







- The security dashboard is a list of all security events on managed Windows endpoints. An event is created when a security module takes an action on a file. For example, the antivirus module blocks a suspicious file, or the containment module runs an unknown file in the container.
- The dashboard lets you view events by event date, by file name, or by device. You can also view a Valkyrie report on the file featured in the event.
- Valkyrie is a file analysis service that tests files with a range of static and behavioral checks. The service helps Comodo establish whether an unknown file is malicious or safe.
- This article explains how to view Valkyrie reports on files which created a security event.

Open the security dashboard

- Open Endpoint Manager
- Click 'Security Sub-Systems' > 'Security Dashboards'
- You can view events by event time, by file name, or by device:

The screenshot shows the security dashboard interface. At the top, there are tabs for 'Event View', 'File View', and 'Device View'. Below these are several action buttons: 'Action on Endpoint', 'Change Rating', 'File Details', 'Download Valkyrie Report', 'Check Valkyrie Details' (circled in red), and 'Export'. A search bar for 'file HASH' is present. Below the search bar is a table of events with columns: DATE TIME, COMPONENTS, ACTION, OS, DEVICE NAME, FILE NAME, FILE PATH, FILE HASH, INITIAL COMODO RATING, and CURRENT COMODO RATING. One event is highlighted with a red circle: 2019/10/29 10:01:11 AM, Containment, Run virtually, UxWin10x64..., iexplore.exe, C:\Prog..., 5D5586..., Unrecognized, Unrecognized. Below the table, the 'Check Valkyrie Details' button is clicked, opening a detailed report for the file 'iexplore.exe'. The report shows a 'CLEAN' verdict with a green checkmark icon. The report details include: File Name: 2018-11-20 14:05:51.339019, File Type: PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows, SHA1: 1f2d314337132a1f2fad1bd141a5897e1a976571, MD5: [redacted], First Seen Date: 2018-11-30 16:19:51 (2 month(s) 8 day(s) ago), Number of Clients Seen: 4, Last Analysis Date: 2018-11-30 16:19:51 (2 month(s) 8 day(s) ago), Human Expert Analysis Result: No human expert analysis verdict given to this sample yet, Verdict Source: Signature Based Detection.

- Select the event which interests you
- Click the 'Check Valkyrie Details' button
- The Valkyrie analysis opens in a new page. The page contains the results of each test, and a trust verdict from each test.






- 
 Copy URL To Clipboard
- 
 Export Results To PDF
- 
 View Virus Total Result
- 
 Send To Kill Chain Report
- 
 Send To Human Expert Analyst
- 
 Object To Human Expert Analysis Verdict
- 
 Download Human Expert Analysis Report
- 
 Analyze Again



MALWARE
Valkyrie Final Verdict

File Name: COT.exe
 File Type: PE32 executable (GUI) Intel 80386, for MS Windows
 SHA1: de4a245146279fac90d0cfb79e115288e4cd1fdd
 MD5: b4bacb4a585e09b8fd7f65a74f60de8c
 Number of Clients Seen: 1
 Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
 Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2017-09-02 06:06:09	Malware 
Static Analysis Overall Verdict	2017-09-02 06:07:16	No Threat Found 
Dynamic Analysis Overall Verdict	2017-09-02 06:07:36	No Threat Found 
File Certificate Validation	2017-09-02 06:08:10	Not Applicable 
Precise Detectors Overall Verdict	2017-09-02 06:07:36	No Match 

- The information in the report is covered in [this Valkyrie help guide page](#)
- You can also download a pdf version of the report by clicking the 'Download Valkyrie Report' button:

Event View File View Device View

Action on Endpoint Change Rating File Details **Download Valkyrie Report** Check Valkyrie Details Export

Search file HASH

DATE TIME	COMPONENTS	ACTION	OS	DEVICE NAME	FILE NAME	FILE PATH	FILE HASH	INITIAL COMODO RATING	CURRENT COMODO RATING
2019/10/29 01:33:35 PM	Application C...	File deleted	UxWin10x64...	UxWin10x64...	System.ni.dll	C:\Wind...	D2784D...	Trusted	Trusted
2019/10/29 01:33:35 PM	Application C...	File deleted	UxWin10x64...	UxWin10x64...	sRuGySFu.exe	C:\User...	480CAD...	Unrecognized	Unrecognized
2019/10/29 10:01:14 AM	Virtual Desk...	Switched to ...	UxWin10x64...	UxWin10x64...					
2019/10/29 10:01:11 AM	Virtual Desk...	Session ter...	UxWin10x64...	UxWin10x64...					
2019/10/29 10:01:11 AM	Containment	Run virtually	UxWin10x64...	UxWin10x64...	iesplora.exe	C:\Prog...	5D5586...	Unrecognized	Unrecognized

Advanced File Analysis System | Valkyrie 1 / 3

Download

VALKYRIE

NO THREAT FOUND

File Name: 2018-11-20 14:06:01.533017
File Type: PE32 executable (console) Intel 80386 Mono/Net assembly, for MS Windows
SHA256: 1879496393665291c24812c789f07251c196
MD5:
First Seen Date: 2018-11-30 10:38:09 UTC
Number of Clients Seen: 2
Last Analysis Date: 2018-11-30 10:38:09 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Valkyrie Automatic Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2018-11-30 10:38:02 UTC	No Match
Static Analysis Overall Verdict	2018-11-30 10:38:09 UTC	No Threat Found
Precise Detectors Overall Verdict	2018-11-30 10:38:09 UTC	No Match
File Certificate Validation		Not Applicable

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

DETECTOR	RESULT
Optional Header LoaderFlags field is valued illegal	Clean
Non-ascii or empty section names detected	Clean