

Cytomic Orion

V 2.07





































































Investigation Console
New event icons



Investigation console icons

The following table shows the icons for the different types of events collected on endpoints and other protected assets, what they mean, and the relationship between the icon in the version prior to 2.07 and the icon in use as of this version.

The first column is the icon before version 2.07 and the second is the new icon.

<v2.7	>=v2.7	Description
		CREATE PROCESS
		PE CREATED
		PE MODIFIED
		LIBRARY LOADED
		PE DELETED
		PE RENAMED
		DIR CREATED
		CMP CREATED
		CMP OPENED
		REGKEY EXE CREATED
		REGKEY EXE MODIFIED
		CREATE REMOTE THREAD
		EXPLOIT HOOK
		DEFAULT EVENTS ICON
<hr/>		
		DOWNLOAD
		NETWORK OPERATION - COMMUNICATIONS
		Creación de proceso, de un fichero desconocido con la protección en Lock sin Shell en memoria (no hay sesión de usuario en el equipo), no bloqueado.
		DOCUMENT OPEN (Data Access)
		REGISTRY OPERATION
		SCRIPT CREATED
		SCRIPT EXECUTED
		DETECTION
		COMMUNICATION BANDWIDTH
		SYSMON EVENT
		DNS OPERATIONS FAILED
		DEVICE OPERATION
		DETECTION & BLOCKED ITEM USER NOTIFICATION
		LOGIN OPERATION
		LOGOUT OPERATION
		ACTIONS TAKEN UNDER A DETECTION (BLOCKED, ANALYZED, SENT TO QUARANTINE)
<hr/>		
		CREATE PROCESS PID0
		CREATED PROCESS. PROCESS LOST
		CREATED PROCESS. WAITING
		CREATED REMOTE PROCESS