Mandiant

AUDIT LOG RECORD CATEGORIZATION

The following values are used in the Section and Action Type columns of the Audit log. The Notes column describes the action completed by the user listed in the User column.

Section	Action Type	Notes
action_profiles	index	A user browsed to the MITRE ATT&CK Dashboard
actions	approve	An Action was approved
actions	create	An Action was created
actions	create_sleep_action	A sleep Action (in Action Queue) was created
actions	destroy	An Action was deleted
actions	run	A Job was run
actions	run_queue	Actions from the queue were run
actions	update_sectech_logo	The logo on a Security Technology was updated
alert_formats	create	A Monitor Notification Format was created
alert_profiles	create	A Monitor Notification Profile was created
analyze	gauge_page	User browsed to the Gauges
analyze	heat_map	User browsed to the Heat Map
bulk_jobs	create_bulk_job	A bulk Job was created
email_profiles	create	An Email Profile was created
endpoint_files	create	A file was added to the Endpoint Library
endpoint_files	download	A file was download from the Endpoint Library
endpoint_products	update	An Endpoint Security Technology was updated
event_filter_rules	create	Creating an Event Filter Rule
event_filter_rules	destroy	Deleting an Event Filter Rule
event_filter_rules	update	Updating an Event Filter Rule
file_transfer_libraries	create	A File was created

Section	Action Type	Notes
file_transfer_libraries	create_action	An Action was created from a File
file_transfer_libraries	create_protected_action	A Protected Action was created from a File
file_transfer_libraries	update	A File was updated
integration_settings	update	An Integration was updated
integrations	create	An Integration was added
integrations	run_test	An Integration's test was run
integrations	update	An Integration was updated
job_actions	update	The include/excude from reports setting on a Job Action was updated
jobs	cancel	A Job was canceled
jobs	clear_queue_all	The Job Queue was cleared
jobs	destroy	A Job was deleted
jobs	run_again_modal	A Job was run using the Run Again option
jobs	run_now	A Job was created and is running
jobs	show	A user viewed a Job
license	verify_license	The License info was reviewed to verify it was still valid
messages	destroy	A Flash card from a User's Messages was deleted
monitor	update_data	A Monitor was updated
monitor_defs	v2_update	A Monitor was updated
network_devices	update	A Network Security Technology was updated
nodes	connect_result	An Actor was registered
nodes	create	An Actor was added
nodes	destroy	An Actor was removed
nodes	destroy_bulk_token	A Bulk Registration token was deleted
nodes	destroy_pending	A Pending Actor token was deleted
nodes	update	An Actor was updated

Section	Action Type	Notes
panel_dashboards	update	A panel on the TAAM Dashboard was updated
registrations	update	A User's password was changed
report_builder	create	A report in Report Builder was created
report_builder	destroy	A report in Report Builder was deleted
report_builder	update	A report in Report Builder was updated
reports	data_exfil	A user viewed the Data Exfil Report
reports	malicious_transfer	A user viewed the Malicious File Transfer Report
reports	summary	A user viewed the Summary Report
scheduled_actions	cancel	A scheduled Job Action was deleted
scheduled_actions	update	A scheduled Job Action was updated
security_technologies	run_discovery	The "Discover Devices" option on a Job was run
security_zones	create	A Security Zone was created
security_zones	update	A Security Zone was updated
sessions	create	A session (process run by the Director) for a user was started
sessions	destroy	A session (process run by the Director) for a user ended
sessions	login	A user logged into the Director
sessions	login_failure	A user entered the incorrect password
sessions	logout	A user logged out of the Director
settings	advanced_update	The Advanced Setting were updated, including changing the Event Filter type for integration event filter rules
settings	check_update	The Update Service was checked to see if there was a new update
settings	content_import	Content was imported
settings	create_backup	A Backup was created
settings	create_operational_notification	An Operational Status Notification was created

Section	Action Type	Notes
settings	create_update_dim_rule	A pass/fail rule for a specific Dimension was created
settings	create_update_vid_rule	A pass/fail rule for a specific VID was created
settings	destroy_operational_notification	An Operation Status Notification was deleted
settings	download_update	An update from the Update Service was downloaded
settings	import_content_apply	Imported Content was applied
settings	login_update	Login Requirements were updated
settings	operational_status_update	An Operation Status Notifcation was updated
settings	run_update	A Director update was applied
settings	ssl	An SSL certificate was added
settings	update_service_running	The system checked to see if an update is running (automated check during the update process)
settings	update_status	A System Update status was updated
settings	verify_license	The License info was reviewed to verify it was still valid
settings	verify_update	An update patch was Uploaded & check to see if it was valid
simulations	create	A Sequence or Evaluation was created
simulations	destroy	A Sequence or Evaluation was deleted
simulations	run_all_content	Run All Actions from the Evaluation Library was used
simulations	update	A Sequence or Evaluation was updated
template_actions	create	An Action from a File Template was created
template_actions	update	An Action based on a File Template was updated
templates	create	A File Template was created
templates	update	A File Template was updated
threat_actor_references	create	A Threat Actor (manual and when Integration syncs) was created

Section	Action Type	Notes
threat_actor_references	update	A Threat Actor (manual and when Integration syncs) was updated
threat_intel_integrations	create	A TIP Integration was added
threat_intel_integrations	update	A TIP Integration was updated
topology	check_time_sync	The Actor's time sync (with the Director) was checked
topology	pull_info_node	**Refresh Actor Info** was clicked and the Actor's info was updated
topology	pull_talk_info_node	An Actor's CTTA info was updated
upload	cancel	a PCAP upload during Action creation was canceled
upload	create_pcap_action	A PCAP Action (by uploading a PCAP) was created
upload	destroy_all	All in-progress PCAP Actions were deleted (uploading a new PCAP during the Action creation process)
upload	destroy_conversations	While creating a PCAP Action, conversations from a PCAP file were deleted
users	create	A user was added to the Director
users	destroy	A user's access was disabled or the user account was deleted
users	enable_user	A user's access was enabled
users	update	A user was updated
users	user_prefs_update	A user updated their preferences