Cynet

AUTONOMOUS BREACH PROTECTION

Cynet 360

WHITELIST FEATURE

OVERVIEW

Cynet Whitelisting allows Cynet users to exclude certain activities from generating alerts in the Cynet Console. Moreover, by using the whitelisting feature, a user can set a list of applications and parameters that are authorized to run in Cynet's environment.

In order to avoid alerts regarding these activities, the whitelisting configuration will apply to a specific alert or all alerts, based on user's analysis and discretion.

For example, if you have proprietary software or internal scripts (e.g. login scripts), a user can exclude Cynet detection by configuring a Whitelisting profile, and in turn Cynet will not generate alerts regarding these activities.

NOTES

- This feature is only available from Cynet Version 3.4.3 and above.
- The whitelisting feature supports different exclusions scenarios, please see Appendix A for information on the feature availability per each version.
- The whitelisting feature can be applied only on Windows OS.
- The best practice approach is to create a new profile for each activity, it is easier to manage the whitelisting profiles this way.

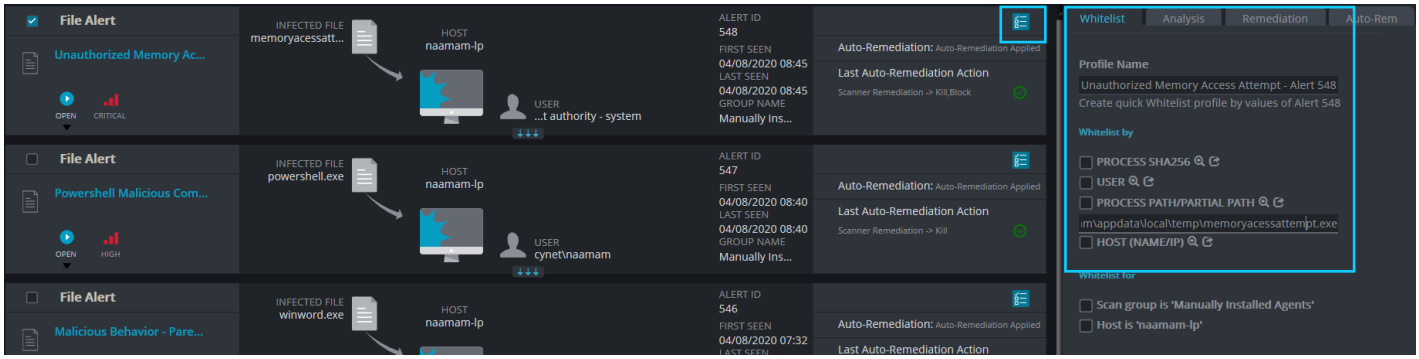
EXCLUDING AN ALERT

There are two ways to exclude an alert:

- Excluding an alert directly from the alert's dashboard (limited parameters).
- Creating an advanced whitelisting profile through the Cynet Settings.

Whitelist Alerts through the Alerts Dashboard

1. Check the alert you want to whitelist
2. Go to Actions (on the top-right corner)
3. On the left panel, you will see the "Whitelist" Tab:

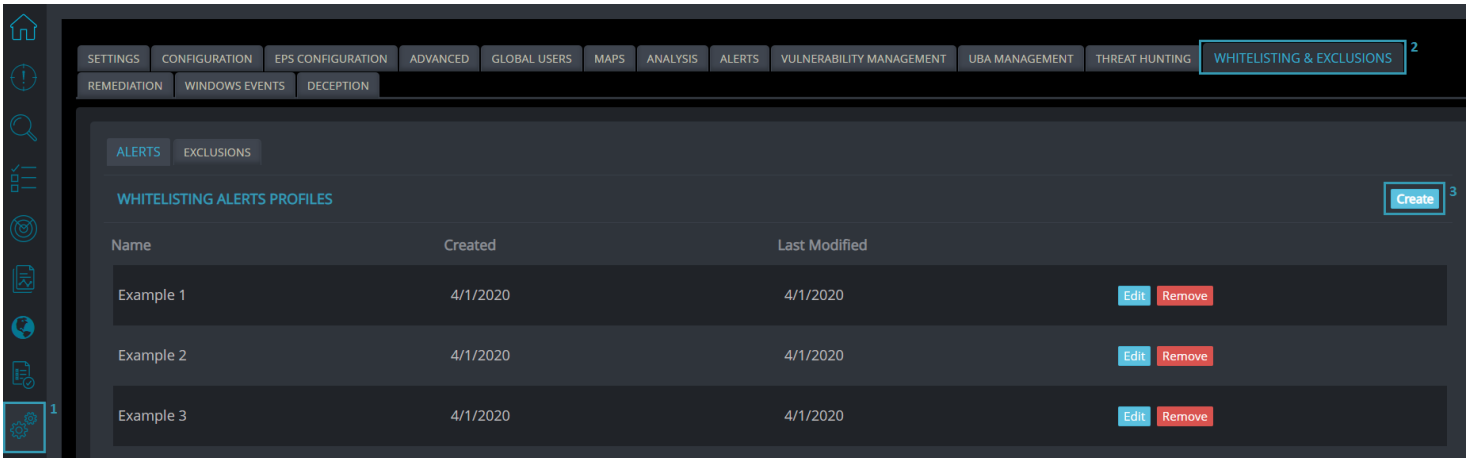


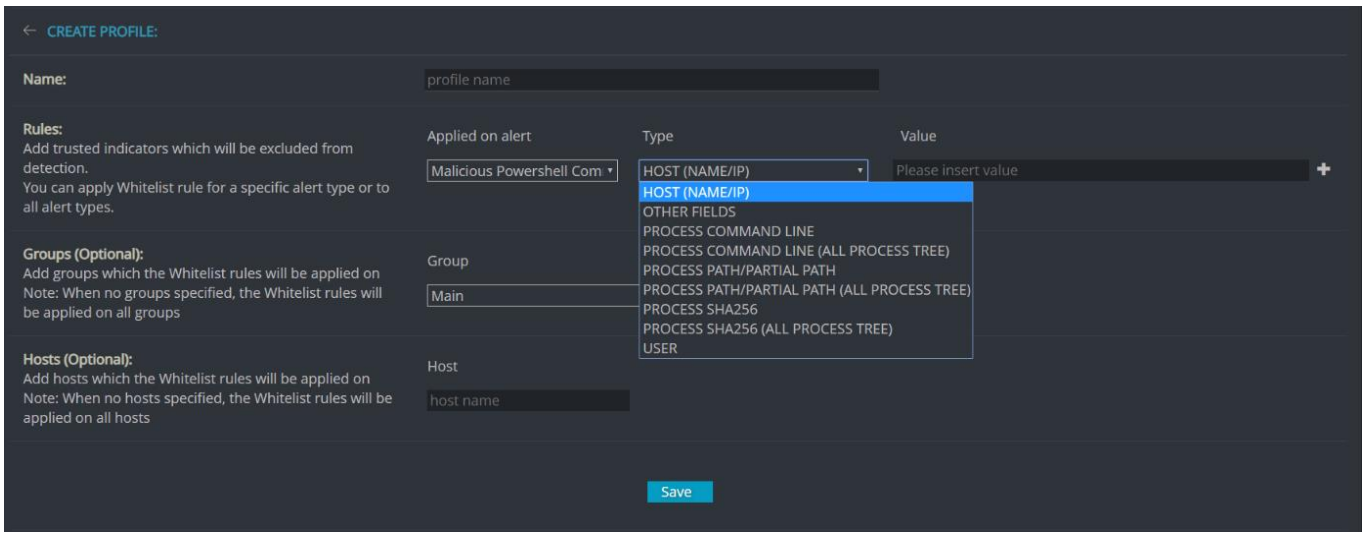
4. Fill the relevant details* as follows:
    a. **Profile name** – the name of the whitelisting profile, this will allow you to identify what is the purpose of the specific whitelisting
    b. **Whitelist by –** you can choose the relevant field to whitelist. You have several options on how to whitelist an activity – by the exact process path or hash, by part of the path (a directory that you want to exclude), or by a specific user or host. In case you want to whitelist something more specific, for example: the command line of the process, you can do it through the second whitelisting option described below.
    c. **Whitelist for –** here you can choose that the whitelisting will apply for a specific scan group or a specific host. If you don't choose any of these options, the whitelisting will apply to all Cynet protected assets.

*Choosing all the options will not create a correlated whitelisting, but will add multiple rules to the same profile (i.e. each whitelisting will apply separately)

Advanced Whitelisting through the Whitelisting Settings Page

1. From the Cynet Dashboard go to Settings.
2. Click on Whitelisting/Whitelisting & Exclusions/Profiles (depends on your Cynet version).
3. Click on "Create" to create a new Whitelisting profile.





4. **Name** - Enter the whitelisting profile name – this will allow you to easily identify what was the purpose of the whitelisting.
5. Rules -
   a. **"Applied on alert"**. Here you may choose the alert you wish to whitelist according to the alert that was triggered under the Cynet Alerts page (see Appendix A for more details about the applicability of each alert).

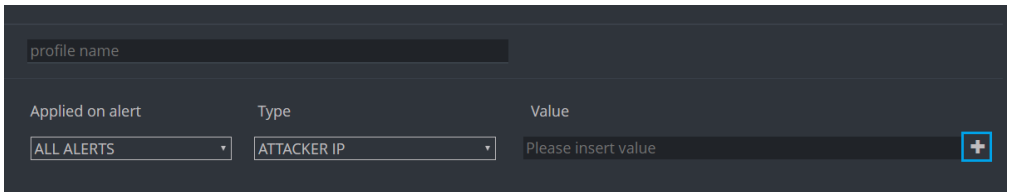
      It is recommended to whitelist a specific alert rather than using "All Alerts" option, since the more specific the whitelisting configuration is, it will reduce the risk of configuring a wide exclusion.

b. **Type -** Select the type of alert on which the exclusion will be based on (see Appendix B - Alert Fields Clarifications).

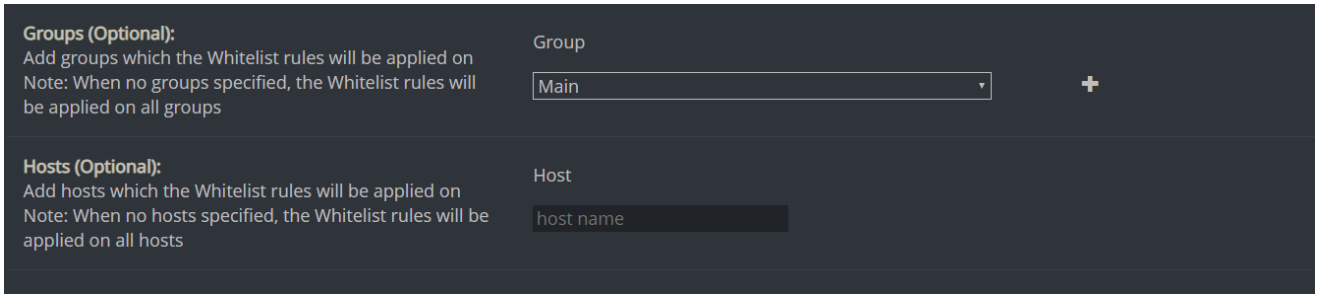
   Note that choosing “Other Fields” will only apply to unique fields that are relevant to the specific alerts (see Appendix C - Other Fields Examples).

c. **Value -** Enter the value according to the type of the information that you chose under the "Type" field (you can copy it from the alert or email alert).
   Please note – there is no option to use regex or wildcards.

6. Select the plus (“+”) button to add the rule to the profile:

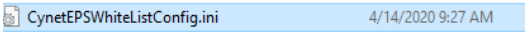


7. **Groups and Hosts** - You can configure the whitelisting to apply on a specific scan group or a specific host. This configuration is optional, if you don’t configure anything, the whitelisting rules will apply on all Cynet’s protected assets



BEST PRACTICE AND CLARIFICATIONS

1. Be sure and precise
    a. Once you add the Whitelisting rule, the alert will not show up anymore according to the rule you have set.
    b. In case you have set the whitelist based on a host, the specific alert will not show up anymore for this host.
2. All Alerts – applying whitelisting on all alerts means that the whitelist will be applied on all Cynet alerts. This whitelisting can risk your environment if it is not configured properly.
3. Other fields – In most of the alerts, you can whitelist unique fields using the "other fields" option. This means the whitelist will apply to unique fields that are applicable for a specific alert you chose. Please see Appendix C for more information on the fields available under "Other Fields". For example, if you want to whitelist "malicious child process" in the parent process alerts, choose "Other Fields" in order to insert the value of the child process.
4. Whitelisting files through forensic screen vs. creating a whitelisting profile – if you whitelist a file through the Forensic tab, it will only apply on alerts that are triggered due to the "Fast Scan" mechanism (i.e. "Threat Intelligence" alerts), and not to all the alerts.

    The best and most efficient way to whitelist a file is through the whitelisting configuration settings.
5. Whitelisting applicability - Once you whitelist an activity in the Cynet server, it will take up to 30 minutes for all the hosts in your environment to get the updated whitelisting configuration. In order to check if the whitelisting applied, you could check when the CynetEPSWhiteListConfig.ini was last modified: 

    This configuration is located in c:\programdata\cynet

CONTACT CYNET CYOPS (CYNET SECURITY OPERATIONS CENTER)

The Cynet CyOps available to clients 24/7 for any issues, questions, or comments related to Cynet 360. For additional information, you may contact us directly at:

Phone (US): +1-347-474-0048

Phone (EU): +44-203-290-9051

Phone (IL): +972-72-336-9736

CyOps Email: soc@cynet.com

APPENDIXES

Appendix A - Alert Names Clarifications

Appendix B - Alert Fields Clarifications

Appendix C - Other Fields Examples

Appendix D - Whitelisting Availability – Version 3.7.9 and Above

Appendix E - Whitelisting Availability – Version 3.7.4-3.7.8

Appendix F - Whitelisting Availability – Version 3.7.0-3.7.3

Appendix G - Whitelisting Availability – Version 3.6.5-3.6.9

Appendix H - Whitelisting Availability – Version 3.6.2-3.6.4

Appendix I - Whitelisting Availability – Version 3.6.1 and Below

Appendix A – Alert Names Clarifications

Applied on Alert The alert that is shown on the whitelisting profile	**Alert Name** The alert name from alert
ARP Spoofing	ARP Spoofing
Attempt to change Cynet Registry	Attempt to change Cynet Registry
Attempt to terminate Cynet process	Attempt to terminate Cynet process
Auto Server Alerts	• User Password Age Is More Than 2 Years Old • User Had 5 High Alerts In The Last 3 Months • User Has Over 10 Failed Connection Attempts • User Has Logged In To Double The Amount Of Machines Than Normally • User Has Logged In To More Than 10 Hosts Today • User Has Logged In To More Than 5 Hosts In One Minute • Host Has Suspicious Command or Script Parent • Host Was Not Scanned • No Scans In Group
Deception Network	Deception Network
Detection Engine – Malicious Binary	This whitelisting refers to any AV/AI alerts (alerts that starts with "Detection Engine")
File Monitoring	File Monitoring
Hooks	Hooks
IP Scanning	IP Scanning
Injection Behavior	Injection Behavior
Injection Behavior - Reflective	Injection Behavior - Reflective
Malicious Behavior – Access Critical File	Malicious Behavior – Access Critical File
Malicious Behavior – Blacklist DLL Group	Malicious Behavior – Blacklist DLL Group
Malicious Behavior – DNS Tunneling	Malicious Behavior – DNS Tunneling
Malicious Behavior – Parent Process	Malicious Behavior – Parent Process
Malicious Behavior – Process Create File On Admin Share	Malicious Behavior – Process Create File On Admin Share
Malicious Behavior – Process Create File on Startup Directory	Malicious Behavior – Process Create File on Startup Directory
Malicious Behavior – Process Create Malicious File	Malicious Behavior – Process Create Malicious File
Malicious Binary	Malicious Binary
Malicious Binary – Process Create Malicious File	Malicious Binary – Process Create Malicious File
Malicious Office Macro	Malicious Office Macro
Malicious Powershell – Family Command	Malicious Powershell – Family Command
Malicious Powershell – Length Command	Malicious Powershell – Length Command
Malicious Powershell – Obfuscation Command	Malicious Powershell – Obfuscation Command
Malicious Process Command	Malicious Process Command

Malicious Registry Access Activity	Malicious Registry Access Activity
Malicious Registry Manipulation Activity	Malicious Registry Manipulation Activity
Malicious Task Existing	Malicious Task Existing
Malicious Task Registered	Malicious Task Registered
Malicious Task Running	Malicious Task Running
Memory Pattern	Memory Pattern
Network Activity Inspection – DNS Tunneling	Network Activity Inspection – DNS Tunneling
Network Activity Inspection – ICMP Tunneling	Network Activity Inspection – ICMP Tunneling
Network Activity Inspection – IP Scanning In	Network Activity Inspection – IP Scanning In
Network Activity Inspection – IP Scanning Out	Network Activity Inspection – IP Scanning Out
Network Activity Inspection – Port Scanning In	Network Activity Inspection – Port Scanning In
Network Activity Inspection – Port Scanning Out	Network Activity Inspection – Port Scanning Out
Network Scanner Attack	Network Scanner Attack
Port Scanning	Port Scanning
PowerShell Malicious Command	PowerShell Malicious Command
Privilege Escalation	Privilege Escalation
Process Access Document File	Process Access Document File
Process Access Unexpected File	Process Access Unexpected File
Process Created Potential Executable File	Process Created Potential Executable File
Raw Disk Write	Raw Disk Write
Ransomware Heuristic	Ransomware Heuristic
Registry Audit	Registry Audit
Responder	Responder
Reverse Shell	Reverse Shell
SOC Classification – Files	The alert appears as the following: • On UI alerts – product name appears twice [for instance – “Putty – Putty”] • On email alerts – the name of the product and the incident number [for instance - “Putty - Incident 607670”]
SOC Classification – Network	Network alerts that contain the word "site", for instance: Phishng Site, Malware Distribution Site, Command and Control Site.etc
Suspicious Task Registered	Suspicious Task Registered
System process Create Executable File	System process Create Executable File

Threat intelligence Detection	Will apply the rule on all the following alerts: 1. Threat Intelligence Detection - Malicious Binary - High Similarity 2. Threat intelligence Detection- Malicious Binary – Blacklist 3. Threat intelligence Detection Malicious Binary 4. Threat intelligence Detection Malware/Trojan/Virus/Adware/Ransom/Worm
Unauthorized Memory Access Attempt	Unauthorized Memory Access Attempt
Unauthorized Registry Operation Attempt	Unauthorized Registry Operation Attempt
Vssadmin	Vssadmin

Appendix B – Alert Fields Clarifications

Field Type As shown on UI	**Details** The field shown in the alert
Attacker MAC	The imposter MAC address
Host (Name/IP)	Hostname or Host IP on which the alert was triggered
Other Fields	Any field that is unique to this specific alert
Process Command Line	Process params (which refers to the command line of the main process in the alert)
Process Command Line (all process tree)	Process params of any of the processes that included in the process tree of the alert (grandparent process, parent process, subject-matter process)
Process Path/ Partial Path	The path of the process that attempted to terminate Cynet process (partial or entire path)
Process Path/ Partial Path (all process tree)	The path of any of the processes that are included in the process tree of the alert (partial or entire path)
Process SHA256	Process Hash (the hash of the main process)
Process SHA256 (all process tree)	Process hash of any of the processes which included in the process tree of the alert
User	Username that run the main process
Attacker IP	The IP address of the endpoint that from which the detected activity was performed
Attacket MAC	The MAC address of the endpoint that from which the detected activity was performed
File Dir Path/Partial Path	The file directory in which the file is located
File Path/Partial Path	The file path (partial or entire path)
File SHA256	File Hash (the hash of the detected file)
Domain	The malicious domain that appears in the alert
IP	The malicious IP that appears in the alert

Appendix C – Other Fields Examples

Alert Name	Field that are considered as "Other Fields" Any field that is unique to this specific alert
ARP Spoofing	No unique fields
Attempt to change Cynet Registry	• Destination Process Name • Destination Process Params
Attempt to terminate Cynet process	• Destination Process Name • Destination Process Params
Auto Server Alerts	No unique fields
Deception Network	No unique fields
Detection Engine – Malicious Binary	No unique fields
File Monitoring	• File Fuzzy Hash
Hooks	• File Fuzzy Hash
IP Scanning	• Scanned Ips • Scanned Ports • Target Port
Injection Behavior	• Injection Info • Payload Sample • Target Process Path • Target Process Sha256
Injection Behavior - Reflective	• Injection Info • Payload Sample • Target Process Path • Target Process Sha256
Malicious Behavior – Access Critical File	• File Fuzzy Hash
Malicious Behavior – Blacklist DLL Group	• Loaded Images
Malicious Behavior – DNS Tunneling	• Loaded Images
Malicious Behavior – Parent Process	• Malicious child process Path •Malicious child process command line • Malicious child process SHA256
Malicious Behavior – Process Create File On Admin Share	• File Path
Malicious Behavior – Process Create File on Startup Directory	• File Fuzzy Hash
Malicious Behavior – Process Create Malicious File	• File Fuzzy Hash
Malicious Binary	• Infected file SHA • File Name
Malicious Binary – Process Create Malicious File	• File Fuzzy Hash
Malicious Office Macro	• Macro • Office Macro Rule
Malicious Powershell – Family Command	• Powershell CommandLine • Malicious Parent Process Command Line • Malicious Parent Process

Malicious Powershell – Length Command	• CommandLine • Powershell CommandLine
Malicious Powershell – Obfuscation Command	• CommandLine
Malicious Process Command	• Malicious Command Line • Malicious Process Path
Malicious Registry Access Activity	• Accessed Key Relative Path
Malicious Registry Manipulation Activity	• Manipulated Key Relative Path • Key Value •Rule Key Path
Malicious Task Existing	• Task Name
Malicious Task Registered	• Task Name • Task Arguments • Task Process Path
Malicious Task Running	• Task Name • Task Arguments
Memory Pattern	• Manipulated Key Relative Path • Key Value • Rule Key Path
Network Activity Inspection – DNS Tunneling	• Collected Samples
Network Activity Inspection – ICMP Tunneling	• Collected Samples
Network Activity Inspection – IP Scanning In	• Network Rule
Network Activity Inspection – IP Scanning Out	• Network Rule
Network Activity Inspection – Port Scanning In	• Source Ports
Network Activity Inspection – Port Scanning Out	• Network Rule • Scanned Addresses
Network Scanner Attack	• SMB Network Directory Enumurate Files
Port Scanning	• Scanned Ports
PowerShell Malicious Command	• CommandLine
Privilege Escalation	• Source process path • Target Elevated process path
Process Access Document File	• File Fuzzy Hash
Process Access Unexpected File	• File Fuzzy Hash
Process Created Potential Executable File	• File Path • File SHA256
Raw Disk Write	No unique fields
Ransomware Heuristic	• New File • New File Ransomware Note • Delete • New File Familiar Previous Extension • Rename Familiar Previous Extension
Registry Audit	No unique fields
Responder	No unique fields

Reverse Shell	• Reverse Shell Process
SOC Classification – Files	No unique fields
SOC Classification – Network	No unique fields
Suspicious Task Registered	• Task Name
System process Create Executable File	No unique fields
Threat intelligence Detection	• File Fuzzy Hash
Unauthorized Memory Access Attempt	• Destination Process Name • Destination Process SHA256
Unauthorized Registry Operation Attempt	• Registry key • Registry data type
Vssadmin	No unique fields

Appendix D - Whitelisting Availability – Version 3.7.9 and Above

Alert	Comments
ARP Spoofing	
Attempt to change Cynet Registry	
Attempt to terminate Cynet process	Whitelisting “Other Fields” is not available
Auto Server Alerts	Refers to the following alerts: • User Password Age Is More Than 2 Years Old • User Had 5 High Alerts In The Last 3 Months • User Has Over 10 Failed Connection Attempts • User Has Logged In To Double The Amount Of Machines Than Normally • User Has Logged In To More Than 10 Hosts Today • User Has Logged In To More Than 5 Hosts In One Minute • Host Has Suspicious Command or Script Parent • Host Was Not Scanned • No Scans In Group
Deception Network	
Detection Engine – Malicious Binary	This whitelisting refers to any AV/AI alerts (alerts that starts with “Detection Engine”)
File Monitoring	Whitelist File Dir Path/Partial Path is not supported
Hooks	
IP Scanning	
Injection Behavior	Whitelisting “Other Fields” is not supported
Injection Behavior - Reflective	
Malicious Behavior – Access Critical File	Whitelisting "File Dir Path” is not supported
Malicious Behavior – Blacklist DLL Group	
Malicious Behavior – DNS Tunneling	Does not apply on Windows XP
Malicious Behavior – Parent Process	
Malicious Behavior – Process Create File On Admin Share	Whitelisting "File Dir Path” is not supported
Malicious Behavior – Process Create File on Startup Directory	Whitelisting "File Dir Path” is not supported
Malicious Behavior – Process Create Malicious File	Whitelisting "File Dir Path” is not supported
Malicious Binary	
Malicious Binary – Process Create Malicious File	
Malicious Office Macro	Whitelisting "File Dir Path” is not supported
Malicious Powershell – Family Command	
Malicious Powershell – Length Command	
Malicious Powershell – Obfuscation Command	
Malicious Process Command	
Malicious Registry Access Activity	
Malicious Registry Manipulation Activity	

Malicious Task Existing	•When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
Malicious Task Registered	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
Malicious Task Running	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by User is not supported
Memory Pattern	Whitelisting “Other Fields” is not supported
Network Activity Inspection – DNS Tunneling	
Network Activity Inspection – ICMP Tunneling	
Network Activity Inspection – IP Scanning In	
Network Activity Inspection – IP Scanning Out	
Network Activity Inspection – Port Scanning In	
Network Activity Inspection – Port Scanning Out	
Network Scanner Attack	
Port Scanning	
PowerShell Malicious Command	
Privilege Escalation	
Process Access Document File	Whitelisting "File Dir Path” is not supported
Process Access Unexpected File	
Process Created Potential Executable File	
Raw Disk Write	
Ransomware Heuristic	
Registry Audit	
Responder	
Reverse Shell	
SOC Classification – Files	The alert appears as follows: • On UI alerts – product name appears twice [for instance – “Putty – Putty”] • On email alerts – the name of the product and the incident number [for instance - “Putty - Incident 607670”]
SOC Classification – Network	Network alerts that contain the word "site", for instance: Phishing Site, Malware Distribution Site, Command and Control Site, etc.
Suspicious Task Registered	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
System process Create Executable File	

Threat intelligence Detection	Will apply the rule on all the following alerts: • Threat Intelligence Detection - Malicious Binary - High Similarity • Threat intelligence Detection- Malicious Binary – Blacklist • Threat intelligence Detection Malicious Binary • Threat intelligence Detection - Malware/Trojan/Virus/Adware/Ransom/Worm • Whitelisting "File Dir Path" is not supported • Whitelisting "Other Fields" is not supported
Unauthorized Memory Access Attempt	Whitelisting "Destination Process Params" is not supported
Unauthorized Registry Operation Attempt	Whitelisting of the following fields is not supported: Other Fields File Dir Path Process SHA256 (All process tree) Process Path (All process tree) Process command line (All process tree)
Vssadmin	

Appendix E - Whitelisting Availability – Version 3.7.4-3.7.8

Alert	Comments
ARP Spoofing	
Attempt to change Cynet Registry	Whitelisting of the following fields is not supported: Other Fields File Dir Path Process SHA256 (All process tree) Process Path (All process tree) Process command line (All process tree)
Attempt to terminate Cynet process	Whitelisting “Other Fields” is not supported
Auto Server Alerts	Refers to the following alerts: User Password Age Is More Than 2 Years Old User Had 5 High Alerts In The Last 3 Months User Has Over 10 Failed Connection Attempts User Has Logged In To Double The Amount Of Machines Than Normally User Has Logged In To More Than 10 Hosts Today User Has Logged In To More Than 5 Hosts In One Minute Host Has Suspicious Command or Script Parent Host Was Not Scanned No Scans In Group
Deception Network	
Detection Engine – Malicious Binary	This whitelisting refers to any AV/AI alerts (alerts that starts with “Detection Engine”)
File Monitoring	Whitelisting by File Dir Path/Partial Path is not supported
Hooks	
IP Scanning	
Injection Behavior	Whitelisting “Other Fields” is not supported
Injection Behavior - Reflective	
Malicious Behavior – Access Critical File	Whitelisting "File Dir Path” is not supported
Malicious Behavior – Blacklist DLL Group	
Malicious Behavior – DNS Tunneling	Does not apply on Windows XP
Malicious Behavior – Parent Process	
Malicious Behavior – Process Create File On Admin Share	Whitelisting "File Dir Path” is not supported
Malicious Behavior – Process Create File on Startup Directory	Whitelisting "File Dir Path” is not supported
Malicious Behavior – Process Create Malicious File	Whitelisting "File Dir Path” is not supported
Malicious Binary	
Malicious Binary – Process Create Malicious File	
Malicious Office Macro	Whitelisting "File Dir Path” is not supported
Malicious Powershell – Family Command	
Malicious Powershell – Length Command	
Malicious Powershell – Obfuscation Command	
Malicious Process Command	

Malicious Registry Access Activity	
Malicious Registry Manipulation Activity	
Malicious Task Existing	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
Malicious Task Registered	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
Malicious Task Running	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by User is not supported
Memory Pattern	Whitelisting “Other Fields” is not supported
Network Activity Inspection – DNS Tunneling	
Network Activity Inspection – ICMP Tunneling	
Network Activity Inspection – IP Scanning In	
Network Activity Inspection – IP Scanning Out	
Network Activity Inspection – Port Scanning In	
Network Activity Inspection – Port Scanning Out	
Network Scanner Attack	
Port Scanning	
PowerShell Malicious Command	
Privilege Escalation	
Process Access Document File	Whitelisting "File Dir Path” is not supported
Process Access Unexpected File	
Process Created Potential Executable File	
Raw Disk Write	
Ransomware Heuristic	
Registry Audit	
Responder	
Reverse Shell	
SOC Classification – Files	The alert appears as the following: • On UI alerts – product name appears twice [for instance – “Putty – Putty”] • On email alerts – the name of the product and the incident number [for instance - “Putty - Incident 607670”]
SOC Classification – Network	Network alerts that contain the word "site", for instance: Phishing Site, Malware Distribution Site, Command and Control Site, etc.
Suspicious Task Registered	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
System process Create Executable File	

Threat intelligence Detection	Will apply the rule on all the following alerts: Threat Intelligence Detection - Malicious Binary - High Similarity Threat intelligence Detection- Malicious Binary – Blacklist Threat intelligence Detection Malicious Binary Threat intelligence Detection Malware/Trojan/Virus/Adware/Ransom/Worm Whitelisting: • Whitelisting "File Dir Path" is not supported • Whitelisting "Other Fields" is not supported.
Unauthorized Memory Access Attempt	Whitelisting "Destination Process Params" is not supported
Unauthorized Registry Operation Attempt	Whitelisting of the following fields is not supported: Other Fields File Dir Path Process SHA256 (All process tree) Process Path (All process tree) Process command line (All process tree)
Vssadmin	

Appendix F - Whitelisting Availability – Version 3.7.0-3.7.3

Alert	Comments
ARP Spoofing	
Attempt to change Cynet Registry	Whitelisting of the following fields is not supported: Other Fields File Dir Path Process SHA256 (All process tree) Process Path (All process tree) Process command line (All process tree)
Attempt to terminate Cynet process	Whitelisting “Other Fields” is not supported
Auto Server Alerts	Refers to the following alerts: User Password Age Is More Than 2 Years Old User Had 5 High Alerts In The Last 3 Months User Has Over 10 Failed Connection Attempts User Has Logged In To Double The Amount Of Machines Than Normally User Has Logged In To More Than 10 Hosts Today User Has Logged In To More Than 5 Hosts In One Minute Host Has Suspicious Command or Script Parent Host Was Not Scanned No Scans In Group
Deception Network	
Detection Engine – Malicious Binary	This whitelisting refers to any AV/AI alerts (alerts that starts with “Detection Engine”)
File Monitoring	Whitelisting by File Dir Path/Partial Path is not supported
Hooks	
IP Scanning	
Injection Behavior	Whitelisting “Other Fields” is not supported
Injection Behavior - Reflective	
Malicious Behavior – Access Critical File	Whitelisting "File Dir Path” is not supported
Malicious Behavior – Blacklist DLL Group	
Malicious Behavior – DNS Tunneling	Does not apply on Windows XP
Malicious Behavior – Parent Process	
Malicious Behavior – Process Create File On Admin Share	Whitelisting "File Dir Path” is not supported
Malicious Behavior – Process Create File on Startup Directory	Whitelisting "File Dir Path” is not supported
Malicious Behavior – Process Create Malicious File	Whitelisting "File Dir Path” is not supported
Malicious Binary	
Malicious Binary – Process Create Malicious File	
Malicious Office Macro	Whitelisting "File Dir Path” is not supported
Malicious Powershell – Family Command	
Malicious Powershell – Length Command	
Malicious Powershell – Obfuscation Command	
Malicious Process Command	

Malicious Registry Access Activity	
Malicious Registry Manipulation Activity	
Malicious Task Existing	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
Malicious Task Registered	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
Malicious Task Running	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by User is not supported
Memory Pattern	Whitelisting “Other Fields” is not supported
Network Activity Inspection – DNS Tunneling	
Network Activity Inspection – ICMP Tunneling	
Network Activity Inspection – IP Scanning In	
Network Activity Inspection – IP Scanning Out	
Network Activity Inspection – Port Scanning In	
Network Activity Inspection – Port Scanning Out	Whitelisting of the process is not supported until 3.7.2
Network Scanner Attack	
Port Scanning	
PowerShell Malicious Command	
Privilege Escalation	
Process Access Document File	Whitelisting "File Dir Path” is not supported
Process Access Unexpected File	
Process Created Potential Executable File	
Raw Disk Write	
Ransomware Heuristic	
Registry Audit	
Responder	
Reverse Shell	
Suspicious Task Registered	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
System process Create Executable File	

Threat intelligence Detection	Will apply the rule on all the following alerts: Threat Intelligence Detection - Malicious Binary - High Similarity Threat intelligence Detection- Malicious Binary – Blacklist Threat intelligence Detection Malicious Binary Threat intelligence Detection Malware/Trojan/Virus/Adware/Ransom/Worm Whitelisting: • Whitelisting "File Dir Path" is not supported • Whitelisting "Other Fields" is not supported.
Unauthorized Memory Access Attempt	Whitelisting "Destination Process Params" is not supported
Unauthorized Registry Operation Attempt	Whitelisting of the following fields is not supported: Other Fields File Dir Path Process SHA256 (All process tree) Process Path (All process tree) Process command line (All process tree)
Vssadmin	

Appendix G - Whitelisting Availability – Version 3.6.5-3.6.9

Alert	Comments
ARP Spoofing	
Attempt to terminate Cynet process	Whitelisting “Other Fields” is not supported
Auto Server Alerts	Refers to the following alerts: User Password Age Is More Than 2 Years Old User Had 5 High Alerts In The Last 3 Months User Has Over 10 Failed Connection Attempts User Has Logged In To Double The Amount Of Machines Than Normally User Has Logged In To More Than 10 Hosts Today User Has Logged In To More Than 5 Hosts In One Minute Host Has Suspicious Command or Script Parent Host Was Not Scanned No Scans In Group
Detection Engine – Malicious Binary	This whitelisting refers to any AV/AI alerts (alerts that starts with “Detection Engine”)
File Monitoring	Whitelisting by File Dir Path/Partial Path is not supported
Hooks	
IP Scanning	
Injection Behavior	Whitelisting “Other Fields” is not supported
Injection Behavior - Reflective	
Malicious Behavior – Access Critical File	Whitelisting "File Dir Path” is not supported
Malicious Behavior – Blacklist DLL Group	
Malicious Behavior – DNS Tunneling	Does not apply on Windows XP
Malicious Behavior – Parent Process	
Malicious Behavior – Process Create File On Admin Share	Whitelisting "File Dir Path” is not supported
Malicious Behavior – Process Create File on Startup Directory	Whitelisting "File Dir Path” is not supported
Malicious Behavior – Process Create Malicious File	Whitelisting "File Dir Path” is not supported
Malicious Binary	
Malicious Binary – Process Create Malicious File	
Malicious Powershell – Family Command	
Malicious Powershell – Length Command	
Malicious Powershell – Obfuscation Command	
Malicious Process Command	
Malicious Registry Access Activity	
Malicious Registry Manipulation Activity	
Malicious Task Existing	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported

Malicious Task Registered	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
Malicious Task Running	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by User is not supported
Network Activity Inspection – IP Scanning Out	
Network Activity Inspection – Port Scanning Out	Whitelisting of the process is not supported
Network Scanner Attack	
Port Scanning	
PowerShell Malicious Command	
Privilege Escalation	
Process Access Document File	Whitelisting "File Dir Path” is not supported
Process Access Unexpected File	
Process Created Potential Executable File	
Raw Disk Write	
Ransomware Heuristic	
Registry Audit	
Responder	
Reverse Shell	
Suspicious Task Registered	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
System process Create Executable File	
Threat intelligence Detection	Will apply the rule on all the following alerts: Threat Intelligence Detection - Malicious Binary - High Similarity Threat intelligence Detection- Malicious Binary – Blacklist Threat intelligence Detection Malicious Binary Threat intelligence Detection Malware/Trojan/Virus/Adware/Ransom/Worm Whitelisting: • Whitelisting "File Dir Path” is not supported • Whitelisting “Other Fields” is not supported.
Unauthorized Memory Access Attempt	Whitelisting “Destination Process Params” is not supported
Vssadmin	

Appendix H – Whitelisting Availability – Version 3.6.2-3.6.4

Alert	Comments
ARP Spoofing	
Auto Server Alerts	Refers to the following alerts: User Password Age Is More Than 2 Years Old User Had 5 High Alerts In The Last 3 Months User Has Over 10 Failed Connection Attempts User Has Logged In To Double The Amount Of Machines Than Normally User Has Logged In To More Than 10 Hosts Today User Has Logged In To More Than 5 Hosts In One Minute Host Has Suspicious Command or Script Parent Host Was Not Scanned No Scans In Group
Detection Engine – Malicious Binary	This whitelisting refers to any AV/AI alerts (alerts that starts with "Detection Engine")
File Monitoring	Whitelisting by File Dir Path/Partial Path is not supported
Hooks	
IP Scanning	
Injection Behavior	Whitelisting "Other Fields" is not supported
Injection Behavior - Reflective	
Malicious Behavior – Access Critical File	Whitelisting "File Dir Path" is not supported
Malicious Behavior – Blacklist DLL Group	
Malicious Behavior – DNS Tunneling	Does not apply on Windows XP
Malicious Behavior – Parent Process	
Malicious Behavior – Process Create Malicious File	Whitelisting "File Dir Path" is not supported
Malicious Binary	
Malicious Powershell – Family Command	
Malicious Powershell – Length Command	
Malicious Powershell – Obfuscation Command	
Malicious Process Command	
Malicious Registry Access Activity	
Malicious Registry Manipulation Activity	
Malicious Task Existing	• When whitelisting "Task Name" - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path" is not supported • Whitelisting by "File SHA256" is not supported
Malicious Task Registered	• When whitelisting "Task Name" - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path" is not supported • Whitelisting by "File SHA256" is not supported
Malicious Task Running	• When whitelisting "Task Name" - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path" is not supported • Whitelisting by User is not supported

Network Activity Inspection – IP Scanning Out	
Network Activity Inspection – Port Scanning Out	Whitelisting of the process is not supported
Network Scanner Attack	
Port Scanning	
PowerShell Malicious Command	
Privilege Escalation	
Process Access Document File	Whitelisting "File Dir Path" is not supported
Process Access Unexpected File	
Process Created Potential Executable File	
Raw Disk Write	
Ransomware Heuristic	
Registry Audit	
Responder	
Reverse Shell	
Suspicious Task Registered	• When whitelisting "Task Name" - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path" is not supported • Whitelisting by "File SHA256" is not supported
System process Create Executable File	
Threat intelligence Detection	Will apply the rule on all the following alerts: Threat Intelligence Detection - Malicious Binary - High Similarity Threat intelligence Detection- Malicious Binary – Blacklist Threat intelligence Detection Malicious Binary Threat intelligence Detection Malware/Trojan/Virus/Adware/Ransom/Worm Whitelisting: • Whitelisting "File Dir Path" is not supported • Whitelisting "Other Fields" is not supported.
Unauthorized Memory Access Attempt	Whitelisting "Destination Process Params" is not supported
Vssadmin	

Appendix I - Whitelisting Availability – Version 3.6.1 and Below

Alert	Comments
ARP Spoofing	
Auto Server Alerts	Refers to the following alerts: User Password Age Is More Than 2 Years Old User Had 5 High Alerts In The Last 3 Months User Has Over 10 Failed Connection Attempts User Has Logged In To Double The Amount Of Machines Than Normally User Has Logged In To More Than 10 Hosts Today User Has Logged In To More Than 5 Hosts In One Minute Host Has Suspicious Command or Script Parent Host Was Not Scanned No Scans In Group
Detection Engine – Malicious Binary	This whitelisting refers to any AV/AI alerts (alerts that starts with "Detection Engine")
File Monitoring	Whitelisting by File Dir Path/Partial Path is not supported
Hooks	
IP Scanning	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Injection Behavior	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available Whitelisting "Other Fields" is not available
Injection Behavior - Reflective	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Malicious Behavior – Access Critical File	Whitelisting "File Dir Path" is not available
Malicious Behavior – Blacklist DLL Group	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Malicious Behavior – DNS Tunneling	Does not apply on Windows XP Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Malicious Behavior – Parent Process	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Malicious Behavior – Process Create Malicious File	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available Whitelisting "File Dir Path" is not available
Malicious Binary	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Malicious Powershell – Family Command	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Malicious Powershell – Length Command	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available Whitelisting "File Dir Path" is not available
Malicious Powershell – Obfuscation Command	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available

Malicious Process Command	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Malicious Registry Access Activity	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Malicious Registry Manipulation Activity	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Malicious Task Existing	•When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
Malicious Task Registered	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "File Dir Path” is not supported • Whitelisting by “File SHA256” is not supported
Malicious Task Running	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself. • Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available • Whitelisting "File Dir Path” is not available • Whitelisting by User is not available
Network Activity Inspection – IP Scanning Out	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Network Activity Inspection – Port Scanning Out	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Network Scanner Attack	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Port Scanning	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
PowerShell Malicious Command	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Privilege Escalation	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Process Access Document File	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available Whitelisting "File Dir Path” is not available
Process Access Unexpected File	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Process Created Potential Executable File	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Raw Disk Write	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Ransomware Heuristic	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available
Registry Audit	
Responder	
Reverse Shell	Whitelisting ""All Process Tree"" fields (Path, SHA256, Command Line) is not available
Suspicious Task Registered	• When whitelisting “Task Name” - apply the value without the '\' before, insert only the task name itself.

	• Whitelisting "File Dir Path" is not supported • Whitelisting by "File SHA256" is not supported
System process Create Executable File	Whitelisting ""All Process Tree"" fields (Path, SHA256, Command Line) is not available
Threat intelligence Detection	Whitelisting "All Process Tree" fields (Path, SHA256, Command Line) is not available • Whitelisting "File Dir Path" is not available • Whitelisting "Other Fields": • whitelisting by "Other Fields" is not available.
Unauthorized Memory Access Attempt	Whitelisting "Destination Process Params" is not supported
Vssadmin	