CYTOMIC

Cytomic Orion V 2.07

Consola de Investigación
Nuevos Iconos para los eventos

Cytomic.ai

Iconos consola de investigación

En la siguiente tabla se presentan los iconos de los diferentes tipos de eventos, recogidos de los endpoints y otros activos protegidos, su significado y la relación entre el icono antes de la versión 2.07 y a partir de esta versión.
La primera columna corresponde al icono antes del al versión 2.07 y la segundo a partir de esta.

<v2.7	>=v2.7	Descripción
		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
		DOWNDLOAD
		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)
		CREATE PROCESS PID0
		CREATED PROCESS. PROCESS LOST
		CREATED PROCESS. WAITING
		CREATED REMOTE PROCESS