

# 정책 : 소프트웨어 정책

## 개요

Carbon Black App Control Software Rules 메뉴에 대한 상세 설명입니다.

## 정책 소개

① 소프트웨어 정책 메뉴 : [App Control] 웹 콘솔 접속 > [Rules] 메뉴 - 'Software Rule' 클릭 후 이동

정책 등록 시에 활용되는 파일, 소프트웨어 등 바이너리는 엔드포인트 센서 스캔을 통해 등록됩니다. 처음으로 에이전트를 배포한 엔드포인트에서 전체 바이너리에 대해서 첫 등록 절차를 밟게 되니, 조직 내에서 첫 배포하는 운영체제 유형 등에 대해 영향을 받을 수 있으므로 클린 OS에 먼저 설치하여 기준 정책을 정의하여 사용함을 권장합니다.

## 1. Updaters

### 1.1. 정책 설명

<input type="checkbox"/> Select 35	Name ^	Platforms	Enabled	Date Created	Created By	Date Modified	Last Modified By
<input checked="" type="checkbox"/> Enabled: Yes		10 item(s)					
<input checked="" type="checkbox"/>	Allow Printer Installations	Windows	Yes	Feb 18 2024 04:46:16 PM	System	Feb 18 2024 04:46:16 PM	System
<input checked="" type="checkbox"/>	Apple System Performance	Mac	Yes	Feb 18 2024 04:46:27 PM	System	Feb 18 2024 04:46:27 PM	System
<input checked="" type="checkbox"/>	Detection of Linux Shutdown sequence	Linux	Yes	Feb 18 2024 04:46:19 PM	System	Feb 18 2024 04:46:19 PM	System
<input checked="" type="checkbox"/>	Linux Self Protection	Linux	Yes	Feb 18 2024 04:46:28 PM	System	Feb 18 2024 04:46:28 PM	System
<input checked="" type="checkbox"/>	Linux System Performance	Linux	Yes	Feb 18 2024 04:46:19 PM	System	Feb 18 2024 04:46:19 PM	System
<input checked="" type="checkbox"/>	Mac App Store Downloads	Mac	Yes	Feb 18 2024 04:46:18 PM	System	Feb 18 2024 04:46:18 PM	System
<input checked="" type="checkbox"/>	Mac System Updates	Mac	Yes	Feb 18 2024 04:46:19 PM	System	Feb 18 2024 04:46:19 PM	System
<input checked="" type="checkbox"/>	Microsoft .NET Framework	Windows	Yes	Feb 18 2024 04:46:16 PM	System	Feb 18 2024 04:46:16 PM	System
<input checked="" type="checkbox"/>	Windows 8, 10 and Server 2012 Updates	Windows	Yes	Feb 18 2024 04:46:18 PM	System	Feb 18 2024 04:46:18 PM	System
<input checked="" type="checkbox"/>	Windows Update Temporary Files - Do Not Report	Windows	Yes	Feb 18 2024 04:46:18 PM	System	Feb 18 2024 04:46:18 PM	System
<input checked="" type="checkbox"/> Enabled: No		54 item(s)					
<input type="checkbox"/>	Adobe Acrobat Reader 10.0	Windows	No	Feb 18 2024 04:46:16 PM	System	Feb 18 2024 04:46:16 PM	System
<input type="checkbox"/>	Adobe Acrobat Reader 9.0	Windows	No	Feb 18 2024 04:46:16 PM	System	Feb 18 2024 04:46:16 PM	System
<input type="checkbox"/>	Adobe Acrobat Reader DC	Windows	No	Feb 18 2024 04:46:16 PM	System	Feb 18 2024 04:46:16 PM	System

Updaters 정책은 승인되지 않은 업데이트 프로그램을 통해 악성 프로그램이 유입되는 동작을 방지하기 위한 정책입니다. Carbon Black App Control 에 정의된 업데이트 프로그램에 대한 허용 여부를 선택하여 사용합니다. 업데이트 프로그램을 허용한 경우 소프트웨어 업데이트가 진행하며, 업데이트 프로그램을 허용하지 않은 경우 프로그램을 통한 소프트웨어 업데이트가 진행되지 않습니다. Updaters 정책의 경우, Carbon Black File Reputation 연동을 통해 최신 버전으로 자동 업데이트 진행됩니다. 또한 Carbon Black 에서 직접 제공 및 관리하는 정책이므로, 사용자가 추가 또는 수정하여 사용할 수 없습니다.

## 2. Rapid Configs

### 2.1. 정책 설명

<input type="checkbox"/> Select 3	Name ^	Description	Enabled	Configured	Platform	Modified By	Policy
<input type="checkbox"/>	Browser Protection	Reports or prevents potentially malicious behavior related to browsers. This includes execution of files downloaded by browsers, modification of the hosts file, and modification of browser related registry entries. Minimum Carbon Black App Control agent version to use this Rapid Config is 8.0.0.	No	No	Windows	System	All Current and Future Policies
<input type="checkbox"/>	Carbon Black App Control Server Tamper Protection	Provides protection against tampering with the Carbon Black App Control Server. Minimum Carbon Black App Control agent version to use this Rapid Config is 7.2.0.	No	Yes	Windows	System	All Current and Future Policies
<input type="checkbox"/>	Carbon Black EDR Tamper Protection	Prevents tampering with Carbon Black EDR. Minimum Carbon Black App Control agent version to use this Rapid Config is 7.2.0.	No	Yes	Windows	System	All Current and Future Policies
<input type="checkbox"/>	Cryptomining Protection	Reports or prevents potentially malicious behavior related to file based cryptomining attacks. Minimum Carbon Black App Control agent version to use this Rapid Config is 8.0.0.	No	No	Windows	System	All Current and Future Policies
<input type="checkbox"/>	Delivery Optimization	Approve files written by the Delivery Optimization Service (DoSvc). This Rapid Config is not needed for agents running version 8.1 and later because files written by the Delivery Optimization Service will automatically be approved in those versions. Minimum Carbon Black App Control agent version to use this Rapid Config is 7.2.0.	No	Yes	Windows	System	All Current and Future Policies
<input type="checkbox"/>	Domain Controller Logon Scripts	Allows and optionally promotes all files under the Sysvol and NetLogon directories of the specified domain controllers if an agent is a member of the specified domain. Minimum Carbon Black App Control agent version to use this Rapid Config is 7.2.0.	No	No	Windows	System	All Current and Future Policies
<input type="checkbox"/>	Protect against the exploit known as Doppelganging on windows systems. Reference: <a href="https://community.carbonblack.com/docs/DOC-">https://community.carbonblack.com/docs/DOC-</a>						

Rapid Configs 정책은 파일에 대한 허용 및 차단 등의 초기 정책 구성이 필요한 App Control의 제품의 특성을 고려하여, 사용자들이 보다 빠르게 안전한 엔드포인트 환경을 구성할 수 있는 정책입니다. 자주 사용되는 공격 기법을 방지하여 보안을 강화하거나 자주 사용되는 소프트웨어에 대한 승인 또는 변조 방지 정책을 미리 지정되어 있어 관리자가 보다 빠른 보안 환경 구성을 도와줍니다. Updater 정책과 동일하게 Carbon Black 에서 직접 제공 및 관리하는 정책이므로, Carbon Black File Reputation 연동을 통해 활성화하며 최신

## 3. Publishers

### 3.1.정책 설명

<input type="checkbox"/> Select 28	Name	State	Date Approved or Banned	Approved or Banned By	First Seen Date	Trust	Acknowledged	First Seen Com
<input type="checkbox"/>	Windows Community Toolkit (.NET Foundation)	Unapproved			Feb 18 2024 05:03:15 PM	Not trusted (Unknown)	No	ETVS\SEUNGMIN
<input type="checkbox"/>	Newtek Inc	Unapproved			Feb 18 2024 05:05:48 PM	Not trusted (Unknown)	No	ETVS\SEUNGMIN
<input type="checkbox"/>	Microsoft Dynamic Code Publisher	Unapproved			Feb 18 2024 05:09:23 PM	Not trusted (Unknown)	No	ETVS\SEUNGMIN
<input type="checkbox"/>	Microsoft Corp Enclave Signer	Unapproved			Feb 18 2024 05:10:09 PM	Not trusted (Unknown)	No	ETVS\SEUNGMIN
<input type="checkbox"/>	Microsoft Windows Early Launch Anti-malware Publisher	Unapproved			Feb 18 2024 05:10:47 PM	Not trusted (Unknown)	No	ETVS\SEUNGMIN
<input type="checkbox"/>	SecureTeam Software	Unapproved			Feb 18 2024 05:11:21 PM	Not trusted (Unknown)	No	ETVS\SEUNGMIN
<input type="checkbox"/>	Nicholas Anderson	Unapproved			Feb 18 2024 05:13:11 PM	Not trusted (Unknown)	No	ETVS\SEUNGMIN
<input type="checkbox"/>	Flexera Software LLC	Unapproved			Feb 18 2024 05:14:40 PM	Not trusted (Unknown)	No	ETVS\SEUNGMIN
<input type="checkbox"/>	Microsoft 3rd Party Application Component	Unapproved			Feb 18 2024 05:23:56 PM	Not trusted (Unknown)	No	ETVS\SEUNGMIN
<input type="checkbox"/>	Intel Corporation - Client Components Group	Unapproved			Feb 18 2024 05:24:34 PM	Medium	No	ETVS\SEUNGMIN
<b>State: Approved 3 item(s)</b>								
<input type="checkbox"/>	Bit9, Inc.	Approved	Feb 15 2024 11:01:13 PM	System	Feb 15 2024 11:01:12 PM	High	No	
<input type="checkbox"/>	Bit9, Inc	Approved	Feb 15 2024 11:01:13 PM	System	Feb 15 2024 11:01:13 PM	High	No	
<input type="checkbox"/>	Carbon Black, Inc.	Approved	Feb 15 2024 11:01:13 PM	System	Feb 15 2024 11:01:13 PM	High	No	

Publishers 정책은 소프트웨어 인증서의 신뢰 여부를 판단하여 악성 소프트웨어 동작을 방지하기 위한 정책입니다. 엔드포인트 스캔을 통해 등록된 소프트웨어 인증서 또는 직접 등록된 소프트웨어 인증서의 승인 여부를 선택하여 소프트웨어 동작을 제어합니다. Carbon Black 에 대한 소프트웨어 인증서는 기본적으로 허용 규칙이 정의되어 있으나, 그 외 소프트웨어 인증서는 승인 여부 선택이 필요합니다.

### 3.2.정책 생성

#### Add Publisher

Select file containing certificate

File Name:

파일 선택

선택된 파일 없음

Only upload files smaller than 100,000,000 bytes.

Save

Cancel

엔드포인트 센서 스캔을 통해 정의된 소프트웨어 인증서 외에 관리자가 추가하고자 하는 소프트웨어 인증서를 업로드하여 사용 가능합니다. 소프트웨어 인증서 파일의 크기는 100MB 미만으로 제한됩니다.

## 4. Users

### 4.1.정책 설명

Saved Views:

(none)

Delete

Save

Saved View Name

Create

Group By:

(none)

Ascending

Show Filters

Show Columns

Export to CSV

Refresh Table

Add Trusted User or Group

Search: Enter Name

☐ Automatically apply

Showing 1 out of 1 item(s)

	Name	Date Created	Created By	Platform
	seungmin	Feb 18 2024 10:20:09 PM	admin	Windows

Showing 1 out of 1 item

Showing all data

Users 정책은 신뢰있는 사용자 또는 그룹을 정의하여 신뢰되는 사용자 또는 그룹을 통해 정책 상으로 동작하지 않던 엔드포인트의 파일 실행, 소프트웨어 실행 등의 행위를 허용하기 위한 정책입니다. 파일 및 소프트웨어 동작이 정의되어 제어하는 App Control 제품 특성 때문에, 소프트웨어 설치 및 파일 실행에 대해 일시적 허용이 필요한 경우 활용 가능합니다. 지속적인 적용이 필요한 경우 규칙을 분리하여 사용하여 관리도 가능하지만, 단발성 동작의 경우에는 신뢰하는 사용자 및 그룹을 설정하여 파일, 소프트웨어 실행에 대한 예외를 적용하여 편리성을 제공할 수 있습니다. 단, 파일 및 소프트웨어 실행에 대해 차단 정책이 적용된 경우는 사용이 불가합니다.

### 4.2.정책 생성

Enter name of trusted user or group

Platform: Windows

Create Trust Type: ☐ User or Group ☒ Pre-defined Group

Group: Power Users

Save & Exit Cancel

OS 플랫폼 별로 사용자 및 그룹을 입력하여 설정 가능합니다.

- Platform : 사용자 및 그룹의 OS 선택
  - Windows
  - Linux
  - Mac
- Create Trust Type : 신뢰 유형 지정
  - User : 사용자 계정 지정
  - Group : 사용자 그룹 지정
  - Pre-defined Group (Windows 만 지원) : 미리 정의된 사용자 그룹 선택

## 5. Directories

### 5.1.정책 설명

Saved Views:

(none)
Delete
Save

Saved View Name
Create

Group By:

(none)
Ascending

Show Filters
Show Columns
Export to CSV
Refresh Table

Add Trusted Directory
Search: Enter Name
Automatically apply
Showing 1 out of 1 item(s)

	Name	Computer Name	Path	Status	Progress	Date Modified	Last Modified By	Policy
	Test Directory	ETVS\SEUNGMIN-WINDOW	C:\test	Enabled (Verifying)	0/0	Feb 18 2024 11:36:06 PM	admin	SM-TEST

Showing 1 out of 1 item
Showing all data

Directories 정책은 컴퓨터 내의 신뢰할 수 있는 폴더 경로를 지정하여, 해당 폴더 내의 파일 및 프로세스 행위를 허용하기 위한 정책입니다. Windows OS의 경우 신뢰하는 폴더 내의 파일 및 프로세스 행위에 대한 제한은 없습니다. 그러나 **커널 등의 권한 상승이 필요한 Linux 및 Mac OS**의 경우 신뢰하는 폴더 내에 파일에 대하여 분석하거나 (테스트 필수..!)

### 5.2.정책 생성

Trusted directory settings

Name: Test Directory

Computer: ETVS\SEUNGMIN-WINDOW

Directory: C:\test

Description:

☐ All Current and Future policies
☒ Selected policies

Note: You can only change policies that you have permission to manage

Policies:

☐ Policy
Filter Policies

☐ Default Policy
☒ SM-TEST

Status: ☒ Enabled ☐ Disabled

Save & Exit Save Cancel

신뢰하는 폴더 경로를 생성합니다.

- Name : 정책 이름
- Computer : 정책을 지정할 엔드포인트의 컴퓨터 이름 (ex : Windows - 도메인 이름\컴퓨터 이름, Other - 컴퓨터 이름\도메인)
- Directory : 신뢰할 폴더 경로 지정
- Description : 정책 설명
- Policies : 정책 적용 범위
  - All Current and Future Policies : 모든 정책에 적용
  - Selected Policies : 선택한 정책에만 적용
- Status : 정책 활성화 여부
  - Enabled : 활성화
  - Disabled : 비활성화

## 6. Files

### 6.1.정책 설명

<input type="checkbox"/> Select 100	Type	Name	File Hash	Source	Is Global
<b>Type: Approval</b> <b>240 item(s)</b>					
<input type="checkbox"/>	Approval	B9CustomAction.dll	d7103f91ecf520fdcf600c6bc24b1139d663be69f4a8a3376369b19ab374bce	Trusted Directory	Yes
<input type="checkbox"/>	Approval	ParityAgentDB.dll	ec337f688a2045bf7210183493618c39662b20d3877547487d5e8bfe26325b3	Trusted Directory	Yes
<input type="checkbox"/>	Approval	cb7zip.dll	96b0ddd51e2027b56ea499a4cd178246d9f3859bd252afd2dd04206702aa69b0	Trusted Directory	Yes
<input type="checkbox"/>	Approval	Crawler.exe	cc85f2e65b0d1add8ebafa31558e62bcaa37745addc68a6e8f7b9f31753ec601	Trusted Directory	Yes
<input type="checkbox"/>	Approval	DasCLI.exe	6581d9cc447c4dfe954e9b2cd674db89003d0f6914db0d3de7a5e5ebd5a52a86	Trusted Directory	Yes
<input type="checkbox"/>	Approval	dbghelp.dll	1e3770a286d59b0a300535ff0c47696353c6549ea668aba1d81ee798e0ebd373	Trusted Directory	Yes
<input type="checkbox"/>	Approval	ipworks8.dll	3d6613377b880f7ef677c414627482b99de340987402507cd27d308890eca0b	Trusted Directory	Yes
<input type="checkbox"/>	Approval	ipworksssl8.dll	2242e0440836426c2d8cb8ee2a39a7392aaa24d8b8256637e649a1cedb9fa0e2	Trusted Directory	Yes
<input type="checkbox"/>	Approval	Notifier.exe	04f29147aae5cb95fbae1bdf26b59549d9d513c3fc62f32f00ff712326f36c7	Trusted Directory	Yes
<input type="checkbox"/>	Approval	NotifierMessages.dll	bba0a01a7809e1637e099749880f8ccaf8c6aa2055fb6c529a9be068196b6fdb	Trusted Directory	Yes
<input type="checkbox"/>	Approval	Parity.exe	d6f884090619a9bca3c49264e031247f2aece394cdfb8761a145db8133ebf8e0	Trusted Directory	Yes
<input type="checkbox"/>	Approval	TimedOverride.exe	bd97271776eb667c3961c9978c601abcc73af7b66de9f3ecf9bae1ac50285355	Trusted Directory	Yes

Files 정책은 엔드포인트 내에서 신뢰되지 않은 프로그램이 실행되어 악성 행위를 진행하는 것을 방지하는 정책입니다.

파일의 해시값을 수집하고 이를 대상으로 실행 가능 여부를 판단하고 정의하여 사용이 가능합니다.

파일의 동작을 차단하는 기능인 만큼 오탐으로 인한 문제 상황이 발생되지 않도록, 모니터링 기능도 제공하여 관리자가 충분한 검토 후에 정책 적용이 진행됩니다.

또한 관리자가 파일의 신뢰 여부를 판단할 수 있도록 각 파일에 대한 세부 정보도 확인할 수 있습니다.

파일은 센서를 통해 수집되며, 수집되는 파일의 대상은 실행이 가능한 파일과 확장자가 일치하는 스트림 파일입니다.

### 6.2.정책 생성

General

Rule Name:

Notepad++.exe

Rule Type:

Approval

Hash Value:

eb595dae9c6f63ccb2e299405ecc2654c78d9fb16b8d0

Description:

Notepad++ Program

Rule Applies To

☐ All Current and Future policies

☒ Selected policies

Note: You can only change policies that you have permission to manage

Policies:

☐ Policy

☐ Default Policy

☒ SM-TEST

Save & Exit

Save

Cancel

실행파일 및 스크립트 파일에 대한 정책을 생성합니다.

- Rule Name : 파일 규칙 이름
- Rule Type : 파일 실행 승인 여부
  - Approval : 승인
  - Ban : 차단
  - Ban (Report Only) : 모니터링
- Hash Value : 파일 해시값
- Description : 파일 규칙 설명
- Policies : 정책 적용 범위 지정
  - All Current and Future Policies : 전체 정책 적용
  - Selected Policies : 선택 정책 적용

## 7. Custom

### 7.1.정책 설명

Rule Type	Name	Action	Operation	Path
Advanced	Mac User Cache App Files	Track	Write, Write Delayed, Delete, Renam...	/Users/*/Library/Caches/*app/Conte
Performance Optimization	Mac User Data Files	Ignore	Write, Write Delayed, Delete, Renam...	/Users/*/Library/Application Support
Performance Optimization	Time Machine	Ignore	Write, Write Delayed, Delete, Renam...	*
Performance Optimization	Ignore Linux Log Files	Ignore	Write, Write Delayed, Delete, Renam...	/var/log/*
Advanced	Track system profile	Track	Write, Write Delayed, Delete, Renam...	<System>\Config\systemprofile\*
Advanced	[Sample] Microsoft App-V Interoperability	Exec [Allow, Finish Rule Group] Wri...	Exec [Execute, Script Execute] Writ...	\device\sftvol\*
Performance Optimization	[Sample] Visual Studio - Ignore Intermediate Files	Ignore	Write, Write Delayed, Delete, Renam...	*.obj (multiple)
Execution Control	[Sample] Visual Studio - Approve Builds	Finish Rule Group, Promote Target P...	Script Execute, Process Create	<Reg:HKLM-Software\X86\Classes\Cl
Performance Optimization	[Sample] VMware Workstation	Ignore	Write, Write Delayed, Delete, Renam...	*
Performance Optimization	[Sample] TortoiseSVN	Ignore	Write, Write Delayed, Delete, Renam...	*
Execution Control	Allow .NET dll executions	Allow, Finish Rule Group	Execute, Script Execute	*.dll
Performance Optimization	Ignore Recycle Bin	Ignore	Write, Write Delayed, Delete, Renam...	<RecycleBin>

## 7.2. 정책 생성

General

Rule Name: [Sample] Report whenever powershell is launched with

Description: Report an event when someone tries to run powershell with an encoded script. This will only work on version 8.0 agents since the <Cmdline>

Status: ☐ Enabled ☒ Disabled

Definition

Platform: Windows

Rule Type: Advanced

Operation: Execute

Execute Action: Report Process Cre

Path or File: Specific Path...

Process: Any Process

User or Group: Any User

<OnlyIf:Bit9Version:Atleast:8.0.0.0><CmdLine:\*Encoded

테스트 필요함

# 8. Memory

## 8.1. 정책 설명

Saved Views:

(none) ▾

Delete

Save

Saved View Name

Create

Group By:

(none) ▾

Ascending ▾

Show Filters ▶

Show Columns ▶

Export to CSV

Refresh Table

+

Add Memory Rule

↕

Export Rules

↕

Import Rules

Search:

Enter Name, Path, Process

☐ Automatically apply
 Showing 1 out of 1 item(s)

<input type="checkbox"/> Select 1	Rank ▲	Status	Platform	Name	Action	Operation	Permissions	Path	Process	User or Group	Date Modified
<input type="checkbox"/>	<div>↕</div> <div>↕</div> <div>1</div>	<input checked="" type="checkbox"/>	Windows	Memory Rule	Block	Create Handle, Duplicate Handle, Al...	Read Access	notepad++.exe	*	Any User	Feb 19 2024 0

Showing 1 out of 1 item

Showing all data

Memory 정책은 인-메모리 공격, 파일리스 공격 등으로부터 메모리를 통한 공격 기법을 방지하기 위한 정책입니다. 지정된 실행 파일 내에 다른 실행파일 또는 사용자(그룹)가 메모리에 접근하거나 수정하지 못하도록 정의하여 사용이 가능합니다. 이는 메모리 공격을 시도하거나, 메모리 공격 발생했을 때에, 발생한 공격이 환경 내로 더 이상 확산되지 않도록 실행파일 내 메모리 접근 및 수정 등의 행위를 차단하여 환경을 보호합니다.

## 8.2. 정책 생성



## General

Name: Memory Rule

Description:

Status: ☒ Enabled ☐ Disabled

## Definition

Expert Mode: ☐ On ☒ Off

Platform: Windows

Action: Block



☒ Use Policy Specific Notifier

Permissions: Read Access



Target Process: notepad++.exe



Source Process: Any Process



User or Group: Any User



## Rule Applies To

☐ All Current and Future policies

☒ Selected policies

Note: You can only change policies that you have permission to manage

Policies:

☐ Policy



Filter Policies

☐ Default Policy

☒ SM-TEST

실행 파일에 대한 메모리 정책을 생성합니다.

- Name : 정책 이름
- Description : 정책 설명
- Status : 정책 사용 여부
- Expert Mode : 전문가 모드 사용 여부
- Platform : Windows OS만 선택 가능
- Action : 메모리 접근 및 수정 행위 발생 시에 동작 방식 선택
  - Block : 차단
  - Prompt : 센서 알림 메시지를 통해 차단 및 허용 여부 선택
  - Report : 이벤트 발생
  - Allow : 허용
  - Block Silently : 센서 알림 메시지 및 이벤트 생성없이 차단
- Permissions : 대상 실행 파일에 허용 또는 차단할 권한 유형 선택
  - Control Process : 프로세스 제어 권한
  - Read Access : 읽기 액세스 권한
  - Write Access : 쓰기 액세스 권한
  - Write + Control : 읽기 및 제어 권한
  - Read + Write + Control : 읽기 및 쓰기 및 제어 권한
  - Dynamic Code Execution : 동적 코드 실행 권한
  - Kernel Memory Access : 사용자 프로세스의 커널 메모리 액세스 권한 (Windows XP 만 지원)
  - Advanced : 세부 제어 설정
- Target Process : 메모리 제어 대상 프로세스
- Source Process : 권한 제어 대상 프로세스
- User or Group : 권한 제어 대상 사용자 또는 그룹
- Policies : 정책 적용 범위

## 9. Registry

### 9.1. 정책 설명

<input type="checkbox"/> Select 7	Rank ▲	Status	Platform	Name	Action	Operation	Path
<input type="checkbox"/>	1	<input checked="" type="radio"/>	Windows	Case Sensitivity: Block Registry Modifications	Block, Finis	Create Key, Rename Key, Delete Key,...	HKLM\SYSTEM\*controlset*\control\filesystem
<input type="checkbox"/>	2	<input checked="" type="radio"/>	Windows	[Sample] Block Suspicious System Changes	Block, Finis	Create Key, Rename Key, Delete Key,...	HKLM\software\microsoft\windows\nt\current
<input type="checkbox"/>	3	<input checked="" type="radio"/>	Windows	[Sample] Prompt on Suspicious changes to Start	Prompt, Fir	Create Key, Rename Key, Delete Key,...	*\software\microsoft\windows\currentversion\
<input type="checkbox"/>	4	<input checked="" type="radio"/>	Windows	[Sample] Report Typical Changes to Startup Files	Report	Create Key, Rename Key, Delete Key,...	*\software\microsoft\windows\currentversion\
<input type="checkbox"/>	5	<input checked="" type="radio"/>	Windows	[Sample] Report Changes to Trusted Zones	Report	Create Key, Rename Key, Delete Key,...	*\software\microsoft\windows\currentversion\
<input type="checkbox"/>	6	<input checked="" type="radio"/>	Windows	[Sample] Report Changes to Home Page or Search	Report	Create Key, Rename Key, Delete Key,...	*\software\microsoft\internet explorer\main\D
<input type="checkbox"/>	7	<input checked="" type="radio"/>	Windows	Autostart Rules	Report	Create Key, Rename Key, Delete Key,...	<AutostartRules>

Registry 정책은 코드 삽입, 파일리스 공격 등으로부터 실행 프로그램에 대한 레지스트리 값이 악의적으로 변경되는 것을 방지하기 위한 정책입니

## 9.2. 정책 생성

- Name : 정책 이름
- Description : 정책 설명
- Status : 정책 사용 여부
- Expert Mode : 전문가 모드 사용 여부
- Platform : Windows OS만 선택 가능
- Write Action : 쓰기 행위 발생 시에 동작 방식 선택
  - Block : 차단
  - Prompt : 센서 알림 메시지를 통해 차단 및 허용 여부 선택
  - Report : 이벤트 발생
  - Allow : 허용
- Registry Path : 제어 대상 레지스트리
- Source Process : 권한 제어 대상 프로세스
- User or Group : 권한 제어 대상 사용자 또는 그룹
- Policies : 정책 적용 범위

## 10. Scripts

### 10.1. 정책 설명

## 10.2. 정책 생성

## General

Rule Name: Batch

Description:

Status: ☒ Enabled ☐ Disabled

## Definition

Platform: Windows

Script Definition: Script Type and Process

Script Type:

\*.cmd  
\*.bat

+ Add

- Remove

Script Process:

<System>\cmd.exe  
<Systemx86>\cmd.exe  
<YaraTags:cmd\_interpreter>\*

+ Add

- Remove












Rescan Computers: ☒ Yes 

스크립트 규칙을 지정하기 위한 스크립트 정책을 생성합니다.

- Rule Name : 정책 이름
- Discription : 정책 설명
- Status : 정책 사용 여부
- Platform : 정책 적용 OS
- Script Definition : 스크립트 유형 정의
  - File Association (Windows OS만 지원) : 응용 프로그램이 연결된 파일
  - Script Type and Process : 스크립트 및 프로세스 파일
- Script Type : 스크립트 파일 이름 및 확장자 지정
- Script Process : 스크립트 파일을 실행할 프로세스 지정
- Rescan Computer : 정책과 일치하는 컴퓨터 재확인

## 11. Yara

### 11.1. 정책 설명

	Yara Rule Name	Namespace ▲	Status	Description	Qualifiers
	Python Script Interpreter	Classification	Enabled	Identifies Interpreters for python scripts	<OnlyIf:Bit9Version:Atleast:8.0.0.2454>
	Microsoft HTML Application Interpreter	Classification	Enabled	Identifies Interpreters for HTML applications	
	Ruby Script Interpreter	Classification	Enabled	Identifies interpreters for Ruby scripts	
	Chrome Extension Interpreter	Classification	Enabled	Identifies interpreters for Chrome extensions	
	Mozilla Extension Interpreter	Classification	Enabled	Identifies interpreters for Mozilla extensions (Firefox browser)	
	UPX Packing detector	Classification	Enabled	Identifies UPX packed exes	
	Msiexec detector	Classification	Enabled	Identifies msiexec	
	FileHeader	IsInteresting	Enabled	File header for the IsInteresting rule set. Includes any import	
	Portable Executable	IsInteresting	Enabled	Identifies win32 portable executables and dlls	
	Windows Installers	IsInteresting	Enabled	Identifies windows installers (MSI and MSP)	
	Systems Management Server Installers	IsInteresting	Enabled	Identifies Microsoft SMS installers	

Yara 정책은 Yara 규칙을 통해 악성코드를 식별하여, 파일 및 스크립트 내용의 악성 여부를 인식하여 보호하는 정책입니다. App Control에서 사전 정의된 Yara 오픈소스 툴을 사용하여 콘텐츠 보호가 가능하며, 그 외 관리자가 Yara 규칙을 새롭게 생성하여 사용 가능합니다. Yara 정책의 경우, 악성코드 시그니처 식별하고 있어 환경에 대한 랜섬웨어 공격을 방지하는 데에 유용하게 사용됩니다.

### 11.2. 정책 생성



\* Name:

Namespace:  ⓘ

Description:

Qualifiers:  ⓘ

Status: ☐ Enabled ☒ Disabled

Rule:

## File Scanning

In order for this Yara rule to work, the tags defined need to be assigned to files.  
The agent can rescan known files, or just begin tagging new or modified files.  
Refer to the user guide for more information on rescanning files.

☐ Rescan known files

Detected Tags: (None) ⓘ

악성코드 식별을 위한 Yara 정책을 생성합니다.

- Name : 정책 이름
- Namespace : 정책 구분
  - Classification : 태그를 기반으로 Custom 정책을 사용하여 작업 수행하는 경우
  - IsInteresting : 자동으로 작업 수행하는 경우
- Description : 정책 설명
- Qualifiers : 정책을 적용할 센서 대상 정의 (작성한 조건에 맞는 센서를 대상으로 정책이 동작)
- Status : 정책 사용 여부
- Rule : 악성코드 식별에 사용할 Yara 규칙 입력
- Rescan known files (Classification 선택 시 사용) : 적용한 규칙에 해당되는 파일이 있는지, 센서가 아는 파일을 기준으로 재검사
- Full scan for new files (IsInteresting 선택 시 사용) : 적용한 규칙에 해당되는 파일이 있는지, 센서가 전체 시스템 기준으로 재검사
- Detected Tags : Carbon Black 에서 제공한 태그를 사용하여 정책 구분

## 12. Reputation

### 12.1. 정책 설명

#### Reputation Approval Settings

☒ Enable reputation approvals

☒ Approve applications with trust greater than or equal to:


☒ Approve publishers with trust greater than or equal to:

Select affected policies:

☐ All Current and Future Policies

☒ Selected policies

<input type="checkbox"/> Policy
<input type="checkbox"/> Default Policy
<input checked="" type="checkbox"/> SM-TEST
<input type="checkbox"/> Template Policy

 Save

Reputation 정책은 Carbon Black App Control에서 제공되는 파일 평판을 기반으로 파일 사용을 자동으로 승인하는 정책입니다.

Reputation 정책은 Carbon Black File Reputation 를 통해 제공되는 파일의 평판 신뢰도를 기준하여 승인되므로 Carbon Black File Reputation  
기능 활성화가 필요한 정책입니다.  
인증서와 응용 프로그램이 정책 적용 대상이 되며, 신뢰도의 기준을 단계별로 구분하여 선택 후 사용됩니다.

---

🔄버전 #26  
★생성 11 1월 2024 21:43:34  
✎수정 18 4월 2025 16:39:15