

THREAT EMULATION REPORTS IN SPLUNK

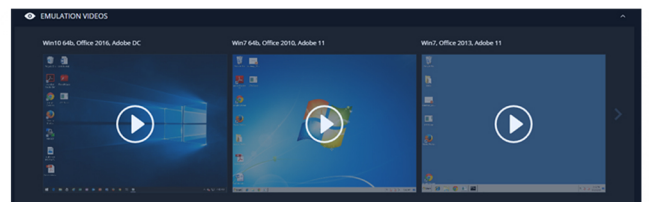
POWERFUL NETWORK FORENSICS FOR SOC ANALYTICS

Check Point delivers easy to understand, automated malware analysis reports that can be accessed directly from your Splunk console.



ADVANCED FORENSICS

Uncover enriched threat intelligence including the attack story and flow, related IoCs, MITRE ATT&CK tactics, malware DNA, emulation videos and more!



SUSPICIOUS ACTIVITIES

CATEGORY	COUNT	DESCRIPTION
Data Loss	1	The program changes file attributes
Don't Show Hidden Files	1	The program sets files as hidden files
Evasion	1	Observe a program that creates a new process
Evasion	1	Observe a program that opens its own process
Evasion	1	The program attempts to directly detect debuggers
Evasion	1	The program calls the dynamic load function dynamically
Evasion	1	The program creates a process in a suspended state
Evasion	1	The program deliberately waits for a long period
Evasion	1	The program dynamically calls imported functions
Evasion	1	The program loads NTDL
Evasion	1	The program opens a foreign process

MITRE ATTACK

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFILTRATION	COMMAND & CONTROL	IMPACT
	Windows Management Instrumentation	Registry Run Keys Startup Folder	Bypass User Account Control	Process Hollowing	Credentials in Files	Security Software Discovery		Email Collection			
	Execution Through API	Change Default File Association	Process Injection	Bypass User Account Control	Credentials from Web Browsers	System Information Discovery		Data from Local System			
	Regsvcs Regasm	AppCert DLLs	AppCert DLLs	Software Packing	Credentials in Registry	Application Window Discovery					
		Windows Management Instrumentation Event Subscription		Process Injection							
				Disabling Security Tools							
				Regsvcs Regasm							

GET STARTED TODAY!

For setup details, [click here](#) or go to Check Point's SecureKnowledge base and search for sk122323.