ACTIONABLE INSIGHTS WITH UNPARALLELED FIM VISIBILITY

Tripwire invented File Integrity Monitoring, however that's only one reason why so many consider "Tripwire" synonymous with this critical security control. Tripwire® Enterprise has taken FIM far beyond basic change auditing. It not only collects highly detailed change data in real time, it also adds change intelligence and automated remediation and then integrates this data with the other critical security controls found in Tripwire's integrated solutions.

Tripwire's industry leading FIM solution not only detects changes to files, but helps IT remediate unauthorized changes, reduce risk and maximize uptime.

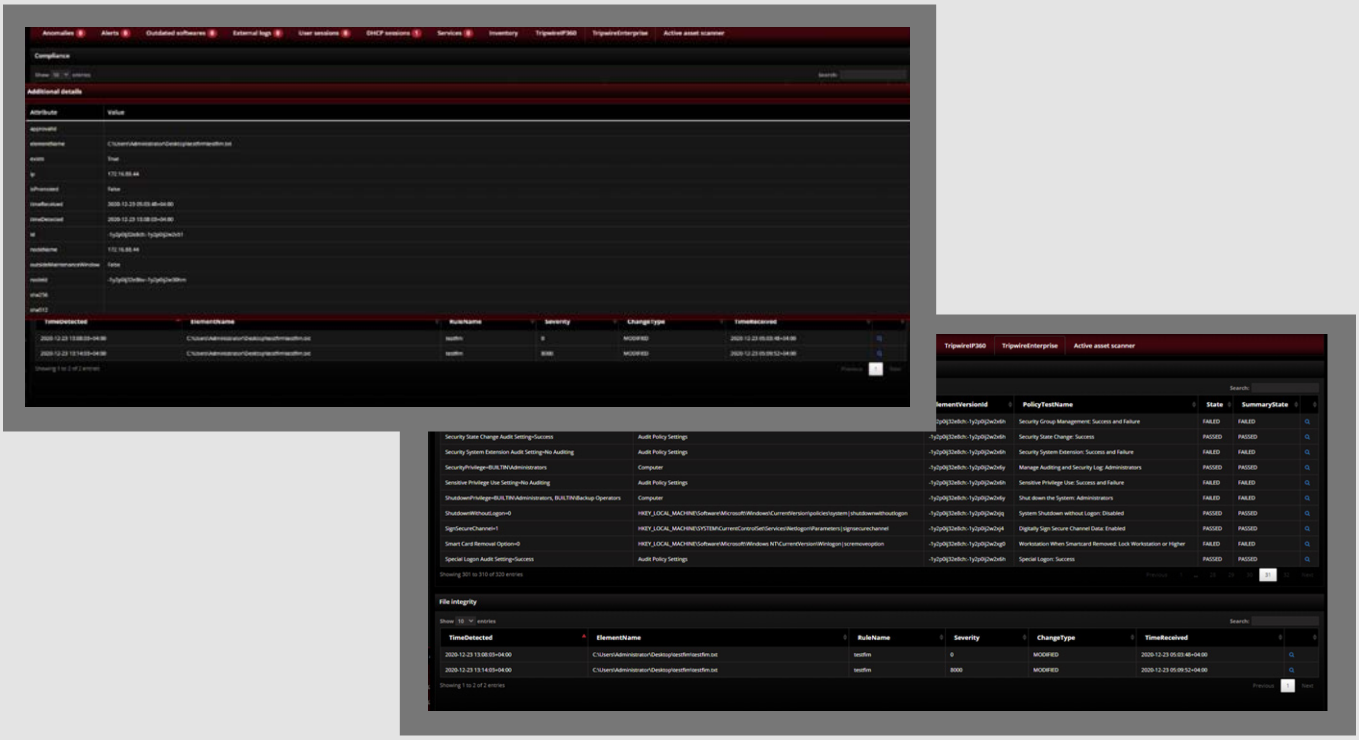
LinkShadow® Cyber Security Analytics Platform is designed to manage threat in real-time utilizing Artificial Intelligence-based Machine Learning to analyze events, perform UEBA, cutting-edge threat hunting & provides threat anticipation.

LinkShadow® provides unparalleled detection of the most sophisticated threats which enhances an organization’s defense against advanced cyber-attacks, zero-day malware and ransomware. The chance of an attacker passing through your network is virtually nonexistent.

INTEGRATION STORY:
LINKSHADOW - TRIPWIRE

LinkShadow® integrates with Tripwire to complete the full cycle of User and Entity Behavioral Analytics and threat hunting to get the optimum benefit of Tripwire Enterprise technology along with proactive threat detection.

LinkShadow gets full visibility from Tripwire Enterprise around system change activities. LinkShadow injects this intelligence into the advanced machine learning algorithms to identify suspicious and anomalous activities based on the behavioral analysis. LinkShadow act proactively to system change activities that might indicate an early stage of an attack for faster resolution and forensic value.



Additional details

Attribute	Value
approvalId	
elementName	C:\Users\Administrator\Desktop\testfim\testfim.txt
exists	True
ip	172.16.88.44
isPromoted	False
timeReceived	2020-12-23 05:03:48+04:00
timeDetected	2020-12-23 13:08:03+04:00
id	-1y2p0ij32e8ch:-1y2p0ij2w2x51
nodeName	172.16.88.44
outsideMaintenanceWindow	False
ruleId	-1y2p0ij32e8ev:-1y2p0ij2w38hm
sha256	
sha512	

TimeDetected	ElementName	RuleName	Severity	ChangeType	TimeReceived
2020-12-23 13:08:03+04:00	C:\Users\Administrator\Desktop\testfim\testfim.txt	testfim	0	MODIFIED	2020-12-23 05:03:48+04:00
2020-12-23 13:14:03+04:00	C:\Users\Administrator\Desktop\testfim\testfim.txt	testfim	8000	MODIFIED	2020-12-23 05:09:52+04:00

Showing 1 to 2 of 2 entries

		ElementVersionId	PolicyTestName	State	SummaryState
		-1y2p0ij32e8ch:-1y2p0ij2w2x6h	Security Group Management: Success and Failure	FAILED	FAILED
Security State Change Audit Setting=Success	Audit Policy Settings	-1y2p0ij32e8ch:-1y2p0ij2w2x6h	Security State Change: Success	PASSED	PASSED
Security System Extension Audit Setting=No Auditing	Audit Policy Settings	-1y2p0ij32e8ch:-1y2p0ij2w2x6h	Security System Extension: Success and Failure	FAILED	FAILED
SecurityPrivilege=BUILTIN\Administrators	Computer	-1y2p0ij32e8ch:-1y2p0ij2w2x6y	Manage Auditing and Security Log: Administrators	PASSED	PASSED
Sensitive Privilege Use Setting=No Auditing	Audit Policy Settings	-1y2p0ij32e8ch:-1y2p0ij2w2x6h	Sensitive Privilege Use: Success and Failure	FAILED	FAILED
ShutdownPrivilege=BUILTIN\Administrators, BUILTIN\Backup Operators	Computer	-1y2p0ij32e8ch:-1y2p0ij2w2x6y	Shut down the System: Administrators	FAILED	FAILED
ShutdownWithoutLogon=0	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\policies\system|shutdownwithoutlogon	-1y2p0ij32e8ch:-1y2p0ij2w2xjq	System Shutdown without Logon: Disabled	PASSED	PASSED
SignSecureChannel=1	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters|signsecurechannel	-1y2p0ij32e8ch:-1y2p0ij2w2xj4	Digitally Sign Secure Channel Data: Enabled	PASSED	PASSED
Smart Card Removal Option=0	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon|scremoveoption	-1y2p0ij32e8ch:-1y2p0ij2w2xg0	Workstation When Smartcard Removed: Lock Workstation or Higher	FAILED	FAILED
Special Logon Audit Setting=Success	Audit Policy Settings	-1y2p0ij32e8ch:-1y2p0ij2w2x6h	Special Logon: Success	PASSED	PASSED

Showing 301 to 310 of 320 entries

File integrity

Show 10 entries

TimeDetected	ElementName	RuleName	Severity	ChangeType	TimeReceived
2020-12-23 13:08:03+04:00	C:\Users\Administrator\Desktop\testfim\testfim.txt	testfim	0	MODIFIED	2020-12-23 05:03:48+04:00
2020-12-23 13:14:03+04:00	C:\Users\Administrator\Desktop\testfim\testfim.txt	testfim	8000	MODIFIED	2020-12-23 05:09:52+04:00

Showing 1 to 2 of 2 entries

HIGHLIGHTS:

- Detecting early stages of threats for faster MTTR
- Gaining visibility on the remote workers
- Detecting malicious file hashes with intelligence feeds
- Correlating unusual file modifications on multiple systems simultaneously

www.tripwire.com