed for CISOs and senior InfoSec managers (such as CIOs, C-level managers, risk officers, SOC managers and IT Infrastructure personnel), Cyber Observer's management platform empowers leadership, security and IT technical teams with continuous, unified views of their entire cybersecurity ecosystem. This enables you to easily identify weaknesses, reduce mean-time-to-detect, prevent breaches and advance organizational cybersecurity posture and maturity.

- Indicators to cybersecurity tools that are misconfigured, malfunctioning, or lacking
- Security gaps that exist, alongside recommendations for steps to improve.
- Building ongoing security program to ensure alignment with new threats.
- Compliance with standards such as ISO, NIST, and others.
- Continuous reporting.
- Continuous analytics provide alerts on deviation from normal behavior.

CYBER OBSERVER

Witz Cybersecurity
Australia & New Zealand Partner

Introducing the all new Cyber Observer version 3.5

1.Continuous Executive view

All the information you need is available in one click from the main screen. The Cyber Observer view page is equipped with an “enriched view” capability for one-click access to all the necessary information: Instantly see what tool has an error, view security coverage by domain, top critical alerts, security trends and more without ever leaving the home screen.

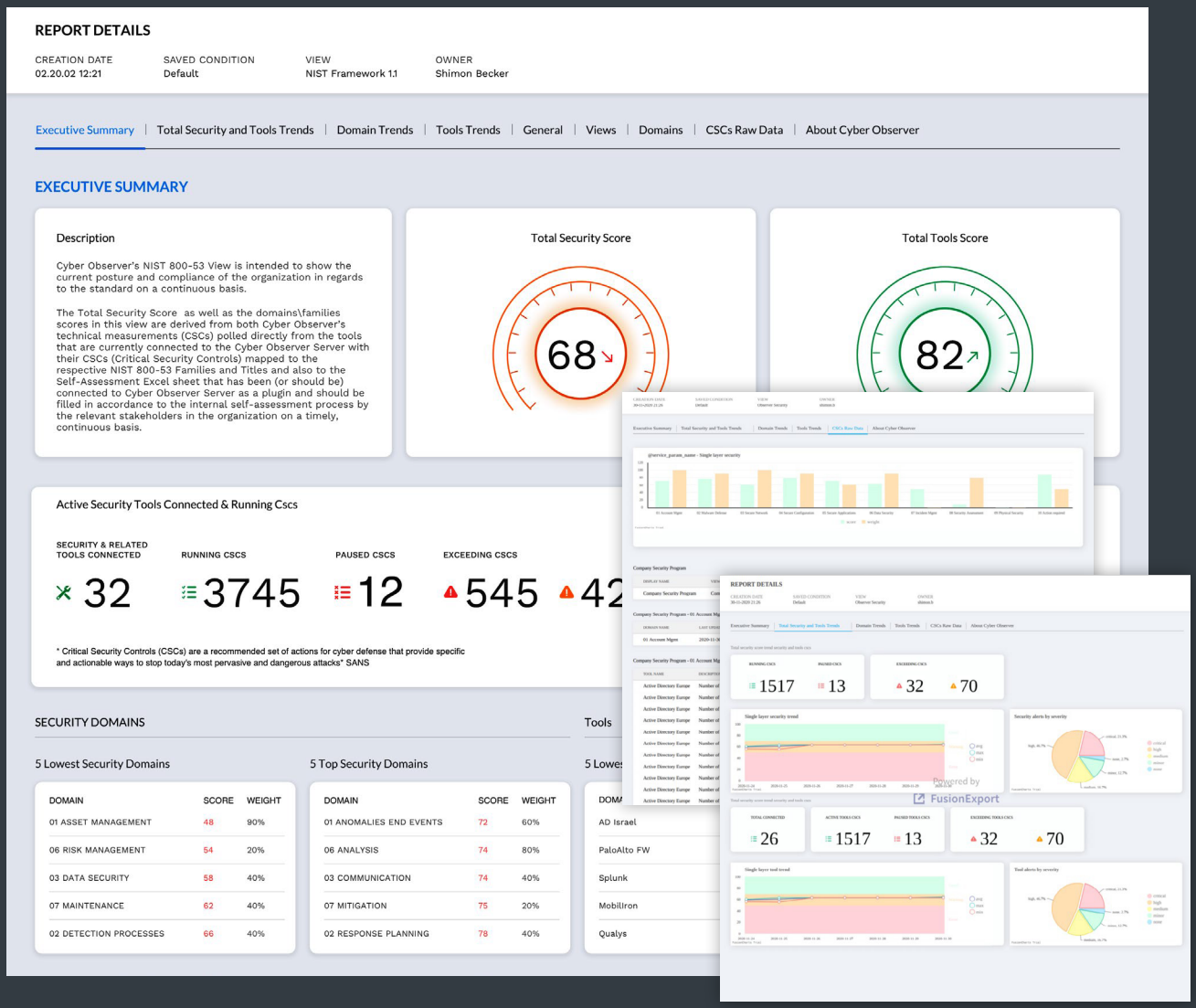
2. All new UI/UX

3. Continuous Reporting

Organizations need to continuously report to board members, C-level management, auditors, risk officers, and other stakeholders about their cybersecurity status and posture. It takes significant coordination, effort, and time to prepare these reports.

Save time and gain continuous results by using Cyber Observer's new built-in reporting module that automates up-to-the-minute reports about the organization's cybersecurity status and cyber posture views, as well as the ability to compare and verify improvement. The reporting engine enables you to view the reports in both tabular and graphical formats.

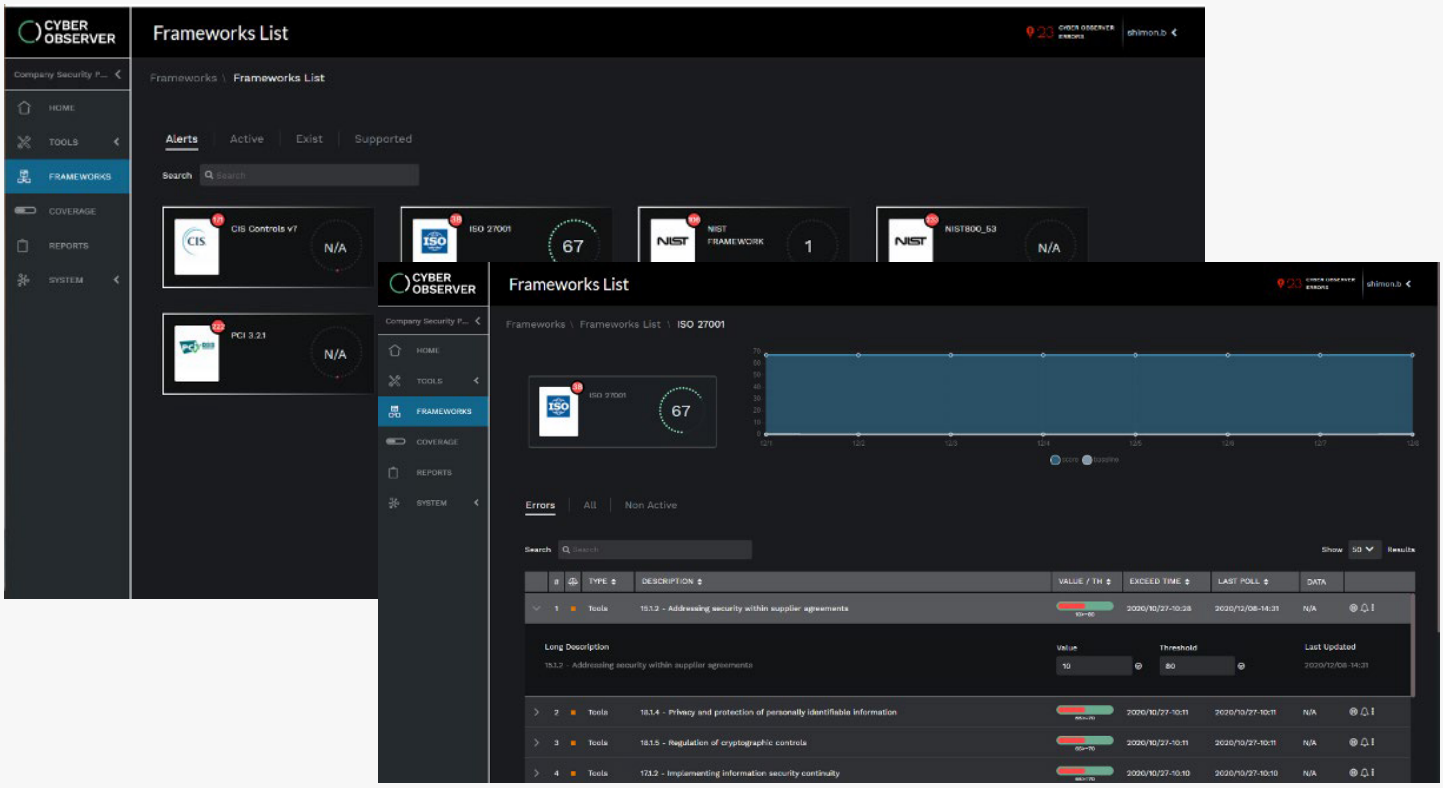
Customize the reports with filters, schedule customized reports for delivery to specific email addresses and download the reports to your computer in PDF and CSV formats.



4. Continuous Standards and Frameworks Compliance Status

Cyber Observer delivers comprehensive management and awareness capabilities regarding organizational compliance with international standards such as NIST, ISO 27001, PCI-DSS, and more by continuously retrieving technical configuration and security data from the various security tools already deployed in an enterprise network.

Out-of-the-box self-assessment templates provide an additional layer of ongoing audit and compliance management that saves time and effort, and most importantly, provides organizations with an unprecedented, continuous view of their compliance status. This revolutionary single-pane-of-glass view enables risk officers, CISOs, and other relevant stakeholders to keep real-time track of their organizations' regulatory compliance statuses and be prepared for timely audits.



5. SWIFT view

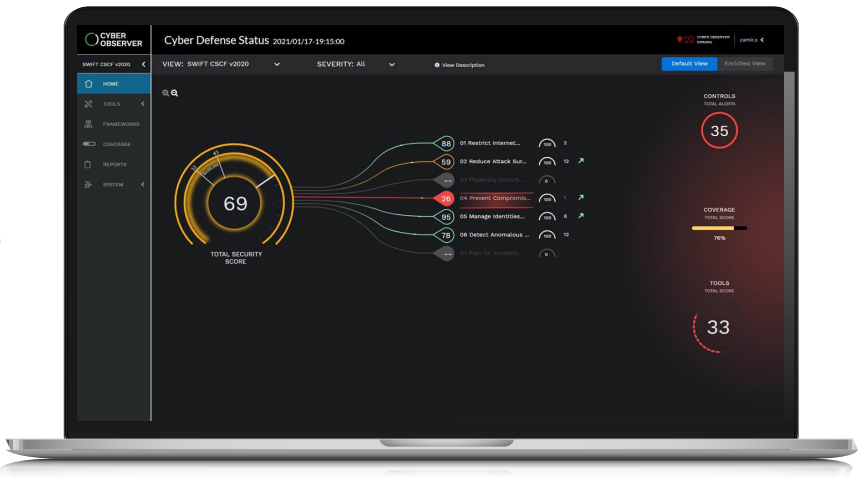
The SWIFT CSCF view is a built-in and pre-defined view in Cyber Observer and contains the framework's security controls domains:

- Restrict Internet Access and Protect Critical Systems from General IT Environment
- Reduce Attack Surface and Vulnerabilities
- Physically Secure the Environment
- Prevent Compromise of Credentials
- Manage Identities and Segregate Privileges
- Detect Anomalous Activity to Systems or Transaction Records
- Plan for Incident Response and Information Sharing

The relevant cyber and IT tools located in the organization's SWIFT infrastructure were mapped to the relevant SWIFT domains following the SWIFT security controls requirement. Then, specific Cyber Observer technical CSCs (Critical Security Controls) were associated from these tools to their relevant SWIFT domains.

For example:

1. Firewalls (such as Check Point) and Virtual Platforms (such as VMware) in the Restrict Internet Access and Protect Critical Systems from General IT Environment security controls domain
2. Configuration\Patch Management tools (such as Bigfix and SCCM) and Vulnerability Scanners (such as Rapid7) in the Reduce Attack Surface and Vulnerabilities security controls domain
3. Directory Services (such as Active Directory) and Privilege Access Management tools (such as CyberArk) in the Manage Identities and Segregate Privileges security controls domain, and so on.

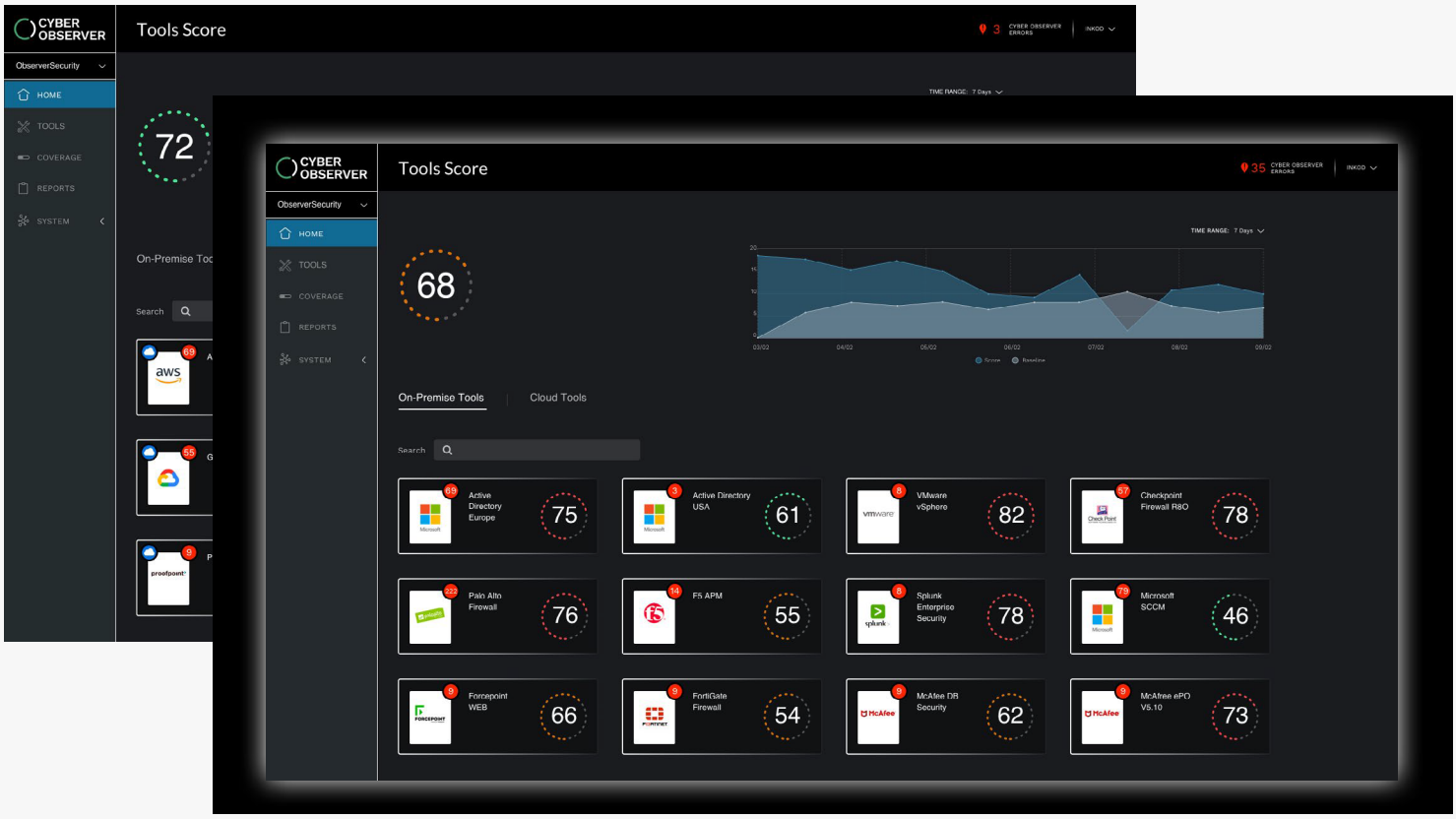


6. Thousands of new predefined CSCs ready to use

Just connect Cyber Observer to your tools and thousands of predefined CSCs based on industry best practices and recommendations as well as standards are ready to use out-of-the-box already mapped to pre-defined views. This will allow your technical teams amd management to continuously see and prioritize mitigation tasks needed to avoid risk and save lots of investigation and learning hours.

7. Support Cloud and On-premises data sources

The core engine of Cyber Observer can retrieve information from hybrid environments, and you can connect as many on-premises/cloud tools as needed to create a holistic view of your network.



8. Flexibility: Building custom views, custom CSCs

The Cyber Observer core engine is very flexible. After reviewing the out of the box views, you can copy, modify and create views as well as security domains for any specific department. Cyber Observer is fully customizable to suit your company's needs. You can modify person or existing CSCs or build new additional CSCs. You can also build views based on your critical assets. The flexibility of Cyber Observer enables you to build views for specific teams, SOC managers, auditor needs, location based views, views you would like to share with specific roles, a view for members of the board, C-level management views and many more.

9. Build your own connector

You can easily create and add your own connectors and retrieve information from your internal/ non-commercial data sources using Cyber Observer's open API.

10. All new API

Cyber Observer's new and improved open API is available to share all the information with third-party tools such as SIEM tools, automation tools and AI tools.

11. Scale-out

You can implement unlimited Cyber Observer core engines within separate networks and correlate all the information to a MOM (manager of managers) view.

12. Historical database

You can store historical CSCs raw data within Cyber Observer's historical database and create historical and comparison reports and retrieve forensic data.