cyber
OBSERVER

Continuous Cybersecurity Management and Awareness Solution

White Paper | November 2019

Contents

The Challenge

'Organizations are failing at early breach detection, with more than **92% of breaches** undetected by the breached organization.
The situation can be improved with stronger threat intelligence, the addition of behavior profiling and better analytics.' [1]*
***Gartner**

'As defenders, we have access to an extraordinary array of security tools and technology, security standards, training and classes, certifications, vulnerability databases, guidance, best practices, catalogs of security controls, and countless security checklists, benchmarks, and recommendations.' But all of this technology, information, and oversight has become a veritable 'Fog of More'.*
***SANS**

Introducing Cyber Observer

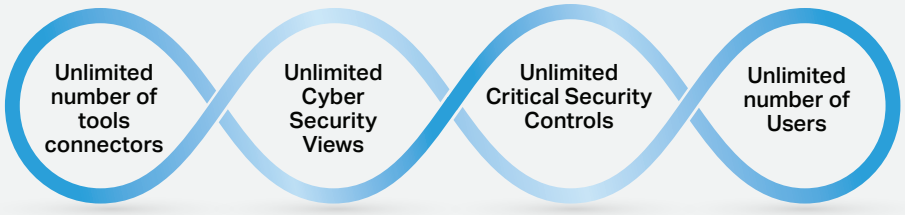
Cyber Observer is holistic cybersecurity management and awareness solution. It continuously measures the cybersecurity status of an organization's security environment by retrieving and analyzing Critical Security Controls (CSCs) from relevant security tools. Critical Security Controls are the most fundamental data, processes and actions that every enterprise should employ in order to prevent, alert, and respond to the attacks that are plaguing enterprises today.

'Many organizations are suffering from investments in disjointed, non-integrated security products that increase cost and complexity.' [2]*
***Ponemon Institute**

The comprehensive information empowers CISOs and executives to make insightful and timely decisions to ensure the cybersecurity of the organization.

Developed for CISOs, Infosec and IT managers, Cyber Observer provides extensive cybersecurity understanding for all stakeholders. By connecting to the security and related third-party vendor tool suite, Cyber Observer provides insights and recommendations to empower effective enterprise cyber defense.

Empowered with **comprehensive awareness**, you can easily identify weaknesses, reduce mean time to detect, prevent breaches, drive strategic planning and report to executive stakeholders. These activities continually improve enterprise **security posture** and **maturity**.



Four Layers of Cybersecurity

Organizations fortify themselves with an abundance of security technologies then may struggle to determine the enterprise level of cybersecurity achieved. Cyber Observer delivers a single-pane-of-glass solution displaying performance data that proactively provides improvement recommendations in near real-time. This single view of enterprise-wide cybersecurity allows the organization to deliver the level of security required, meeting both compliance and business risk needs.

Tools Status:

Based on manufacturers best practices and industry recommendations, Cyber Observer provides internal scoring on your current Security Tools configurations and presents the optimization status of your tools.

Figure 1: Cyber Observer Tools screen

Security Views:

Based on industry-recognized frameworks and Critical Security Controls (CSCs) Cyber Observer provides near real-time assessment of all your security domains and recommendations to improve.

Figure 2: Cyber Observer Security views screen

Coverage Status:

Based on a given industry framework, Cyber Observer provides an on-going cybersecurity program, gap analysis, and risk mitigation management to enhance your security environment.

Figure 3: Cyber Observer Coverage screen

Deviation from normal behavior:

Leveraging near-real time monitoring of security tools and domains, Cyber Observer's core engine provides continuous analytics and alerts in case of deviation from normal behavior.

Figure 4: Cyber Observer Behavior screen

Real-Time Scoring of an enterprise Cybersecurity

Cyber Observer automatically constructs up-to-date cybersecurity posture based on embedded security tools in the organizational infrastructure, and processes in all areas of security. Every security tool and/or process carries significance, as does each area of control and security. Taken together, they serve to calculate a security status in each domain of security as well as the overall cybersecurity of the enterprise.

Cybersecurity Domains

Cyber Observer distinguishes an overall security framework into security domains. The platform measures enterprise security posture by pre-configured out-of-the-box security domains:

- **Account Management**
- **Malware Defense**
- **Secure Network**
- **Secure Configuration**
- **Secure Application**
- **Data security**
- **Incident Management**
- **Security Assessment**
- **Physical Security**

'Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principal benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results.' [3]*
***SANS**

'The Controls take the best-in-class threat data and transform it into actionable guidance to improve individual and collective security in cyberspace.' [4]*
***SANS**

Figure 5: SANS critical security controls view concept

Critical Security Controls (CSCs)

Critical Security Controls (CSCs) are the most fundamental data, processes and actions that every company should employ in order to prevent, alert, and respond to the attacks that are plaguing enterprises today.

Cyber Observer's methodology is based on continuously implementing, retrieving and analyzing CSCs from all relevant data sources existing in the organization. CSCs are customized to meet the needs of each organization, and quantified to establish baselines for each domain and for overall security within the cyber eco-system.

'CISOs are under increasing pressure to ensure their organizations do not become victims of external attackers, while simultaneously maintaining compliance with regulations.' [5]*
***Gartner**

Cyber Observer's CSC database is based on the cybersecurity industry and leading vendor's best practices. In addition, the frameworks and recommendations of NIST, ISO, NERC-CIP, the Council on CyberSecurity and more, as well as requests from CISO's and the company's knowledge are used to effectively manage the complicated cyber security eco-system.
The CSC database is continuously updated based on new threats, relevant information, security tools and intelligence received from cybersecurity agencies.

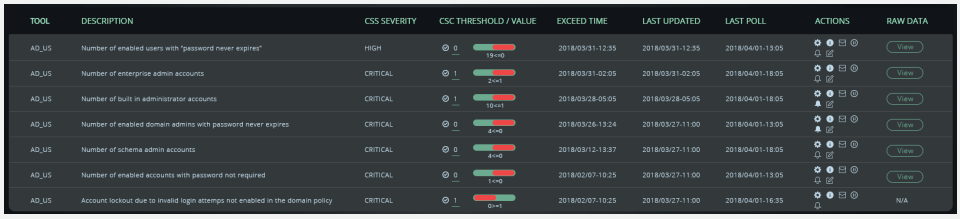


Figure 6: CSCs, showing various criticalities and details.

Build a Cyber-secure Enterprise Ecosystem

Cyber Observer automatically builds and assesses a security eco-system based on an enterprise's existing cybersecurity infrastructure. The platform continuously quantifies baseline security and vulnerability levels in various domains and customizes Critical Security Controls (CSCs) to ensure continuous and robust enterprise protection.

Real-Time Security Status evaluation and alert in case of deviation from normal behavior

Once the existing cybersecurity eco-system is defined and in place, Cyber Observer monitors and delivers alerts regarding deviations, security breaches, potential risks and threats, in specific areas as they relate to other systems across an enterprise. Security status across an enterprise is quantified and presented in clear, easy-to-read data-visualiation views.

Figure 7: Deviation from normal behavior

'Greater visibility into all applications, data and devices and how they are connected lowers and organization's security risk.' [6]*
***Ponemon Institute**

Gain Comprehensive Coverage

To deliver on-going Cybersecurity program capabilities, Cyber Observer continuously monitors your cyber ecosystem while presenting real-time Coverage gap analysis. Coverage Gap analysis indicates and presents cybersecurity coverage gaps in currently deployed enterprise tools. The platform proactively provides a list of lacking security capabilities for optimal coverage recommended by the industry.
The moment our platform is deployed in an enterprise network, Cyber Observer Server identifies and analyses the capabilities of connected security tools. Cyber Observer automatically maps these capabilities into the pre-defined Security Domains, such as Account Management, Network Security, Security Assessment, Data Security, Secure Configuration, Malware Defense, etc.
Cyber Observer provides a comprehensive visuality into uncovered security areas. It is the most essential information to generate an on-going cybersecurity program and more comprehensive cybersecurity awareness and maturity.

Figure 8: Cyber Observer comprehensive Coverage view

Proactive Cyber Security Approach

Effective cyber defense ideally prevents an incident from taking place. The best action is a pre-emptive and proactive approach. Cyber Observer utilizes a proactive mindset and approach in order to protect enterprise's infrastructure and sensitive corporate data from attack before the attackers strike. Cyber Observer's proactive cybersecurity approach provides actionable intelligence so you can recognize vulnerabilities and potential attack vectors as well as mitigate them before attackers gain a foothold in your environment. Proactive Cybersecurity puts you firmly in control of your security eco-system.

Cost of a data breach highlight

$3.92M
Average Total Cost of a Data Breach

25,575 records
Average Size of a Data Breach

$150
Cost per Lost Record

279 days
Time to Identify and Contain a Breach

[7] **Ponemon Institute**

Maintain Awareness in a Constantly Changing Environment

Cyber Observer enables security professionals to maintain management control in a highly dynamic environment, where new technologies are constantly being introduced, along with new and unexpected threats.
Data is provided in clear, real time, role-based views, with a design emphasis on communicating data concisely and easily to ensure that CISOs and senior InfoSec managers receive the relevant data easily, expediting decisions and facilitating accountability for network security.

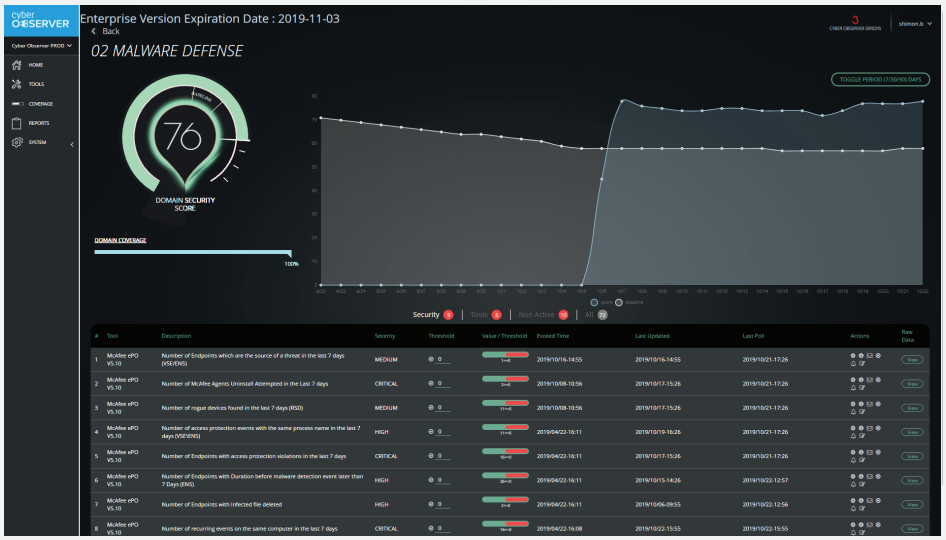


Figure 8: Historical Reference, showing improving overall (blue) and baseline (white) scores.

Cyber Observer Highlights

Time to Deploy:
Up to 4 hours

Time to add new Tool:
1-2 hours

Deployment method:
OVA (Virtual Machine)

Real value Demonstrated:
Within hours

Cyber Observer presents unlimited views to diverse system users.
Users can build additional views per business unit, threat, standard, role, etc.

Cyber Observer provides:

- Status of tools and steps to improve
- Status of each security domain and recommends steps to improve
- Status on coverage and recommendations for additional capabilities needed
- Alerts in cases of deviation from normative behavior

Cyber Observer currently encompasses PCI DSS, ISO 27001, NIST 800-53, NIST Framework and CIS Framework v7. The system supports adding unlimited standards, which we prioritize based on customer's requests.

Built-in automatic Reporting capabilities

The Cyber Observer System Reports feature provides real-time reports about each of the cyber defense tools and views in your organization, e.g.:

- Security posture
- Tools status
- Executive reports
- Cyber Observer audit

The reporting engine enables you to use filters and create standard and customized reports :

- View the reports in tabular and graphical formats
- Customize the reports with filters
- Save customized reports
- Schedule customized reports for delivery to specific email addresses
- Download the reports to your computer in PDF and Excel formats

Reference

[1] Gartner, Inc., Magic Quadrant for Security Information and Event Management, K. Kavanaugh, O. Rochford, July 20, 2015
[2] Ponemon Institute, Research Report, Separating the Truths from the Myths in Cybersecurity
[3] SANS, CIS Critical Security Controls, The CIS Critical Security Controls for Effective Cyber Defense
[4] SANS, CIS Critical Security Controls, The CIS Critical Security Controls for Effective Cyber Defense
[5] Gartner, Forecast: Information Security, Worldwide, 2016-2022, 2Q18.
[6] Ponemon Institute, Research Report, Separating the Truths from the Myths in Cybersecurit
[7] Ponemon Institute, The Cybersecurity Illusion: The Emperor Has No Clothes