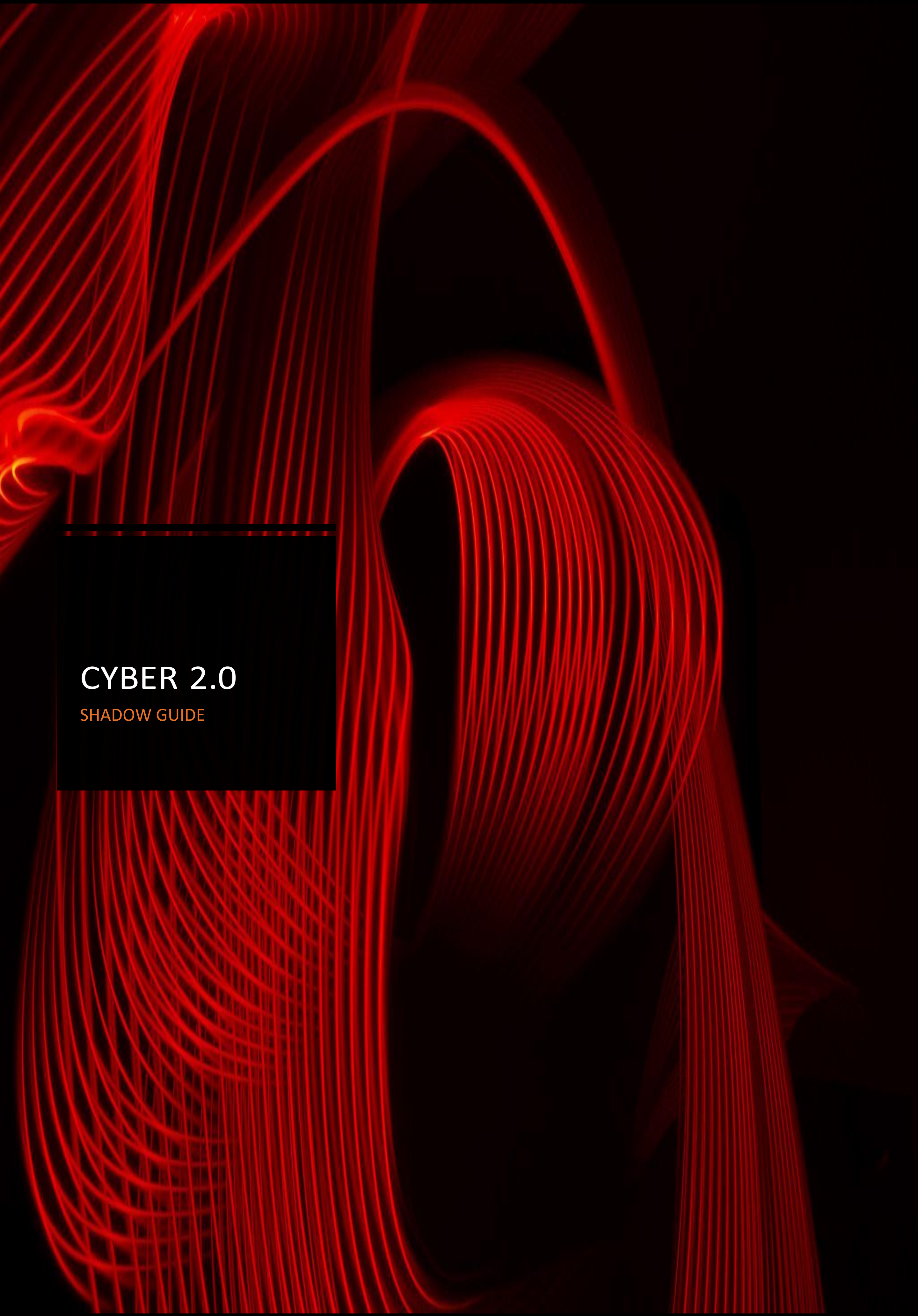


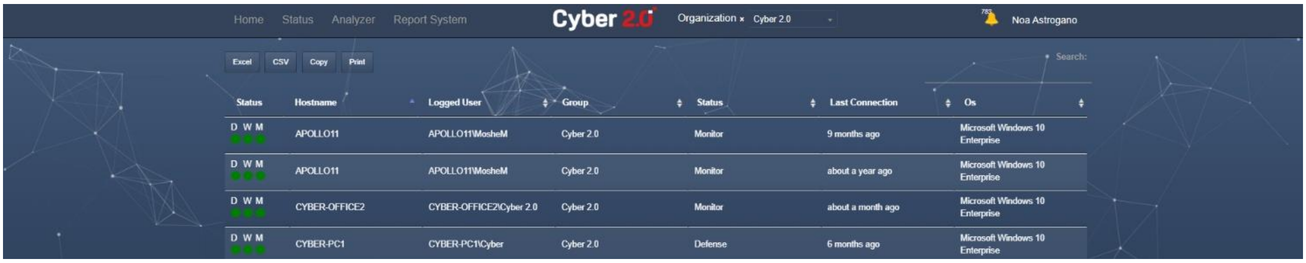
CYBER 2.0

SHADOW GUIDE

About

- The Shadow system is Cyber 2.0 Analyzing System, that enables you to view, analyze and understand, the apps, processes and end-points behavior in your network.
- The system helps to mitigate attacks and receive various alerts regarding malicious activities in the network.

Home Tab:



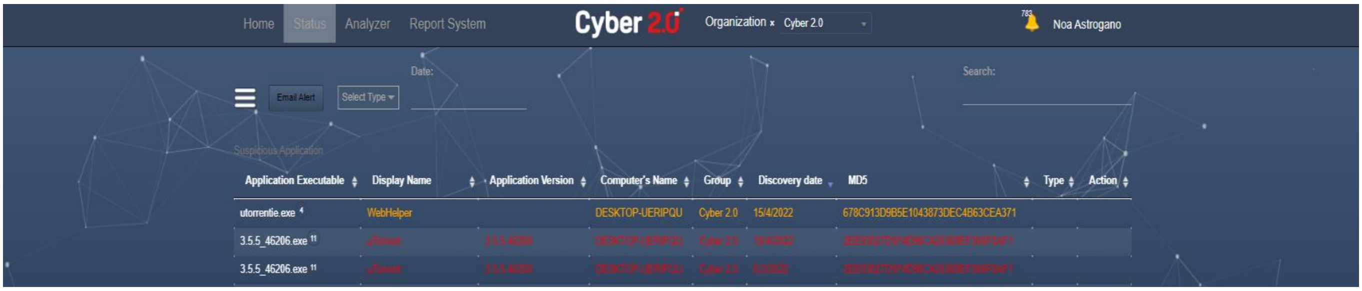
Status	Hostname	Logged User	Group	Status	Last Connection	Os
D W M ● ● ●	APOLLO11	APOLLO11\MosheM	Cyber 2.0	Monitor	9 months ago	Microsoft Windows 10 Enterprise
D W M ● ● ●	APOLLO11	APOLLO11\MosheM	Cyber 2.0	Monitor	about a year ago	Microsoft Windows 10 Enterprise
D W M ● ● ●	CYBER-OFFICE2	CYBER-OFFICE2\Cyber 2.0	Cyber 2.0	Monitor	about a month ago	Microsoft Windows 10 Enterprise
D W M ● ● ●	CYBER-PC1	CYBER-PC1\Cyber	Cyber 2.0	Defense	6 months ago	Microsoft Windows 10 Enterprise

- Displays a list of protected computers in the organization that are connected to Cyber 2.0 cloud.
- Use the built-in search bar on the top right corner in order to access a specific computer.
- The Information can be Printed, copied or exported to excel or CSV format.
- Clicking on any computer, will display all the apps used by this specific computer.
- Use the filter bar to arrange information according to various parameters, such as date or hostname.

Status Tab:

- <u>The Status tab contains three sub-tabs:</u>

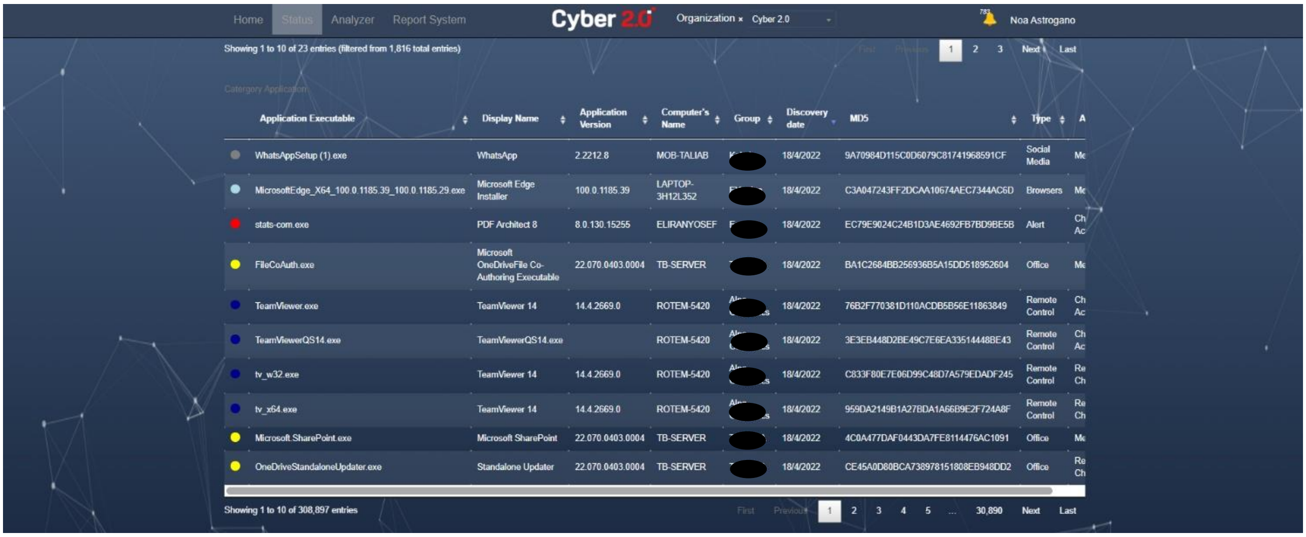
  1. **<u>Suspicious Applications:</u>**



Application Executable	Display Name	Application Version	Computer's Name	Group	Discovery date	MD5	Type	Action
utorrentie.exe [4]	WebHelper		DESKTOP-UERIPQU	Cyber 2.0	15/4/2022	678C913D9B5E1043873DEC4B63CEA371		
3.5.5_46206.exe [11]	uTorrent	3.5.5.46206	DESKTOP-UERIPQU	Cyber 2.0	[illegible]	[illegible]		
3.5.5_46206.exe [11]	uTorrent	3.5.5.46206	DESKTOP-UERIPQU	Cyber 2.0	[illegible]	[illegible]		

- ❖ Displays all suspicious applications that were scanned by cyber-2.0.
- ❖ Displays Information regarding the suspicious app, such as: Application Executable, Display name, Application version, Computer's name, Discovery date, MD5.
- ❖ The color on the row indicates the severity of the alert.
- ❖ The Type and Actions columns on the table, indicates the category of the app and the recommend Action.
- ❖ Click on the 'Application Executable' Colum of any alert will open a link to virus total for more information regarding the app.

2. Category (Interesting Applications):



Showing 1 to 10 of 23 entries (filtered from 1,816 total entries)

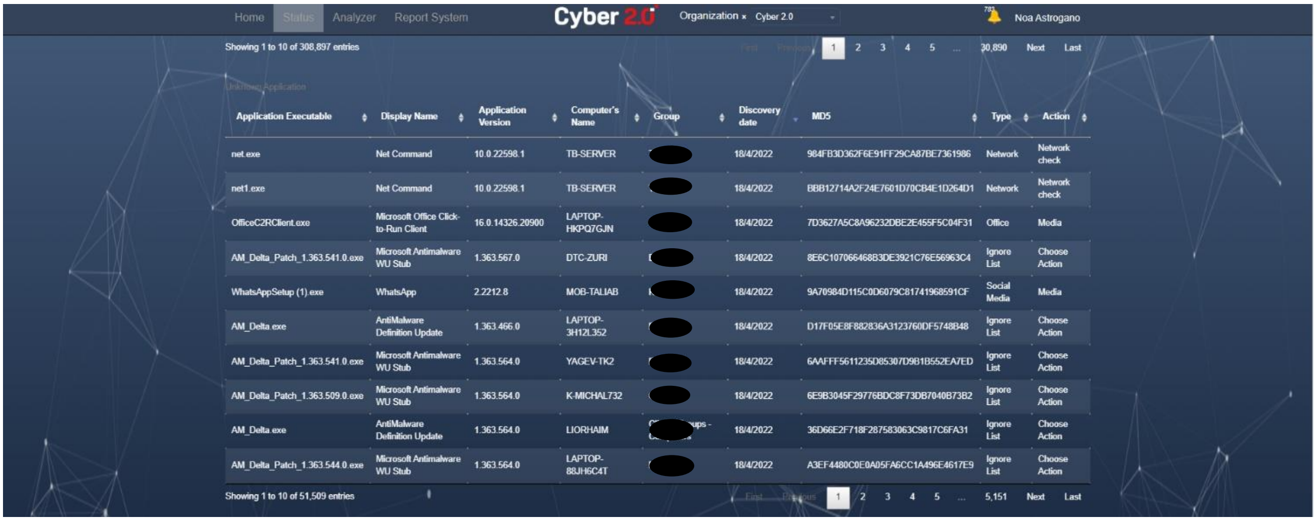
Catergory Application

	Application Executable	Display Name	Application Version	Computer's Name	Group	Discovery date	MD5	Type	A
●	WhatsAppSetup (1).exe	WhatsApp	2.2212.8	MOB-TALIAB	[redacted]	18/4/2022	9A70984D115C0D6079C81741968591CF	Social Media	Me
●	MicrosoftEdge_X64_100.0.1185.39_100.0.1185.29.exe	Microsoft Edge Installer	100.0.1185.39	LAPTOP-3H12L352	[redacted]	18/4/2022	C3A047243FF2DCAA10674AEC7344AC6D	Browsers	Me
●	stats-com.exe	PDF Architect 8	8.0.130.15255	ELIRANYOSEF	[redacted]	18/4/2022	EC79E9024C24B1D3AE4692FB7BD9BE5B	Alert	Ch Ac
●	FileCoAuth.exe	Microsoft OneDriveFile Co-Authoring Executable	22.070.0403.0004	TB-SERVER	[redacted]	18/4/2022	BA1C2684BB256936B5A15DD518952604	Office	Me
●	TeamViewer.exe	TeamViewer 14	14.4.2669.0	ROTEM-5420	[redacted]	18/4/2022	76B2F770381D110ACDB5B56E11863849	Remote Control	Ch Ac
●	TeamViewerQS14.exe	TeamViewerQS14.exe		ROTEM-5420	[redacted]	18/4/2022	3E3EB448D2BE49C7E6EA33514448BE43	Remote Control	Ch Ac
●	tv_w32.exe	TeamViewer 14	14.4.2669.0	ROTEM-5420	[redacted]	18/4/2022	C833F80E7E06D99C48D7A579EDADF245	Remote Control	Re Ch
●	tv_x64.exe	TeamViewer 14	14.4.2669.0	ROTEM-5420	[redacted]	18/4/2022	959DA2149B1A27BDA1A66B9E2F724A8F	Remote Control	Re Ch
●	Microsoft.SharePoint.exe	Microsoft SharePoint	22.070.0403.0004	TB-SERVER	[redacted]	18/4/2022	4C0A477DAF0443DA7FE8114476AC1091	Office	Me
●	OneDriveStandaloneUpdater.exe	Standalone Updater	22.070.0403.0004	TB-SERVER	[redacted]	18/4/2022	CE45A0D80BCA738978151808EB948DD2	Office	Re Ch

Showing 1 to 10 of 308,897 entries

- ❖ Displays interesting applications that were scanned by cyber 2.0
- ❖ The applications are sorted by various colors representing these main categories – Remote control apps, Media, Games, Network, browsers and more.
- ❖ To see the color of each category, press the button 'Email alert' on the top left.

3. Unknown Applications:



Showing 1 to 10 of 308,897 entries

First Previous 1 2 3 4 5 … 30,890 Next Last

Application Executable	Display Name	Application Version	Computer's Name	Group	Discovery date	MD5	Type	Action
net.exe	Net Command	10.0.22598.1	TB-SERVER	[redacted]	18/4/2022	984FB3D362F6E91FF29CA87BE7361986	Network	Network check
net1.exe	Net Command	10.0.22598.1	TB-SERVER	[redacted]	18/4/2022	BBB12714A2F24E7601D70CB4E1D264D1	Network	Network check
OfficeC2RClient.exe	Microsoft Office Click-to-Run Client	16.0.14326.20900	LAPTOP-HKPQ7GJN	[redacted]	18/4/2022	7D3627A5C8A96232DBE2E455F5C04F31	Office	Media
AM_Delta_Patch_1.363.541.0.exe	Microsoft Antimalware WU Stub	1.363.567.0	DTC-ZURI	[redacted]	18/4/2022	8E6C107066468B3DE3921C76E56963C4	Ignore List	Choose Action
WhatsAppSetup (1).exe	WhatsApp	2.2212.8	MOB-TALIAB	[redacted]	18/4/2022	9A70984D115C0D6079C81741968591CF	Social Media	Media
AM_Delta.exe	AntiMalware Definition Update	1.363.466.0	LAPTOP-3H12L352	[redacted]	18/4/2022	D17F05E8F882836A3123760DF5748B48	Ignore List	Choose Action
AM_Delta_Patch_1.363.541.0.exe	Microsoft Antimalware WU Stub	1.363.564.0	YAGEV-TK2	[redacted]	18/4/2022	6AAFFF5611235D85307D9B1B552EA7ED	Ignore List	Choose Action
AM_Delta_Patch_1.363.509.0.exe	Microsoft Antimalware WU Stub	1.363.564.0	K-MICHAL732	[redacted]	18/4/2022	6E9B3045F29776BDC8F73DB7040B73B2	Ignore List	Choose Action
AM_Delta.exe	AntiMalware Definition Update	1.363.564.0	LIORHAIM	[redacted]	18/4/2022	36D66E2F718F287583063C9817C6FA31	Ignore List	Choose Action
AM_Delta_Patch_1.363.544.0.exe	Microsoft Antimalware WU Stub	1.363.564.0	LAPTOP-88JH6C4T	[redacted]	18/4/2022	A3EF4480C0E0A05FA6CC1A496E4617E9	Ignore List	Choose Action

Showing 1 to 10 of 51,509 entries

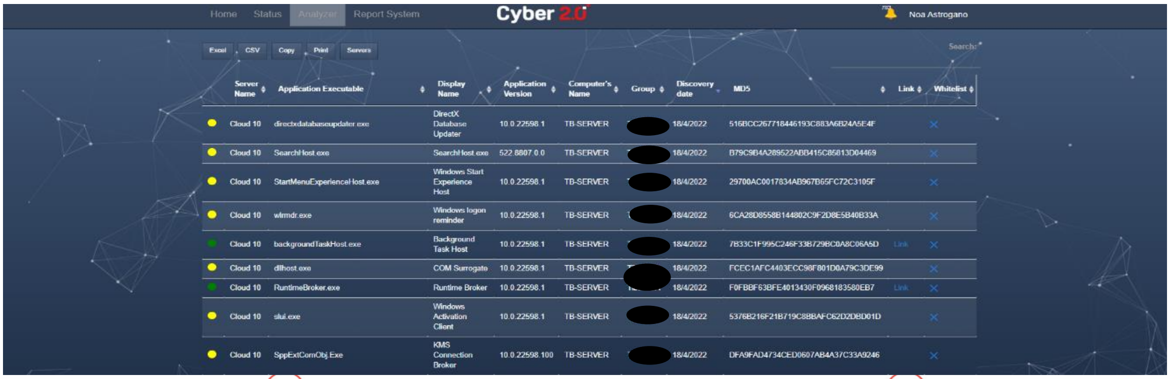
First Previous 1 2 3 4 5 … 5,151 Next Last

- Displays new and unknown applications and updates that were scanned by cyber 2.0.

More features of status tab:

- The status tab has a built-in search bar that can be accessed on the top right corner.
- Use the filter bar to arrange information according to date or type on the top left corner.
- Use the menu Icon on the top left corner to add the category or unknown applications.
- Email Alert feature: Set a personal email alert on the top left corner. the alert will notify you via email when an app from a specific category was active in your organization. Choose the desired category, and set the time and priority.

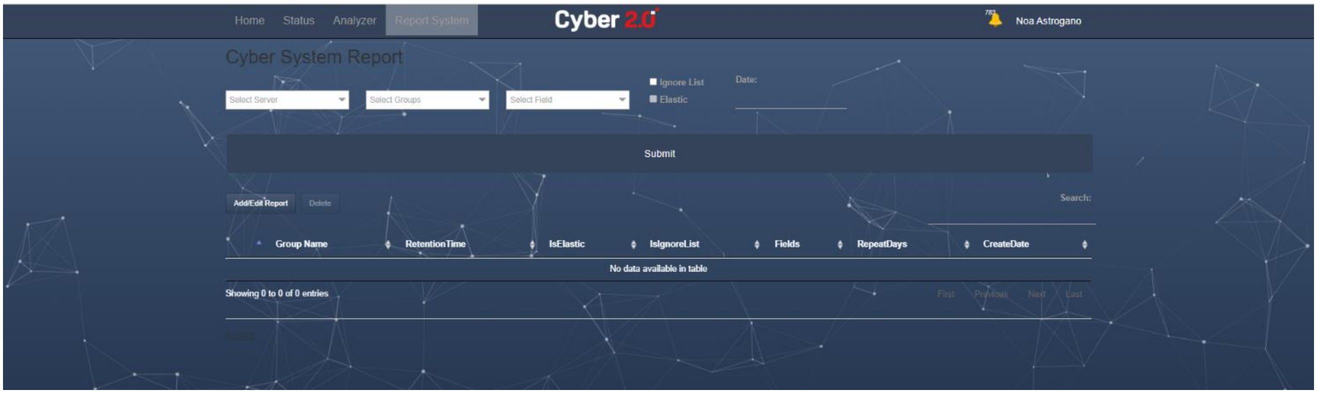
Analyzer Tab:



	Server Name	Application Executable	Display Name	Application Version	Computer's Name	Group	Discovery date	MD5	Link	Whitelist
●	Cloud 10	directxdatabaseupdater.exe	DirectX Database Updater	10.0.22598.1	TB-SERVER	[redacted]	18/4/2022	516BCC267718446193C883A6B24A5E4F		×
●	Cloud 10	SearchHost.exe	SearchHost.exe	522.8807.0.0	TB-SERVER	[redacted]	18/4/2022	B79C9B4A289522ABB415C85813D04469		×
●	Cloud 10	StartMenuExperienceHost.exe	Windows Start Experience Host	10.0.22598.1	TB-SERVER	[redacted]	18/4/2022	29700AC0017834AB967B65FC72C3105F		×
●	Cloud 10	wlrmdr.exe	Windows logon reminder	10.0.22598.1	TB-SERVER	[redacted]	18/4/2022	6CA28D8558B144802C9F2D8E5B40B33A		×
●	Cloud 10	backgroundTaskHost.exe	Background Task Host	10.0.22598.1	TB-SERVER	[redacted]	18/4/2022	7B33C1F995C246F33B729BC0A8C06A5D	Link	×
●	Cloud 10	dllhost.exe	COM Surrogate	10.0.22598.1	TB-SERVER	[redacted]	18/4/2022	FCEC1AFC4403ECC98F801D0A79C3DE99		×
●	Cloud 10	RuntimeBroker.exe	Runtime Broker	10.0.22598.1	TB-SERVER	[redacted]	18/4/2022	F0FBBF63BFE4013430F0968183580EB7	Link	×
●	Cloud 10	slui.exe	Windows Activation Client	10.0.22598.1	TB-SERVER	[redacted]	18/4/2022	5376B216F21B719C8BBAFC62D2DBD01D		×
●	Cloud 10	SppExtComObj.Exe	KMS Connection Broker	10.0.22598.100	TB-SERVER	[redacted]	18/4/2022	DFA9FAD4734CED0607AB4A37C33A9246		×

- The Analyzer is a super inventory, that allows you to view all the apps that were active inside the organization since Cyber 2.0 was deployed.
- The Information can be Printed, copied or exported to excel or CSV format.

Report system:



Cyber System Report

Group Name	RetentionTime	IsElastic	IsIgnoreList	Fields	RepeatDays	CreateDate
No data available in table						

Showing 0 to 0 of 0 entries

- Enable you to generate custom reports from the system.
- Choose which fields will be display in the report on the top filter bar.
- Choose the requested dates.
- Checking the elastic box will generate an additional report, consisting of network flows, please (note that the elastic report is large)
- Set an auto report that will be sent to your Email, on the 'Add/Edit Report' option on the left corner above the table.