CYBER OBSERVER

Cyber Observer White Paper

Remote Cybersecurity Management

Turn your cybersecurity chaos into clarity

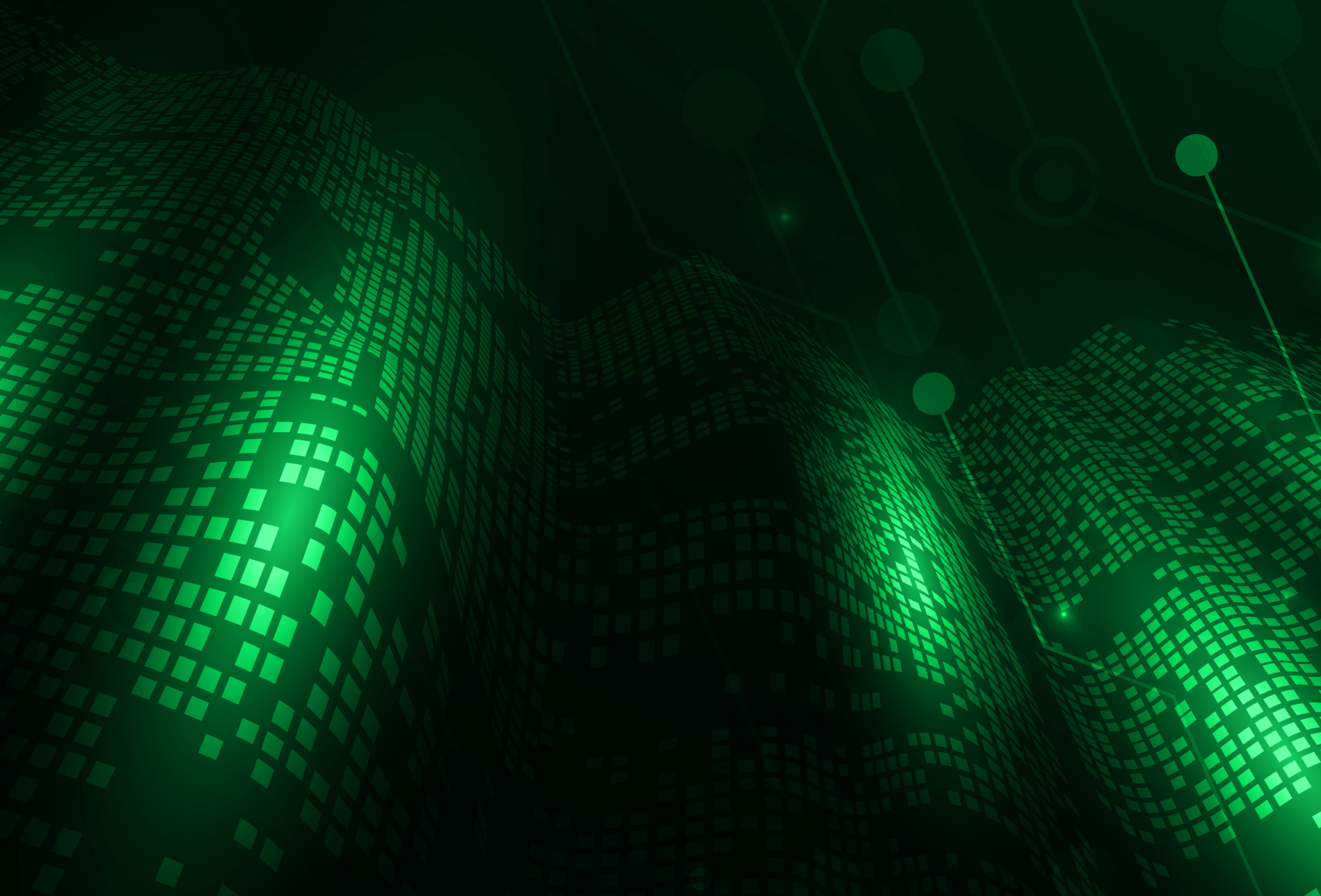


Table of contents

Introduction

As the world works to prevent the spread of the COVID-19 virus, organizations are moving their employees at groundbreaking speeds to a remote workforce model. This puts additional strain on security teams and raises critical cybersecurity issues. At the same time, cyber adversaries are busy designing new tactics and techniques to exploit this wave of confusion and chaos. How can you maintain efficient and effective cybersecurity in these challenging times?

Core elements of remote cybersecurity management

Remote work increases the risk of cyberattacks and challenges CISOs and security teams to maintain the organization's healthy cybersecurity posture. Organizations must consider real cybersecurity challenges in these challenging days.

Key factors that can ensure remote cybersecurity:

- Make sure your current security and related tools are up-to-date and running. Keeping strong cybersecurity hygiene is critical for the remote work environment.
- Comply with the latest security frameworks. Verify your security portfolio includes remote working access management, including coverage for personal devices.
- Maintain updated data privacy policies for employees who access documents and data.
- Identify gaps in your security coverage as required, and close the gaps with available solutions.
- Be aware on anomalous deviations in cybersecurity behavior and review the history and analytics.

Cyber Observer cybersecurity management approach

Cyber Observer experts are uniquely qualified to help organizations transition smoothly to a more secure environment. The Cyber Observer platform is ideally suited to provide CISOs and security teams with continuous visibility into their enterprise cybersecurity posture, including coverage gaps, malfunctioning tools, abnormal deviations and more.
Cyber Observer has supported its own widely dispersed workforce since the company was founded, so we know the challenges and how to solve them.

Cyber Observer can help you manage your cybersecurity from home:

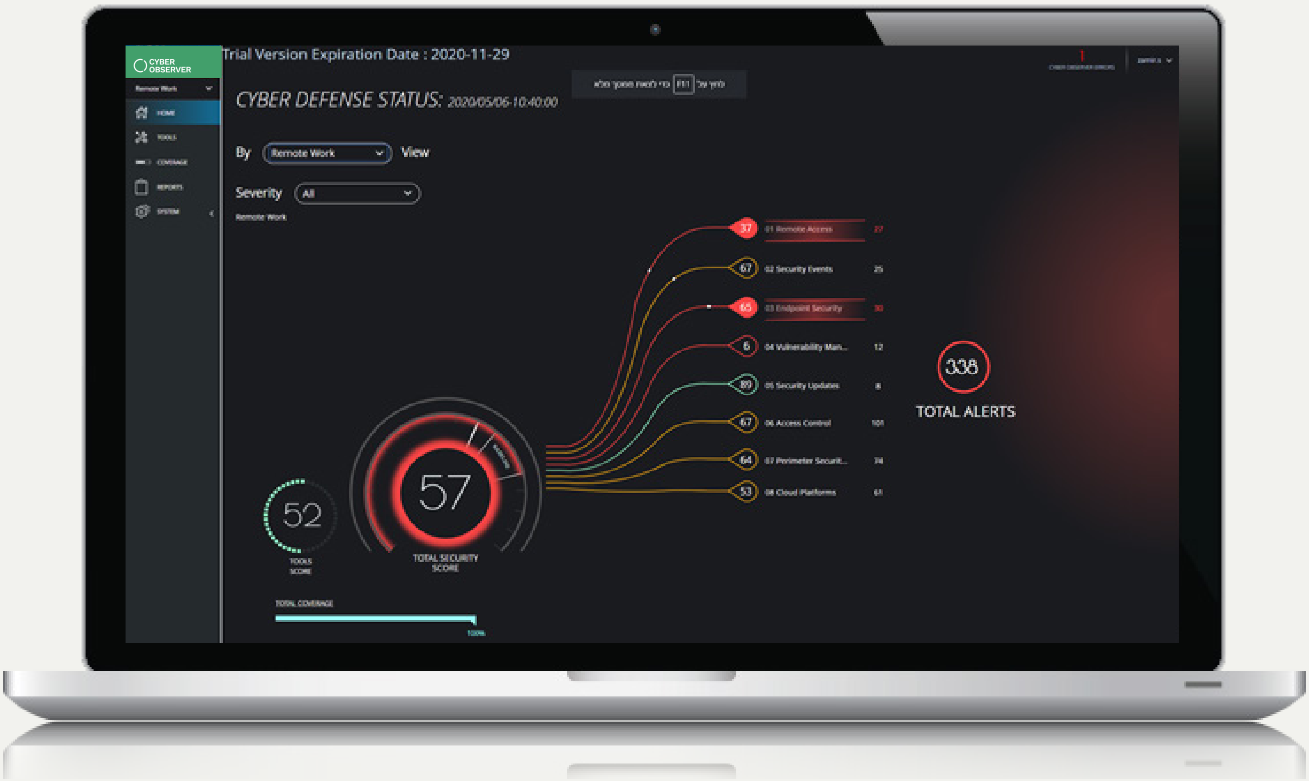
- Continuous security tools monitoring
- Real-time comprehensive visibility into the performance of your cybersecurity portfolio
- Continuous coverage status
- Real-time alerts of deviations from normal behavior

Remote cybersecurity management tactics

Companies have increased the use of software-as-a-service (SaaS) and cloud-based remote connectivity services to enable and support employees working from home. Remote working services may pose a potential security risk when combined with possible human-error-enabled security lapses. Criminal actors continually seek to collect credentials for these services, potentially allowing them to gain access to their victims' SaaS accounts and organizational data.

Cyber Observer developed a bespoke Remote Workspace Management view that continuously monitors the entire enterprise security stack, measures its capabilities of security and related tools, and detects and classifies a severity status based on predefined Critical Security Control (CSC) indications. It also alerts when detecting deviations from normal behavior. The Remote Workspace Management view covers these areas:

- Remote Connections
- Security Events
- Endpoint Security
- Vulnerabilities
- Assessments
- Security Updates
- Access Control
- Perimeter Security
- Cloud Platforms



Trial Version Expiration Date : 2020-11-29

CYBER DEFENSE STATUS: 2020/05/06-10:40:00

By Remote Work View

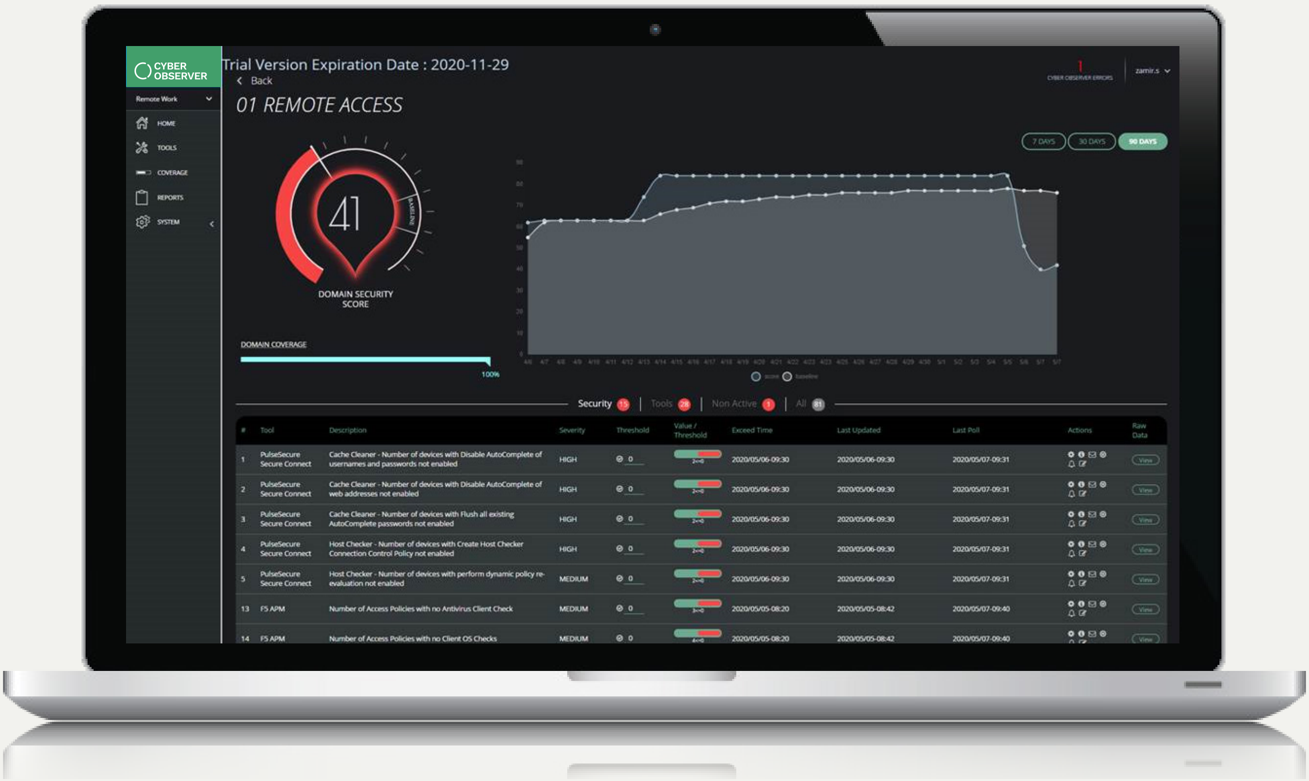
Severity All

Figure 1. **Remote Work View**

Remote access

To enable secure and fast remote access to corporate resources from any network, and from any device, you need to protect your network with SSL VPN capabilities.
Examples of CSCs we look for in this domain:

- Number of admin realms with two-factor authentication disabled
- Number of access policies with allowed any vendor antivirus client check
- Number of local user db with force password check disabled
- Number of realms with host checker policies that do not contain
- Patch management rule type
- Number of VPN virtual servers with unsafe SSL ciphers in use



Trial Version Expiration Date : 2020-11-29

Back

01 REMOTE ACCESS

#	Tool	Description	Severity	Threshold	Value / Threshold	Exceed Time	Last Updated	Last Poll	Actions	Raw Data
1	PulseSecure Secure Connect	Cache Cleaner - Number of devices with Disable AutoComplete of usernames and passwords not enabled	HIGH	0	2<=0	2020/05/06-09:30	2020/05/06-09:30	2020/05/07-09:31		View
2	PulseSecure Secure Connect	Cache Cleaner - Number of devices with Disable AutoComplete of web addresses not enabled	HIGH	0	2<=0	2020/05/06-09:30	2020/05/06-09:30	2020/05/07-09:31		View
3	PulseSecure Secure Connect	Cache Cleaner - Number of devices with Flush all existing AutoComplete passwords not enabled	HIGH	0	2<=0	2020/05/06-09:30	2020/05/06-09:30	2020/05/07-09:31		View
4	PulseSecure Secure Connect	Host Checker - Number of devices with Create Host Checker Connection Control Policy not enabled	HIGH	0	2<=0	2020/05/06-09:30	2020/05/06-09:30	2020/05/07-09:31		View
5	PulseSecure Secure Connect	Host Checker - Number of devices with perform dynamic policy re-evaluation not enabled	MEDIUM	0	2<=0	2020/05/06-09:30	2020/05/06-09:30	2020/05/07-09:31		View
13	F5 APM	Number of Access Policies with no Antivirus Client Check	MEDIUM	0	3<=0	2020/05/05-08:20	2020/05/05-08:42	2020/05/07-09:40		View
14	F5 APM	Number of Access Policies with no Client OS Checks	MEDIUM	0	4<=0	2020/05/05-08:20	2020/05/05-08:42	2020/05/07-09:40		View

Figure 2. **Access Control Domain**

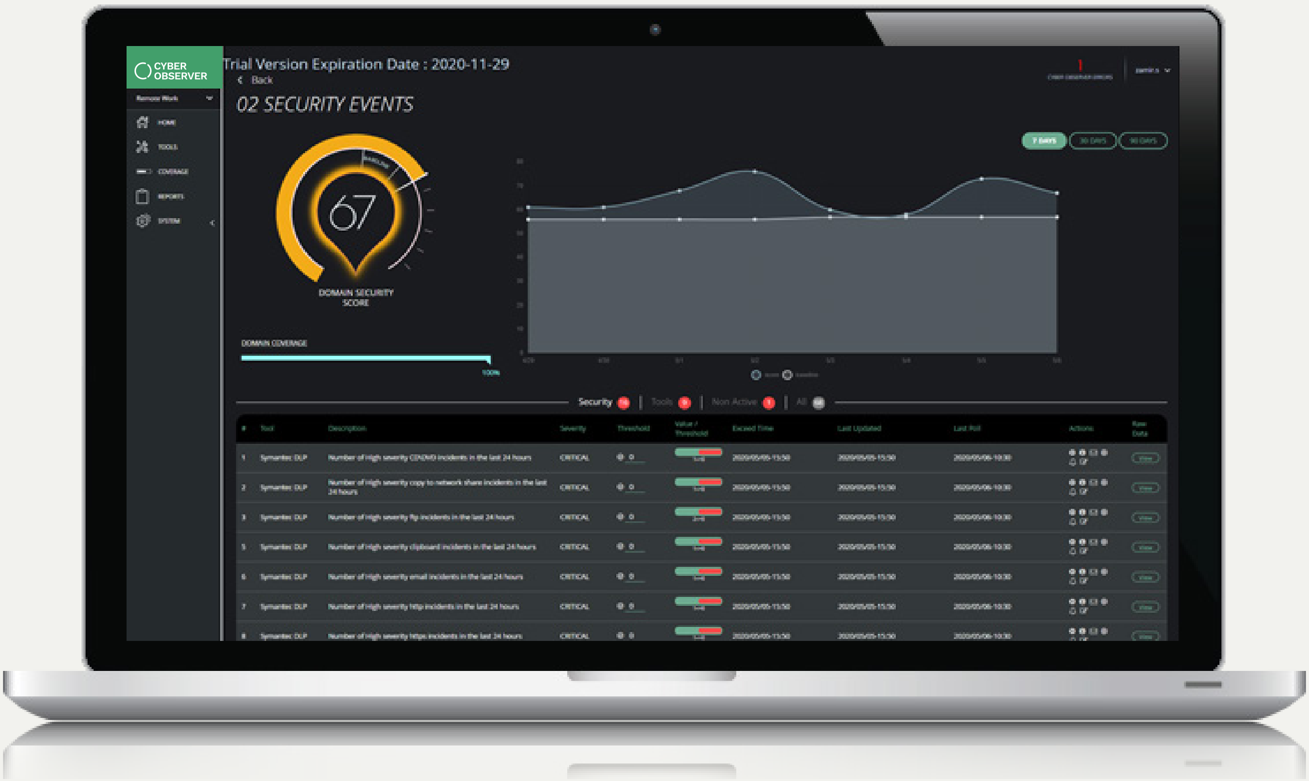
Security events

Event detection time is key to successfully manage security incidents.

Cyber Observer applies automated rules to validate and identify potential incidents in the remote workspace environment.

Examples of CSCs we look for in this domain:

- Number of high severity removable storage device incidents in the last 24 hours
- Number of high severity investigation incidents in the last 24 hours
- Number of high severity http incidents in the last 24 hours
- Number of denial of service attacks detected in the last 90 days
- Number of high severity email incidents in the last 24 hours



Trial Version Expiration Date : 2020-11-29

Back

02 SECURITY EVENTS

#	Tool	Description	Severity	Threshold	Value / Threshold	Exceed Time	Last Updated	Last Poll	Actions	Raw Data
1	Symantec DLP	Number of High severity CD/DVD incidents in the last 24 hours	CRITICAL	0	[illegible]	2020/05/05-15:30	2020/05/05-15:30	2020/05/06-10:30		View
2	Symantec DLP	Number of High severity copy to network share incidents in the last 24 hours	CRITICAL	0	[illegible]	2020/05/05-15:30	2020/05/05-15:30	2020/05/06-10:30		View
3	Symantec DLP	Number of High severity ftp incidents in the last 24 hours	CRITICAL	0	[illegible]	2020/05/05-15:30	2020/05/05-15:30	2020/05/06-10:30		View
5	Symantec DLP	Number of High severity clipboard incidents in the last 24 hours	CRITICAL	0	[illegible]	2020/05/05-15:30	2020/05/05-15:30	2020/05/06-10:30		View
6	Symantec DLP	Number of High severity email incidents in the last 24 hours	CRITICAL	0	[illegible]	2020/05/05-15:30	2020/05/05-15:30	2020/05/06-10:30		View
7	Symantec DLP	Number of High severity http incidents in the last 24 hours	CRITICAL	0	[illegible]	2020/05/05-15:30	2020/05/05-15:30	2020/05/06-10:30		View
8	Symantec DLP	Number of High severity https incidents in the last 24 hours	CRITICAL	0	[illegible]	2020/05/05-15:30	2020/05/05-15:30	2020/05/06-10:30		View

Figure 3. **Security Events Domain**

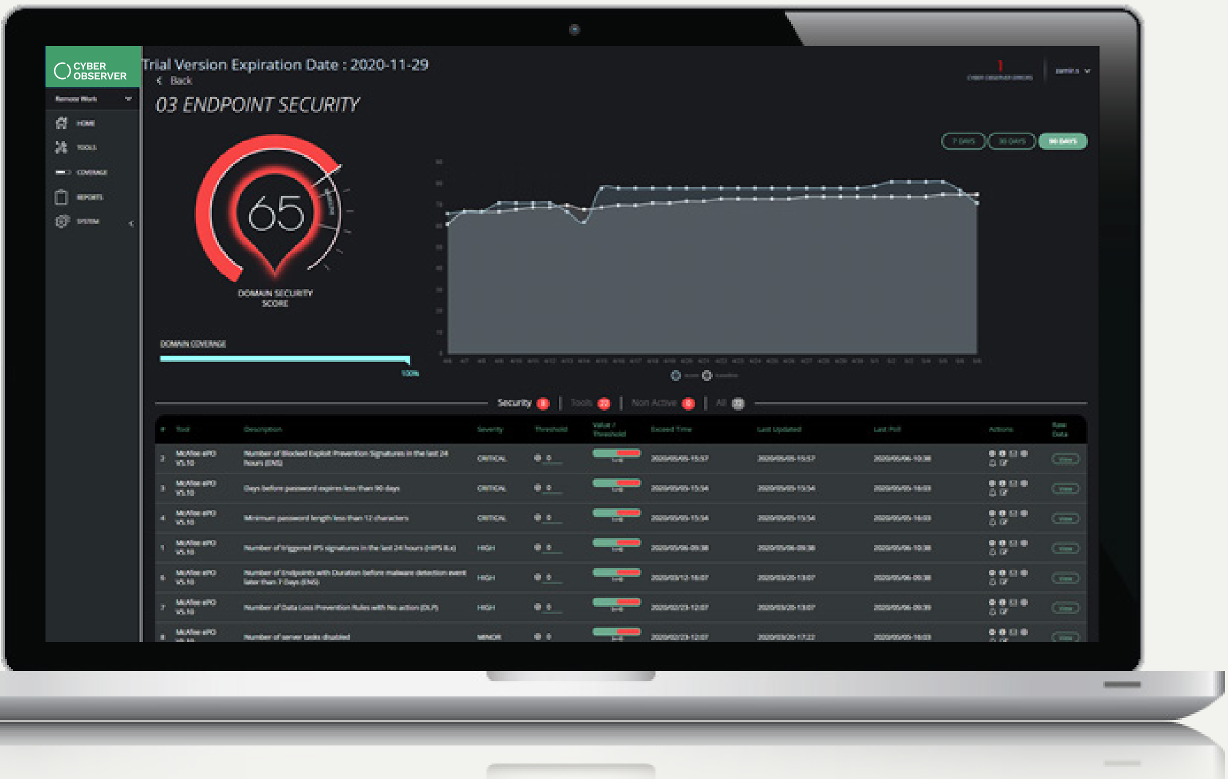
Endpoint security

Working from home means using various personal devices. Unprotected endpoints will undoubtedly serve as ideal vulnerabilities for the next wave of malicious attacks.

Now, more than ever, it is important to gain real-time visibility into your endpoints.

Examples of CSCs we use in this domain for endpoint security management:

- Number of users infected in the last 7 days
- Number of adaptive threat protection events in the last 7 days
- Number of endpoints with access protection disabled
- Number of endpoints with exploit prevention disabled
- Number of endpoints not scanned in the last 7 days
- Number of DLP incidents in the last 24 hours
- Number of triggered IPS signatures in the last 24 hours



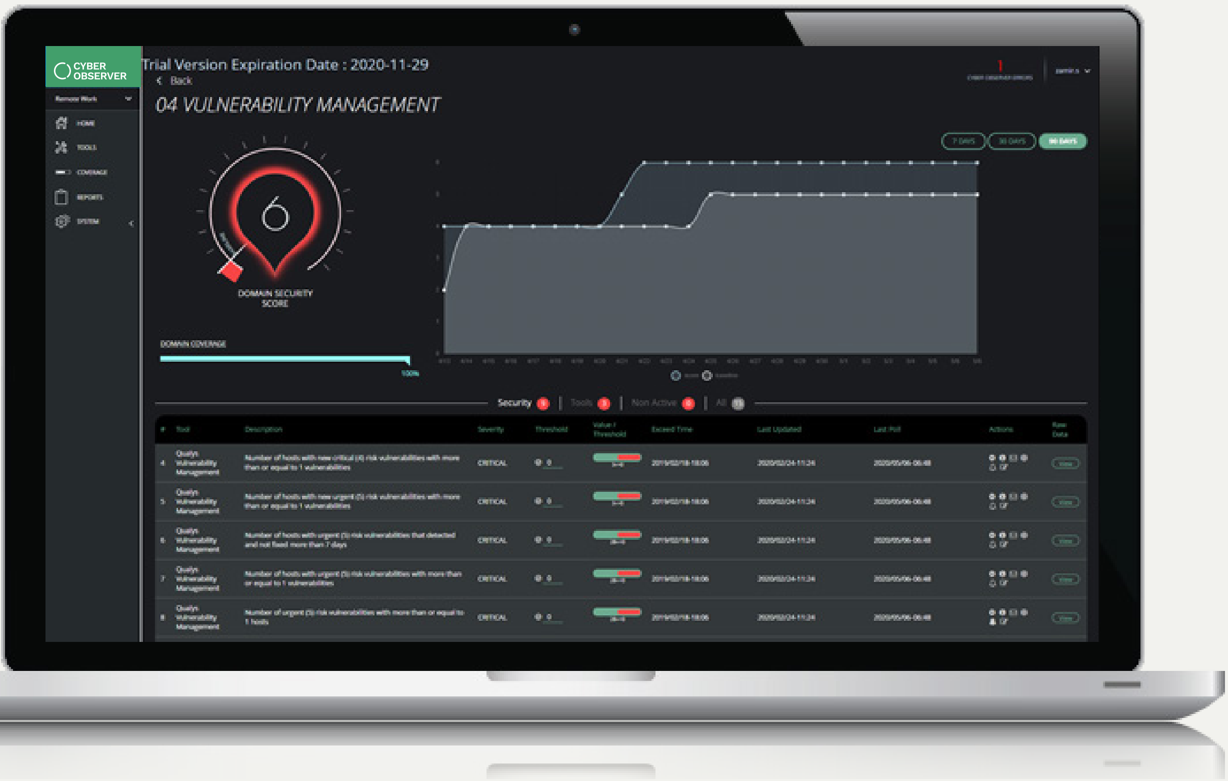
#	Tool	Description	Severity	Threshold	Value / Threshold	Exceed Time	Last Updated	Last Poll	Actions	Raw Data
2	McAfee ePO V5.10	Number of Blocked Exploit Prevention Signatures in the last 24 hours (ENS)	CRITICAL	0		2020/05/05-15:57	2020/05/05-15:57	2020/05/06-10:38		View
3	McAfee ePO V5.10	Days before password expires less than 90 days	CRITICAL	0		2020/05/05-15:54	2020/05/05-15:54	2020/05/05-16:03		View
4	McAfee ePO V5.10	Minimum password length less than 12 characters	CRITICAL	0		2020/05/05-15:54	2020/05/05-15:54	2020/05/05-16:03		View
1	McAfee ePO V5.10	Number of triggered IPS signatures in the last 24 hours (HIPS 8.x)	HIGH	0		2020/05/06-09:38	2020/05/06-09:38	2020/05/06-10:38		View
6	McAfee ePO V5.10	Number of Endpoints with Duration before malware detection event later than 7 Days (ENS)	HIGH	0		2020/03/12-16:07	2020/03/20-13:07	2020/05/06-09:38		View
7	McAfee ePO V5.10	Number of Data Loss Prevention Rules with No action (DLP)	HIGH	0		2020/02/23-12:07	2020/03/20-13:07	2020/05/06-09:39		View
8	McAfee ePO V5.10	Number of server tasks disabled	MINOR	0		2020/02/23-12:07	2020/03/20-17:22	2020/05/05-16:03		View

Figure 4. **Endpoint Security Domain**

Vulnerability assessment

Organizations are increasingly supporting employees working from home by setting up remote working systems, such as virtual desktop servers, remote desktop connections and more.
For this to work, it is essential to have a robust vulnerability assessment view in place, to help protect against security gaps when using the new remote work systems.
Examples of CSCs we look for in this domain:

- Number of hosts with critical (4) risk vulnerabilities that are detected and not fixed more than 7 days
- Number of hosts with urgent (5) risk vulnerabilities that are detected and not fixed more than 7 days
- Number of hosts with new urgent (5) risk vulnerabilities
- Number of hosts not scanned in the last 30 days



Trial Version Expiration Date : 2020-11-29

Back

04 VULNERABILITY MANAGEMENT

#	Tool	Description	Severity	Threshold	Value / Threshold	Exceed Time	Last Updated	Last Poll	Actions	Raw Data
4	Qualys Vulnerability Management	Number of hosts with new critical (4) risk vulnerabilities with more than or equal to 1 vulnerabilities	CRITICAL	0	[illegible]	2019/02/18-18:06	2020/02/24-11:24	2020/05/06-06:48		View
5	Qualys Vulnerability Management	Number of hosts with new urgent (5) risk vulnerabilities with more than or equal to 1 vulnerabilities	CRITICAL	0	[illegible]	2019/02/18-18:06	2020/02/24-11:24	2020/05/06-06:48		View
6	Qualys Vulnerability Management	Number of hosts with urgent (5) risk vulnerabilities that detected and not fixed more than 7 days	CRITICAL	0	[illegible]	2019/02/18-18:06	2020/02/24-11:24	2020/05/06-06:48		View
7	Qualys Vulnerability Management	Number of hosts with urgent (5) risk vulnerabilities with more than or equal to 1 vulnerabilities	CRITICAL	0	[illegible]	2019/02/18-18:06	2020/02/24-11:24	2020/05/06-06:48		View
8	Qualys Vulnerability Management	Number of urgent (5) risk vulnerabilities with more than or equal to 1 hosts	CRITICAL	0	[illegible]	2019/02/18-18:06	2020/02/24-11:24	2020/05/06-06:48		View

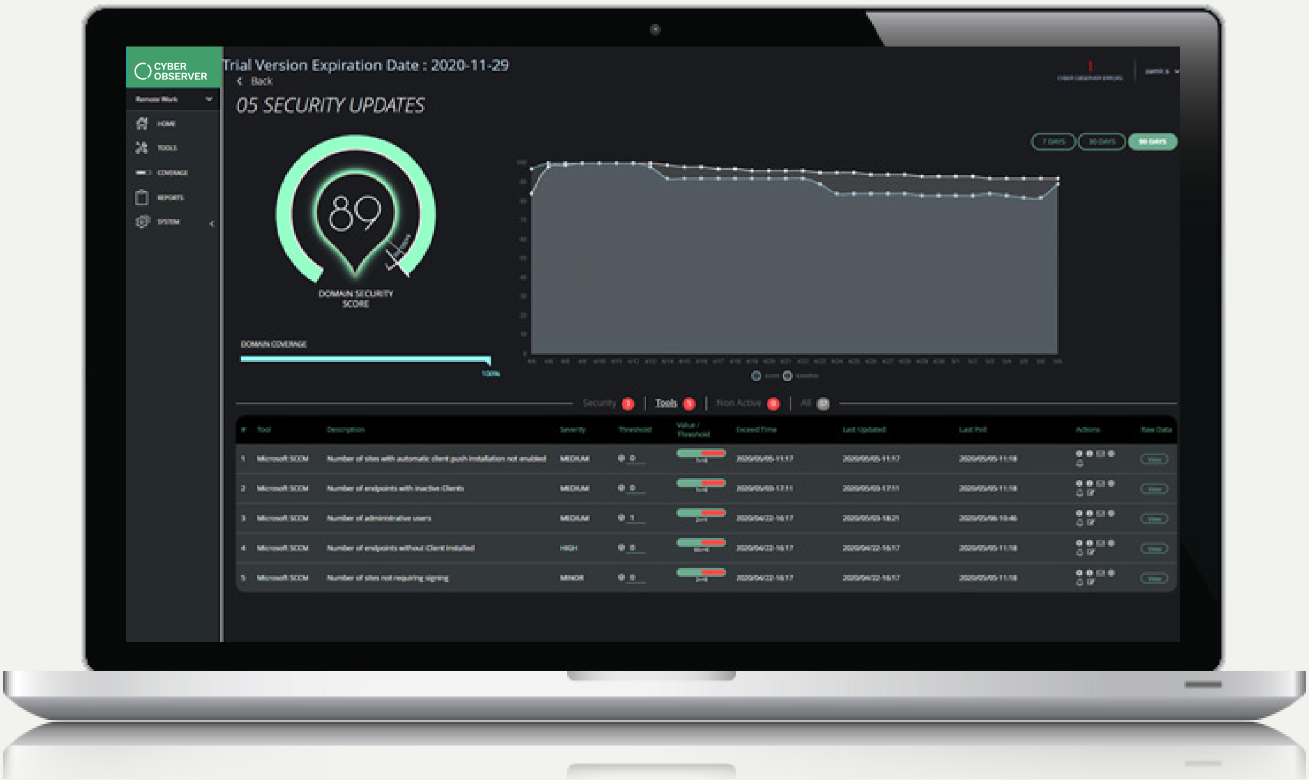
Figure 5. **Vulnerability Assessment Domain**

Security updates

Security updates are one of the most important and effective actions you can do to protect your systems and network. Cyber Observer's Security Updates domain provides essential information to efficiently maintain your patch management.

Examples of CSCs we look for in this domain:

- Number of servers requiring critical severity security updates with release date more than 7 days
- Number of workstations with end-of-life Internet Explorer versions
- Number of endpoints without client installed
- Number of endpoints with SQL server 2005 products (end of extended support)



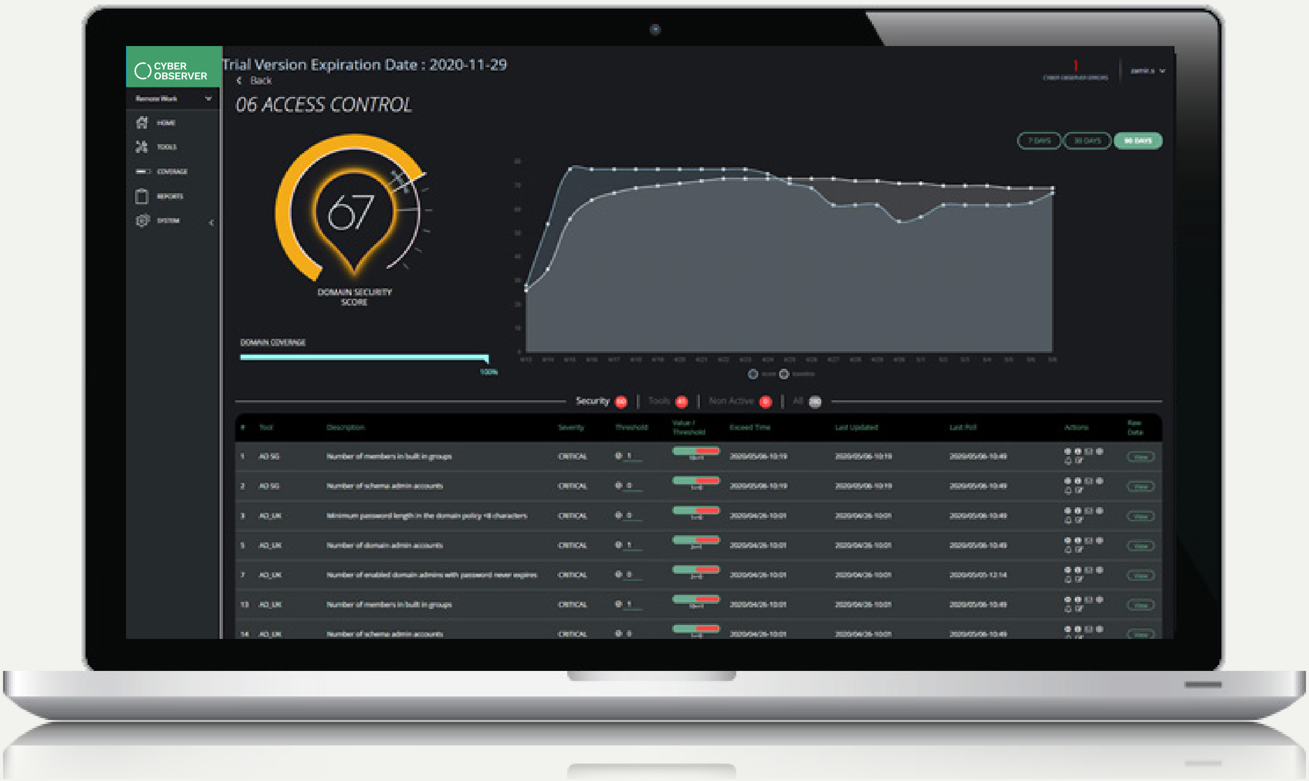
#	Tool	Description	Severity	Threshold	Value / Threshold	Exceed Time	Last Updated	Last Poll	Actions	Raw Data
1	Microsoft SCCM	Number of sites with automatic client push installation not enabled	MEDIUM	0		2020/05/05-11:17	2020/05/05-11:17	2020/05/05-11:18		View
2	Microsoft SCCM	Number of endpoints with inactive Clients	MEDIUM	0		2020/05/03-17:11	2020/05/03-17:11	2020/05/05-11:18		View
3	Microsoft SCCM	Number of administrative users	MEDIUM	1		2020/04/22-16:17	2020/05/03-18:21	2020/05/06-10:46		View
4	Microsoft SCCM	Number of endpoints without Client installed	HIGH	0		2020/04/22-16:17	2020/04/22-16:17	2020/05/05-11:18		View
5	Microsoft SCCM	Number of sites not requiring signing	MINOR	0		2020/04/22-16:17	2020/04/22-16:17	2020/05/05-11:18		View

Figure 6. **Security Updates Domain**

Access control

Access control monitoring is key to data security. Employees may be connecting from a variety of personal devices - laptops, tablets, and Android and iPhone mobile devices - so you must deploy policies that encompass appropriate access to company data, whether employees access through corporate-owned or personal devices.
Examples of CSCs we look for in this domain:

- Number of domain admin accounts
- Number of enabled accounts with password not required
- Number of locked domain admin users due to invalid login attempts in the last 7 days
- Number of schema admin accounts
- Number of enabled domain admins with never-expiring passwords



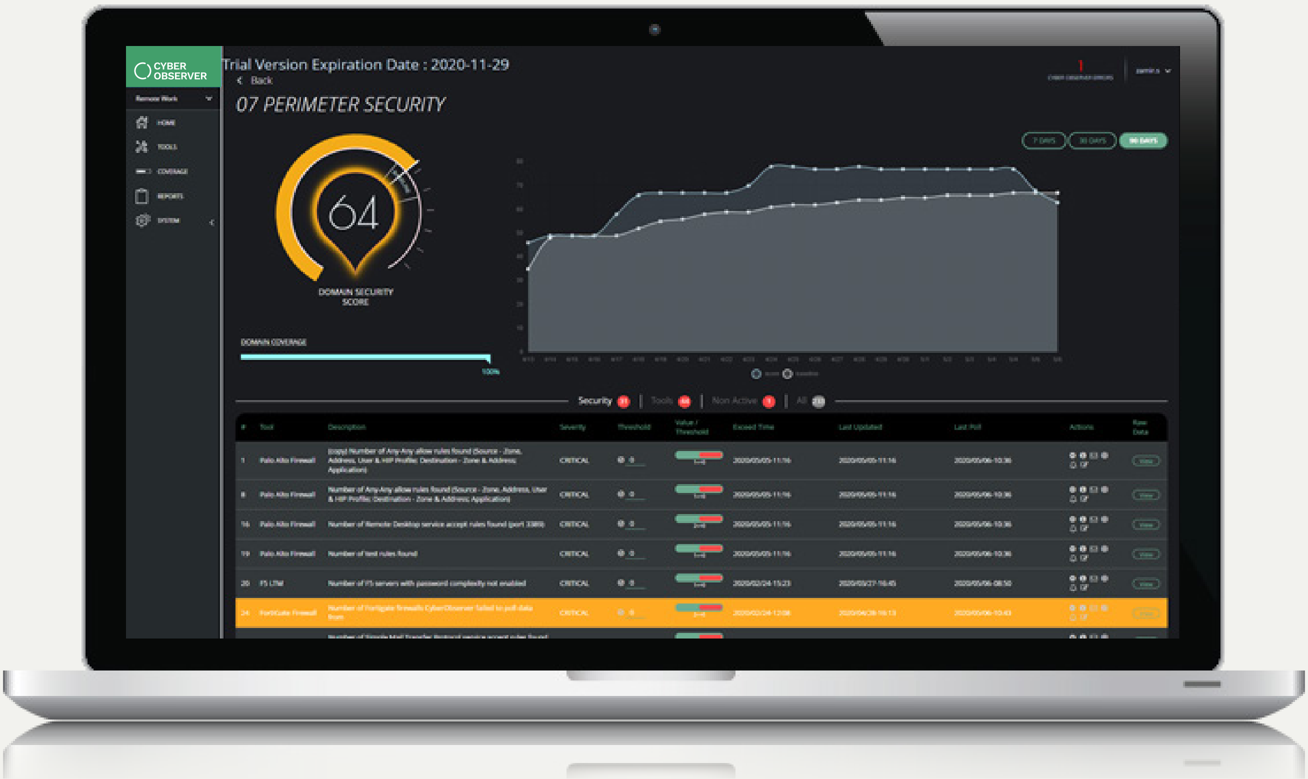
#	Tool	Description	Severity	Threshold	Value / Threshold	Exceed Time	Last Updated	Last Poll	Actions	Raw Data
1	AD SG	Number of members in built in groups	CRITICAL	1		2020/05/06-10:19	2020/05/06-10:19	2020/05/06-10:49		View
2	AD SG	Number of schema admin accounts	CRITICAL	0		2020/05/06-10:19	2020/05/06-10:19	2020/05/06-10:49		View
3	AD_UK	Minimum password length in the domain policy <8 characters	CRITICAL	0		2020/04/26-10:01	2020/04/26-10:01	2020/05/06-10:49		View
5	AD_UK	Number of domain admin accounts	CRITICAL	1		2020/04/26-10:01	2020/04/26-10:01	2020/05/06-10:49		View
7	AD_UK	Number of enabled domain admins with password never expires	CRITICAL	0		2020/04/26-10:01	2020/04/26-10:01	2020/05/05-12:14		View
13	AD_UK	Number of members in built in groups	CRITICAL	1		2020/04/26-10:01	2020/04/26-10:01	2020/05/06-10:49		View
14	AD_UK	Number of schema admin accounts	CRITICAL	0		2020/04/26-10:01	2020/04/26-10:01	2020/05/06-10:49		View

Figure 7. **Access Control Domain**

Perimeter security

Maintaining an accurate, up-to-date picture of organizational risk becomes more important as workers move from traditional offices to work-from-home environments. Laptops leaving the safety of the office security perimeter often have sensitive information and provide users with access to critical systems. Organizations must maintain a clear understanding of the security posture of these systems, regardless of where they are located. Cyber Observer Perimiter Security domain helps you to look for:

- Number of any-any allow rules found
- Number of remote desktop service accept rules found
- Number of enabled test rules found
- Number of temporary rules found
- Number of DoS protection profiles with bot signatures malicious categories action not set to block
- Number of systems with license expired



Trial Version Expiration Date : 2020-11-29

07 PERIMETER SECURITY

#	Tool	Description	Severity	Threshold	Value / Threshold	Exceed Time	Last Updated	Last Poll	Actions	Raw Data
1	Palo Alto Firewall	(copy) Number of Any-Any allow rules found (Source - Zone, Address, User & HIP Profile; Destination - Zone & Address; Application)	CRITICAL	0		2020/05/05-11:16	2020/05/05-11:16	2020/05/06-10:36		View
8	Palo Alto Firewall	Number of Any-Any allow rules found (Source - Zone, Address, User & HIP Profile; Destination - Zone & Address; Application)	CRITICAL	0		2020/05/05-11:16	2020/05/05-11:16	2020/05/06-10:36		View
16	Palo Alto Firewall	Number of Remote Desktop service accept rules found (port 3389)	CRITICAL	0		2020/05/05-11:16	2020/05/05-11:16	2020/05/06-10:36		View
19	Palo Alto Firewall	Number of test rules found	CRITICAL	0		2020/05/05-11:16	2020/05/05-11:16	2020/05/06-10:36		View
20	F5 LTM	Number of F5 servers with password complexity not enabled	CRITICAL	0		2020/02/24-15:23	2020/03/27-16:45	2020/05/06-08:50		View
24	FortiGate Firewall	Number of Fortigate firewalls CyberObserver failed to poll data from	CRITICAL	0		2020/02/24-12:08	2020/04/28-16:13	2020/05/06-10:43		View
		Number of Simple Mail Transfer Protocol service accept rules found								

Figure 8. **Perimeter Security Domain**

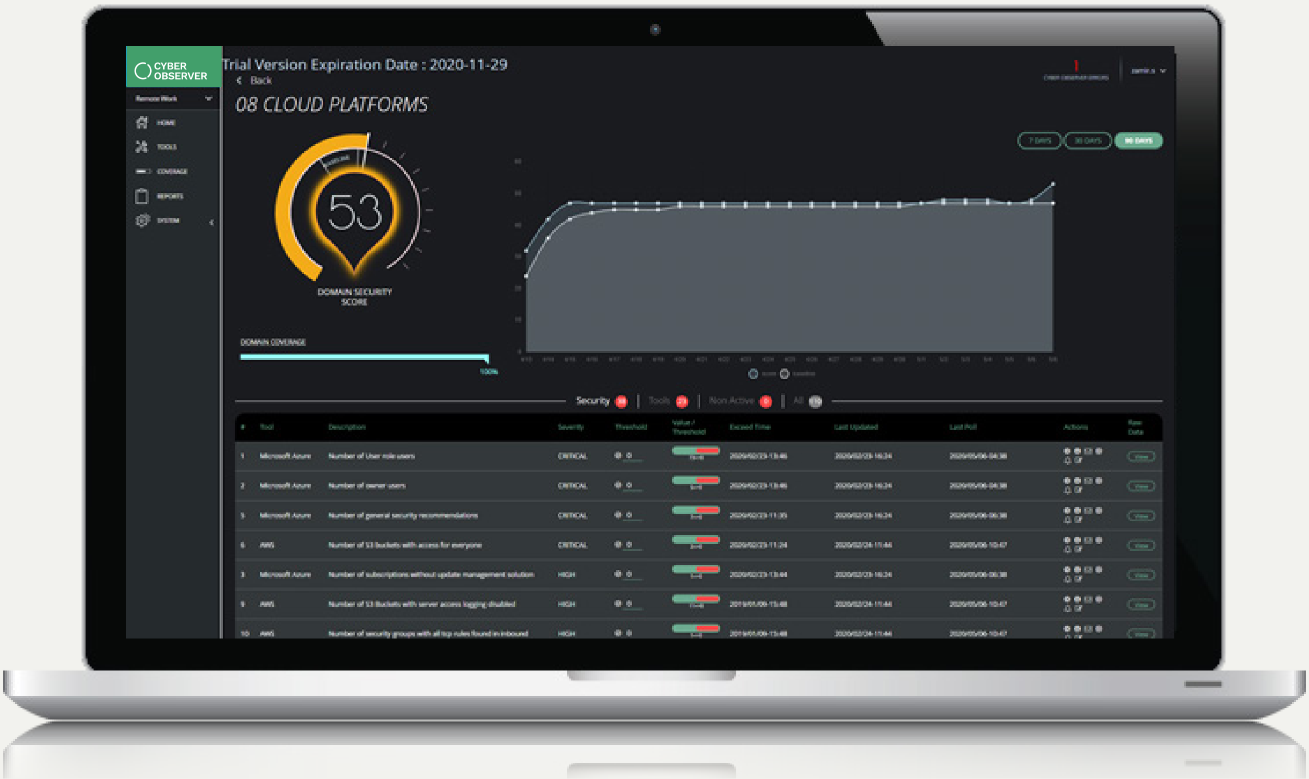
Cloud platforms

Given COVID-19 circumstances, organizations are looking to cloud services to ensure they can continue to operate remotely.

Now more than ever, cloud security must be a top priority, to ensure proper protection for organizations moving their resources to cloud platforms.

Examples of CSCs we look for in this domain:

- Number of Windows virtual machines without endpoint protection
- Number of S3 buckets with access for everyone
- Number of subscriptions with advanced security turned number of accounts with root account MFA disabled
- Number of users with MFA disabled
- Number of security groups with all TCP rules found in outbound
- Number of Linux virtual machines without anti-malware protection



Trial Version Expiration Date : 2020-11-29

08 CLOUD PLATFORMS

#	Tool	Description	Severity	Threshold	Value / Threshold	Exceed Time	Last Updated	Last Poll	Actions	Raw Data
1	Microsoft Azure	Number of User role users	CRITICAL	0	[illegible]	2020/02/23 13:46	2020/02/23 16:24	2020/05/06 04:38		View
2	Microsoft Azure	Number of owner users	CRITICAL	0	[illegible]	2020/02/23 13:46	2020/02/23 16:24	2020/05/06 04:38		View
5	Microsoft Azure	Number of general security recommendations	CRITICAL	0	[illegible]	2020/02/23 11:35	2020/02/23 16:24	2020/05/06 06:38		View
6	AWS	Number of S3 buckets with access for everyone	CRITICAL	0	[illegible]	2020/02/23 11:24	2020/02/24 11:44	2020/05/06 10:47		View
3	Microsoft Azure	Number of subscriptions without update management solution	HIGH	0	[illegible]	2020/02/23 13:44	2020/02/23 16:24	2020/05/06 06:38		View
9	AWS	Number of S3 Buckets with server access logging disabled	HIGH	0	[illegible]	2019/01/09 13:48	2020/02/24 11:44	2020/05/06 10:47		View
10	AWS	Number of security groups with all tcp rules found in inbound	HIGH	0	[illegible]	2019/01/09 13:48	2020/02/24 11:44	2020/05/06 10:47		View

Figure 9. **Cloud Platforms Domain**

Managing cybersecurity remotely together

Cybersecurity continues to be mission-critical to organization, enabling business continuity. Most importantly, it provides the peace of mind that employees and customers are protected and can continue focusing on the things that matter most.

About Cyber Observer

Cyber Observer is a 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. The comprehensive information empowers CISOs and executives to make insightful and timely decisions to ensure the cybersecurity of their 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 continuously improve enterprise security posture and maturity.