Ntiva

SaaS Alerts

DATA SHEET / LEVELS OF SERVICE

www.ntiva.com

Ntiva SaaS Alerts

Ntiva SaaS Alerts is an automated, SaaS security threat detection and response tool, which exposes advanced threats and immediately takes action to keep clients SaaS environments safe. This solution allows Ntiva to react promptly to any potential SaaS security incidents that may disrupt a client's business operations. Ntiva's SaaS Alerts monitoring and automatic remediation capabilities will enhance our client's security posture for their SaaS applications. Document the current state workflow and diagnose problems/pain points.

SUMMARY

Ntiva's SaaS alerts is a product responsible for handling alerts generated by the platform's monitoring and alerting system. This product is designed to log, alert and potentially respond automatically to alerts promptly and effectively, ensuring that any issues or problems are addressed quickly.

The SaaS Alerts product includes the following features:

Logging

Ntiva SaaS Alerts will collect logs for over 200 different events that occur within the supported SaaS applications. This information will be retained for 365 days of the event date to help diagnose issues and conduct forensics. This allows Ntiva to search and filter alert logs based on various criteria, such as severity level, User, or time frame, to quickly identify and address issues.

Alerting

Ntiva SaaS Alerts offers unified, 24/7 real-time monitoring to protect against data theft, data-at risk and bad actors. This feature sends notifications to Ntiva's NOC when an alert is triggered via ConnectWise Manage via an API integration. This feature helps prioritize alerts based on severity and impact, allowing the response team to focus on critical issues first. This will also manage the response to an alert by tracking the status of the incident, assigning tasks to team members, and providing a centralized location for communication and collaboration.

Respond

Ntiva's SaaS alerts respond module is a component that is responsible for responding to detected threats within seconds of a breach with pre-configured steps to stop bad actors from inflicting damage. If a breach is deemed highly likely the users account will automatically be blocked and a ticket will be created for Ntiva to act.

Reporting

Ntiva SaaS Alerts reporting of user behavior and SaaS application events provides a comprehensive and timely view of the current state of SaaS security for our clients. The reporting functionality of a Ntiva SaaS Alerts system includes reports for SaaS Cyber Assessment, SaaS Risk Reports, Account Details, External Shared Files, File Share Events, Alerts, and MFA Settings report. These reports can be run ad hoc or

scheduled to be sent to specific groups of people (internal and external) on a regular basis.
Ntiva's SaaS Alerts also include an Interactive risk dashboard that provides a visual representation of alert data through interactive dashboards, allowing system administrators to easily view and analyze data.

HOW NTIVA SAAS ALERTS WORK

This solution creates the ability to deeply monitor, alert and respond to compatible SaaS based solutions 24 hours a day. Ntiva SaaS Alerts uses approved API connections to establish secure access to SaaS solutions. This connection allows the ability to read logs and respond to potential breaches based on predefined conditions.

Our tool will categorize and store all the log entries into three thresholds:

Low Alerts

- Low alerts are gathered for reporting purposes as well as the ability to analyze past actions. These are deemed non-actionable alerts and will not generate a ticket into ConnectWise Manage. An example of Low alert is successful login from a known and approved location. These alerts are maintained in Ntiva's SaaS Alerts solution for 365 days.

Medium Alerts

- These are considered an actionable alert that requires investigation to determine if an actional breach is occurring. These are deemed a P1 for priority and will create a ticket on the NOC board for action. An example of a medium alert is an email rule being created. While this can be a typical action by a user it is also an action taken by bad actors after a user breach has occurred. Ntiva will validate with the user that this was a valid action as well as use locations of successful authentications to determine if a user has been compromised.

Critical Alerts

- These are considered actionable alerts that require investigation to determine if an actional breach is occurring. These are deemed a P1 for priority and will create a ticket on the NOC board for action. An example of a critical alert is a user being elevated to administrative privileges. While this could be a valid action, Ntiva will investigate this alert to verify this should have occurred. As you will note, there is little difference between Critical and Medium alerts, as they both create a ticket for immediate action.

Ntiva SaaS Alerts also have the ability to take immediate action if pre-defined conditions occur within the SaaS solutions logs. **See below:**

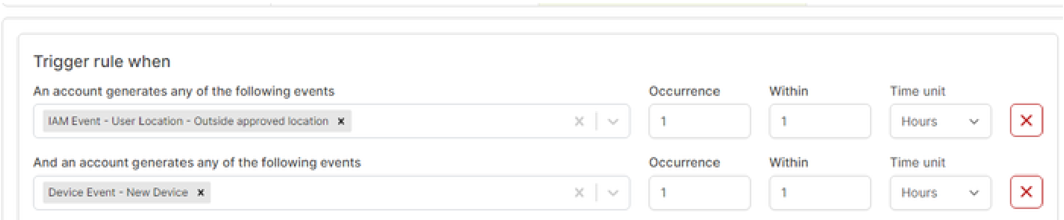
RESPOND:

Will analyze events that occur within a supported SaaS solution and if certain conditions occur in the pre-defined time period a set of actions will automatically be performed. Example of available actions are:

- **Expire Account logins** – Logs out all connections for the user within the SaaS solutions.
- **Change User Password** – Automatically change a user's password.
- **Setup User MFA** – Enable MFA to be setup for the user.
- **Block Sign-in** – Blocks any new authentications for the user's account.

This provides the ability to proactively secure the users account while a critical ticket is created and added to the NOC's board within ConnectWise Manage.

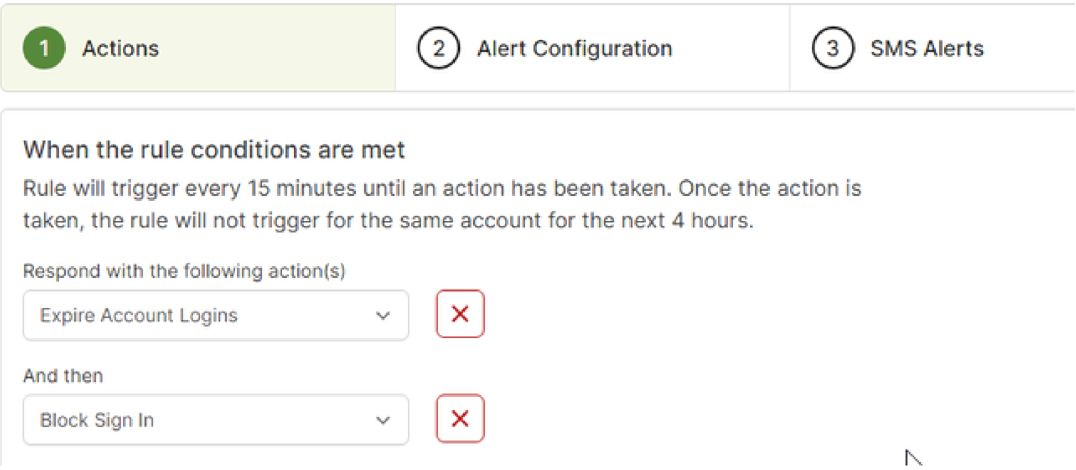
Example of a Respond Condition:



Trigger rule when

An account generates any of the following events	Occurrence	Within	Time unit
IAM Event - User Location - Outside approved location	1	1	Hours

And an account generates any of the following events	Occurrence	Within	Time unit
Device Event - New Device	1	1	Hours



When the rule conditions are met

Rule will trigger every 15 minutes until an action has been taken. Once the action is taken, the rule will not trigger for the same account for the next 4 hours.

Respond with the following action(s): Expire Account Logins

And then: Block Sign In

- This rule will automatically log out all current connections and block future logins if an account is accessed outside the approved locations and is a new device for that user, which is deemed highly likely a breach has occurred.

DEPLOYMENT

Ntiva's SaaS Solution will be deployed by the onboarding team for any new or renewed client agreements. Any Ad Hoc additions outside new or renewal contracts for Ntiva's SaaS Alert protection will be configured by the Product Management Team.

REPORTING

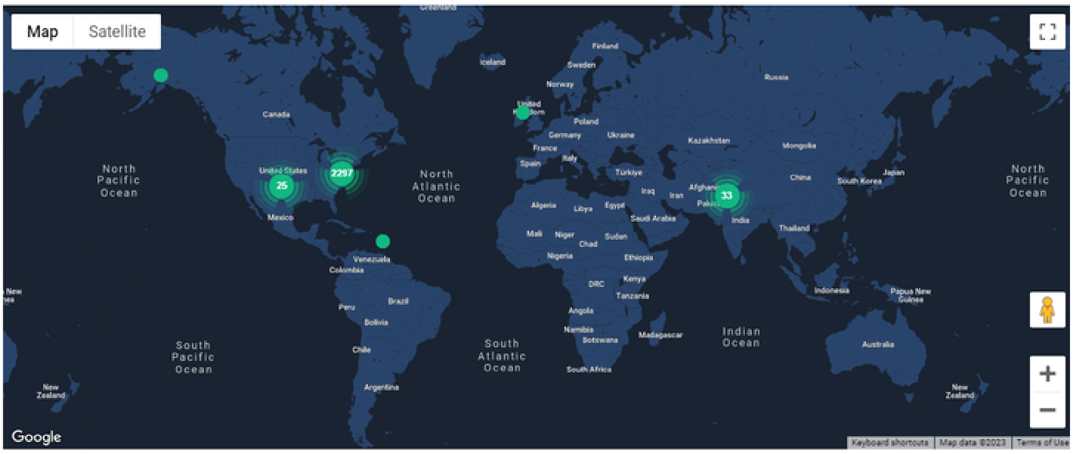
Ntiva's SaaS Alerts solution provides robust reporting that can help clients understand the importance of further security enhancements. The reporting will also help educate the client on current usage of their SaaS based solutions. Reporting can be requested from the Product Management team to be sent to the Account Manager, VCISO or VCIO on an ad hoc or scheduled occurrence.

Current Reports are:

SaaS Cyber Assessment which contains:

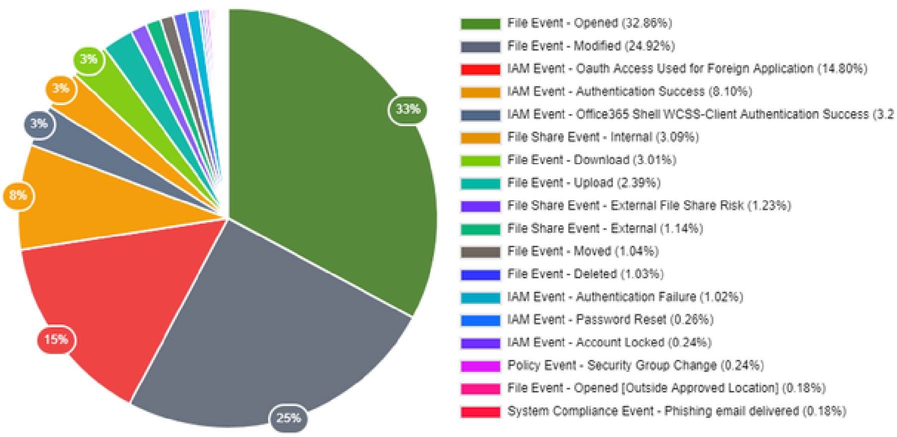
Account Logins & Events

Logins	Logged Events	Medium Alerts	Critical Alerts
2361	28330	25	1



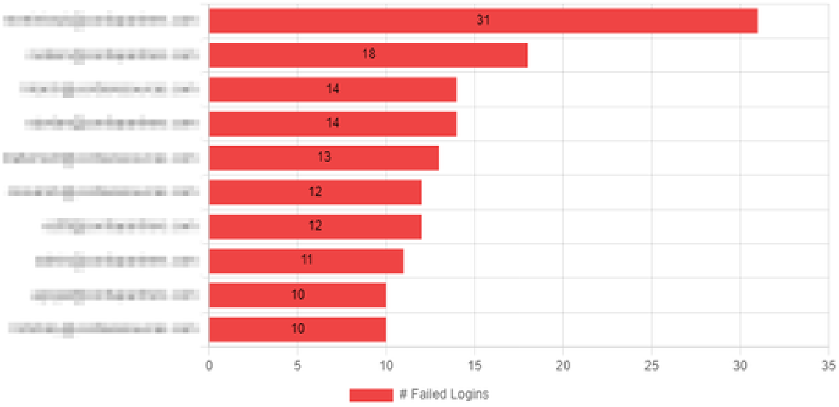
Incident breakdown

This pie chart displays all of the different types of events we have seen occur during this reporting period.



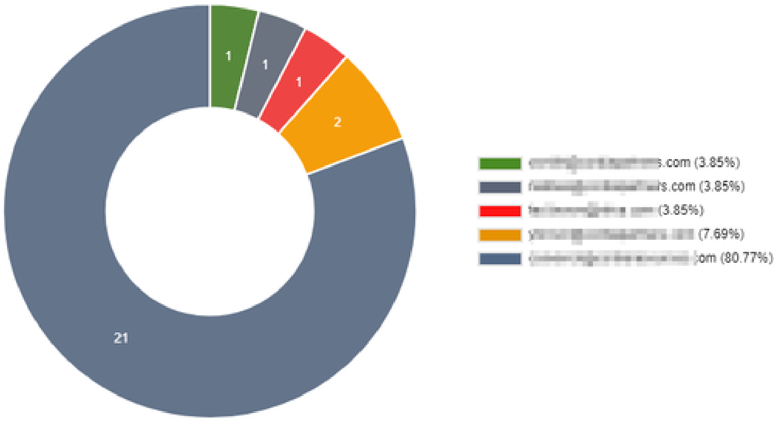
Failed logins

The graph below displays the top 10 users within your company who were unable to login to their accounts. The chart displays the number of failed attempts while trying to login to their accounts



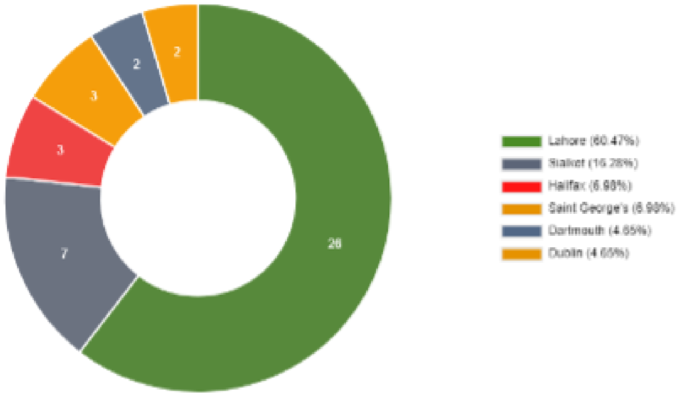
Account alerts

Below is a chart displaying top 10 Accounts within your business that triggered the most alerts in the selected period.



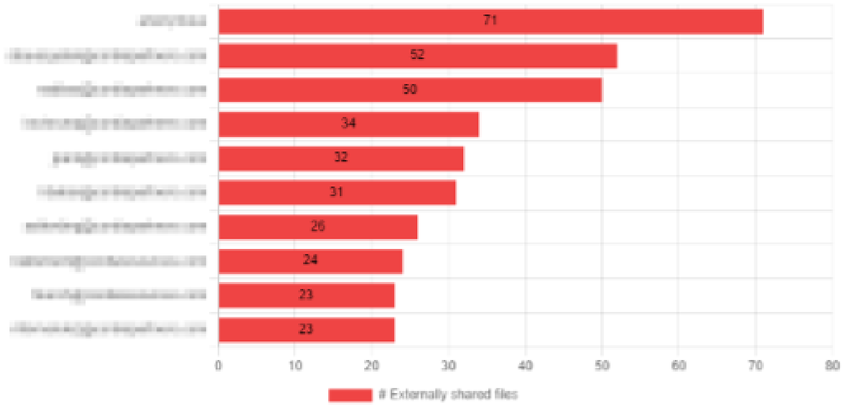
Unapproved locations

Below are the top 10 locations where we have detected and prevented account takeover attempts for your organization.

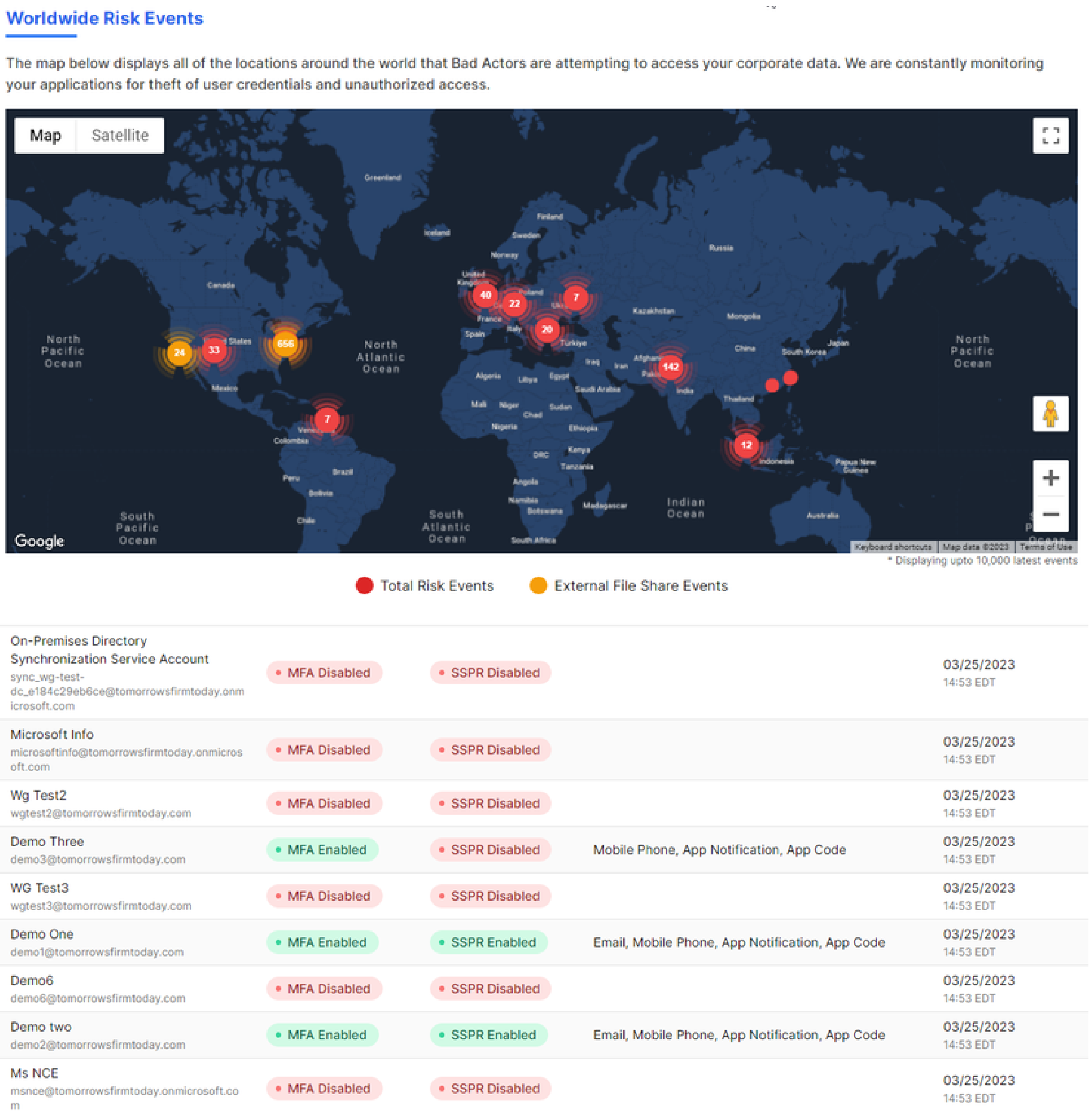


Externally Shared File Events

The chart below displays the top 10 accounts within the organization that have the most number of external file share events. Since the chart is showing events, the same file shared multiple times will add to the event count. Account names displayed as a unique id instead of an email address are Anonymous account ids identified by MSFT.



SaaS Risk Report which contains:



Worldwide Risk Events

The map below displays all of the locations around the world that Bad Actors are attempting to access your corporate data. We are constantly monitoring your applications for theft of user credentials and unauthorized access.

* Displaying upto 10,000 latest events

● Total Risk Events ● External File Share Events

On-Premises Directory Synchronization Service Account sync_wg-test-dc_e184c29eb6ce@tomorrowsfirmtoday.onmicrosoft.com	● MFA Disabled	● SSPR Disabled		03/25/2023 14:53 EDT
Microsoft Info microsoftinfo@tomorrowsfirmtoday.onmicrosoft.com	● MFA Disabled	● SSPR Disabled		03/25/2023 14:53 EDT
Wg Test2 wgtest2@tomorrowsfirmtoday.com	● MFA Disabled	● SSPR Disabled		03/25/2023 14:53 EDT
Demo Three demo3@tomorrowsfirmtoday.com	● MFA Enabled	● SSPR Disabled	Mobile Phone, App Notification, App Code	03/25/2023 14:53 EDT
WG Test3 wgtest3@tomorrowsfirmtoday.com	● MFA Disabled	● SSPR Disabled		03/25/2023 14:53 EDT
Demo One demo1@tomorrowsfirmtoday.com	● MFA Enabled	● SSPR Enabled	Email, Mobile Phone, App Notification, App Code	03/25/2023 14:53 EDT
Demo6 demo6@tomorrowsfirmtoday.com	● MFA Disabled	● SSPR Disabled		03/25/2023 14:53 EDT
Demo two demo2@tomorrowsfirmtoday.com	● MFA Enabled	● SSPR Enabled	Email, Mobile Phone, App Notification, App Code	03/25/2023 14:53 EDT
Ms NCE msnce@tomorrowsfirmtoday.onmicrosoft.com	● MFA Disabled	● SSPR Disabled		03/25/2023 14:53 EDT

Below is a summary of what is monitored with each level of service:

Alerts	Description	Monitor	Alert	Respond
New Device Outside Approved Locations	User sign in activity contains unfamiliar properties, such as a new country never before signed in from, concurrent sessions from different geographical regions and from an unfamiliar device.	●	●	●
Possible Indicators of Compromise	Auto-forwarding or email forwarding rule created AND user is logging in from an unapproved location.	●	●	●
Brute Force Successful Attack	Users account has 30 failed login attempts in one hour and then a successful login.	●	●	●
Account Lock Protection	Alert is triggered if users account has 30 failed login attempts in one hour.	●	●	
An Application API connection Has Failed	Ntiva's SaaS alerts has lost connection to monitored application.	●	●	
IAM Event - Conditional Access Violation	A condition of IAM access has been violated (Microsoft specific).	●	●	
Custom Compliance Event-High	Critical O365 Custom Compliance Event violated.	●	●	

Alerts	Description	Monitor	Alert	Respond
IAM Event - Multi-Factor Authentication Disabled	MFA has been turned OFF by a user.	●	●	
IAM Event - Multiple Password Reset	A users PW has been reset more than 3 times in one hour.	●	●	
System Compliance Event - Email Forwarding	Email forwarding has been configured.	●	●	
System Compliance Event - Email Sending Restriction	Number of outbound emails has exceeded the restriction amount.	●	●	
System Compliance Event - Exchange Admin	Exchange Admin has been added.	●	●	
System Compliance Event - Exchange Forwarding	Forwarding checkbox has been clicked in Exchange.	●	●	
System Compliance Event - User Restriction Email	User has exceeded outbound sending limits.	●	●	
Policy Event-Admin Access Granted	User has been given admin credentials.	●	●	
Email Event-Email Rule Enabled	Email rule was created on user's mailbox.	●	●	

Alerts	Description	Monitor	Alert	Respond
IAM Event-Multi-Factor Authentication Disabled	MFA has been turned OFF by a user.	●	●	
System Compliance Event-Email Limit	Email size limit exceeds "xyz" amount.	●	●	
System Compliance Event-Unusual Sending Activity	Items are being sent from an unfamiliar location in MSFT.	●	●	
Add Mailbox Permission	A mailbox permission to view or send an email on behalf of an user was added in Microsoft Exchange.	●		
Add Recipient Permission	A new recipient permission was added to have full access, read or sent emails on behalf of another user.	●		
Custom Compliance Event-Medium	Medium O365 Custom Compliance Event violated.	●		
IAM Event-Multi-Factor Authentication Enabled	MFA has been turned ON by a user.	●		
IAM Event-Multiple Account Locks	User account has been locked more than 3 times in one hour.	●		
IAM Event-User Location-Outside Approved Location	This user is successfully logged in from an area outside an approved location set within SaaS Alerts. ***This is critical!!***	●		

Alerts	Description	Monitor	Alert	Respond
Policy Event-Security Group Change	This user's security group has changed.	●		
Custom Compliance Event-Low	Low O365 Custom Compliance event violated.	●		
Data Loss Prevention Event	Prevented DLP event.	●		
IAM Event - Unknown Actor Is Attempting To Access Domain	An unknown actor is trying to guess the account name format for this domain.	●		
File Event-Download	A file has been downloaded.	●		
File Event-Emptied From Recycle Bin	All deleted files were removed from the Recycle Bin.	●		
File Event-Permanent Deletion	A file was deleted permanently, and cannot be restored from Recycle Bin.	●		
File Event-Moved	A file was moved to a different location.	●		
File Share Event-External	A file has been opened.	●		

Alerts	Description	Monitor	Alert	Respond
File Share Event-Internal	A file has been shared within the organization.	●		
Email Event-Forwarding Rule Changed	Event forwarding rule has been changed.	●		
Email Event-Forwarding Rule Deleted	Event forwarding rule has been deleted.	●		
IAM Event-Authentication Success	User successfully authenticated when logging into their account.	●		
IAM Event-Multiple Login Connections From Different IP Addresses	A user is logged into multiple SaaS apps at the same time, resulting in an impossible travel type scenario.	●		
IAM Event-Password Reset	The users password has been reset one time within an hour.	●		

Ready to Experience the Difference? Get Started with SaaS Alerts Today!

Take control of your software-as-a-service landscape and ensure seamless operations with our powerful monitoring platform. Empower your team and make downtime a thing of the past.

CONTACT US TO GET STARTED

www.ntiva.com