


SHADOWSPEAR SAAS MONITORING REPORT

SPEAR[▲]TIP


A company of  ZURICH[®]

Account Logins & Events




Logins

29655




Logged Events

120066



Medium Alerts

13



Critical Alerts

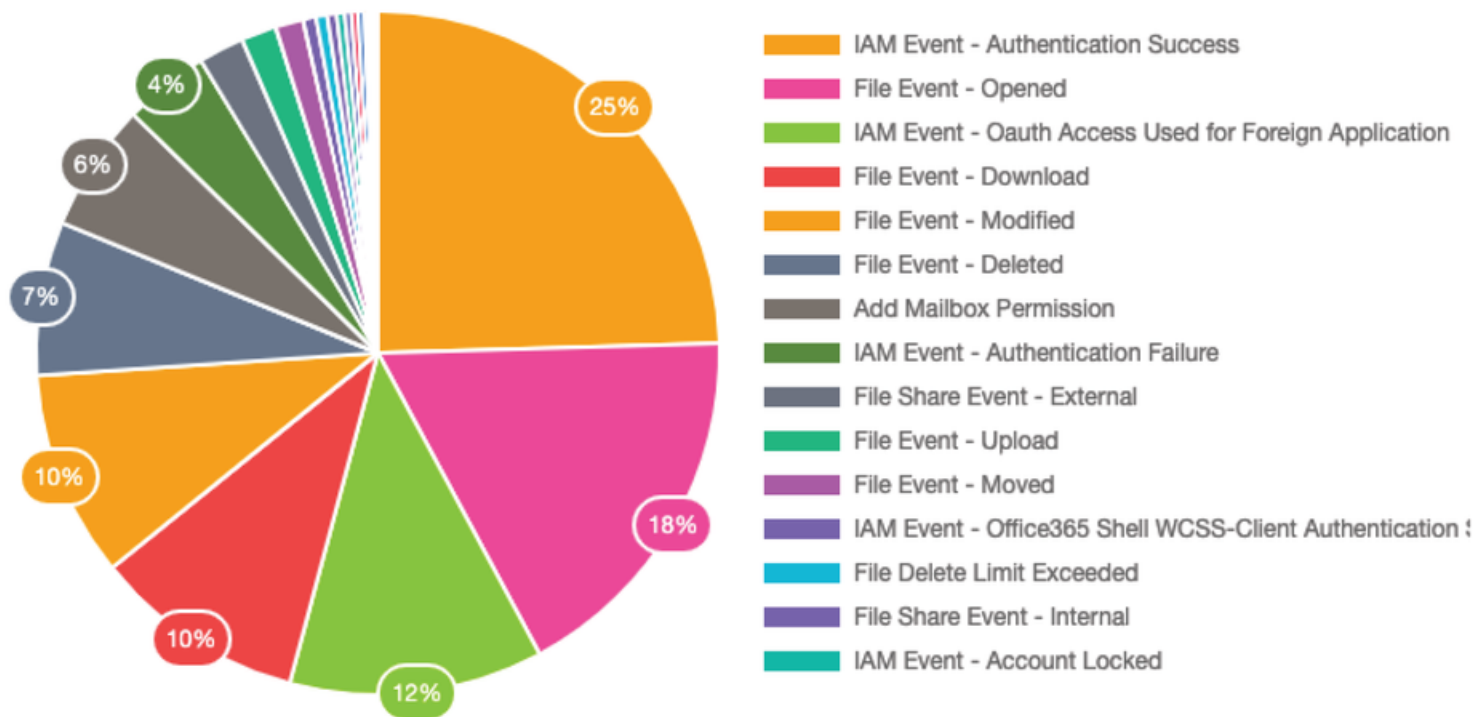
73



● Low Events ● Medium Alerts ● Critical Alerts

Incident breakdown

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

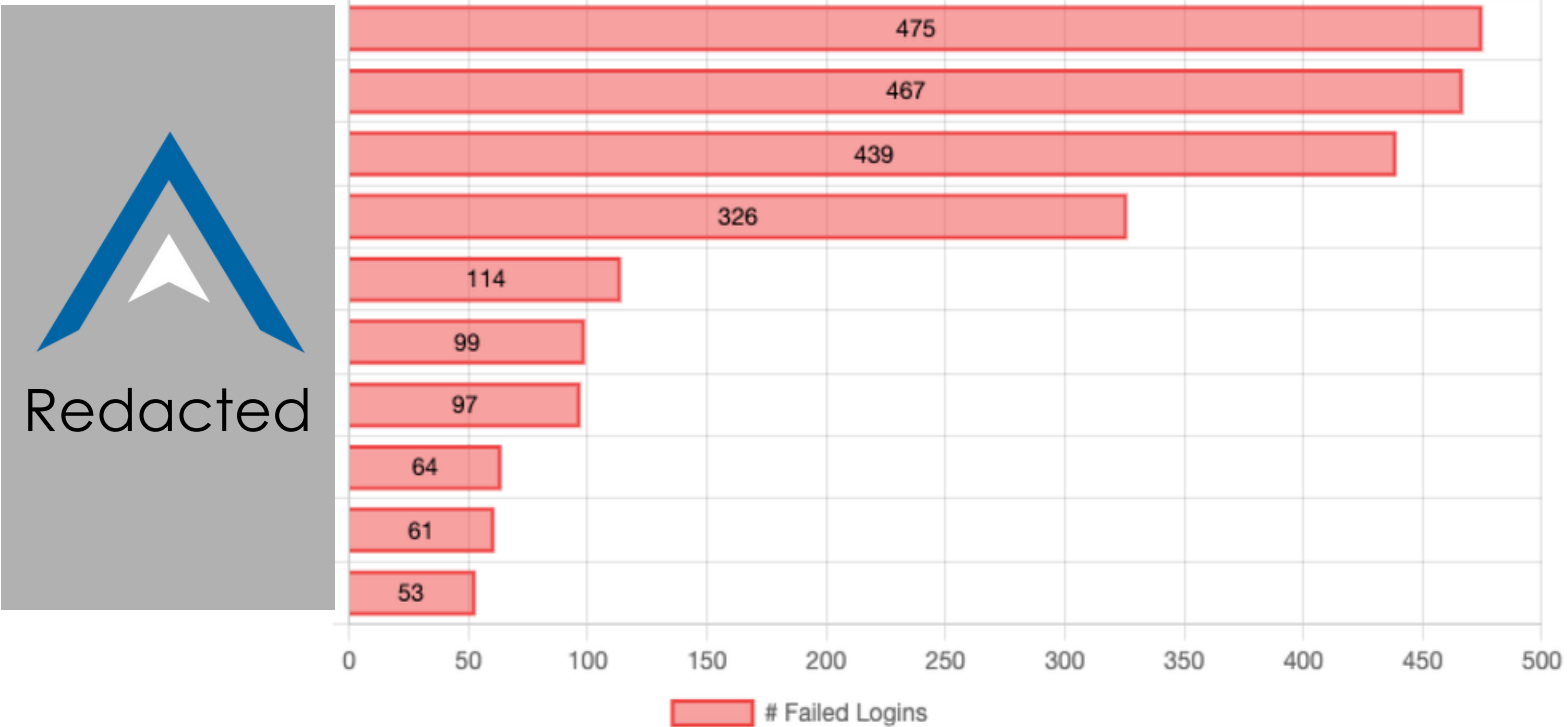


Our continued monitoring of your applications and data provide us a comprehensive and a timely view of the current state of SaaS application security and data.

SaaS Alerts MSFT	Microsoft	account.locks	05/15/2023 19:18 EDT	at_af3@saas alerts.net	107.170.58.26	Digitalocean LLC	New York City, NY, US	Agent - Chrome / Windows 10 / Method - Password / Activity - Login:login	IAM Event - Account Locked	
SaaS Alerts MSFT	Microsoft	login.failure	05/15/2023 19:18 EDT	at_af3@saas alerts.net	107.170.58.26	Digitalocean LLC	New York City, NY, US	OfficeHome from Chromium Browser for Windows NT 10.0 Auth Method: Password Succeeded: false Result detail: Incorrect password	IAM Event - Authentication Failure	
SaaS Alerts MSFT	Microsoft	multiple.account.locks	05/15/2023 19:18 EDT	at_af3@saas alerts.net	107.170.58.26	Digitalocean LLC	New York City, NY, US	Agent - Chrome / Windows 10 / Method - Password / Activity - Login:login	IAM Event - Multiple Account Locks	autotaskpsa, connectwise 532243

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



Bad actors are constantly knocking at the door of every SaaS application in your business trying to gain access through end user accounts. Brute force attacks are a very common method deployed by hackers to compromise accounts. What is a brute force attack? A brute force attack, also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted password until the correct password is discovered

Account alerts

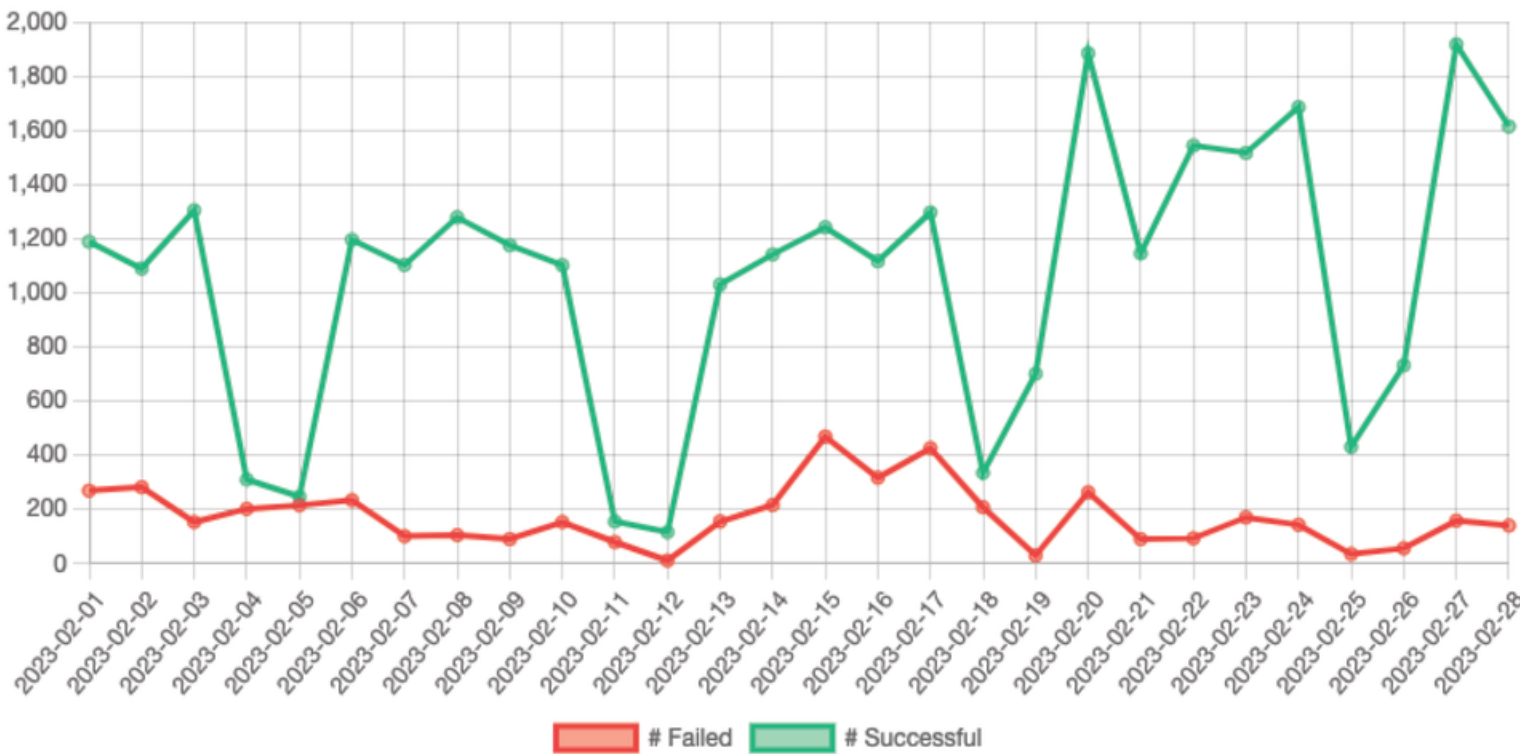
Below is a chart displaying top 10 Accounts within your business that triggered the most alerts in the selected period.



The key is understanding which events rise to the level of an alert and thus that needs to be remediated to mitigate risk. The data above provides the total number of events associated with each account that have risen to a level of a critical alert or an alert. To protect your business, we evaluate every “alert” and “critical alert” and make sure it is remediated on behalf of your organization to prevent a security breach.

Login activity

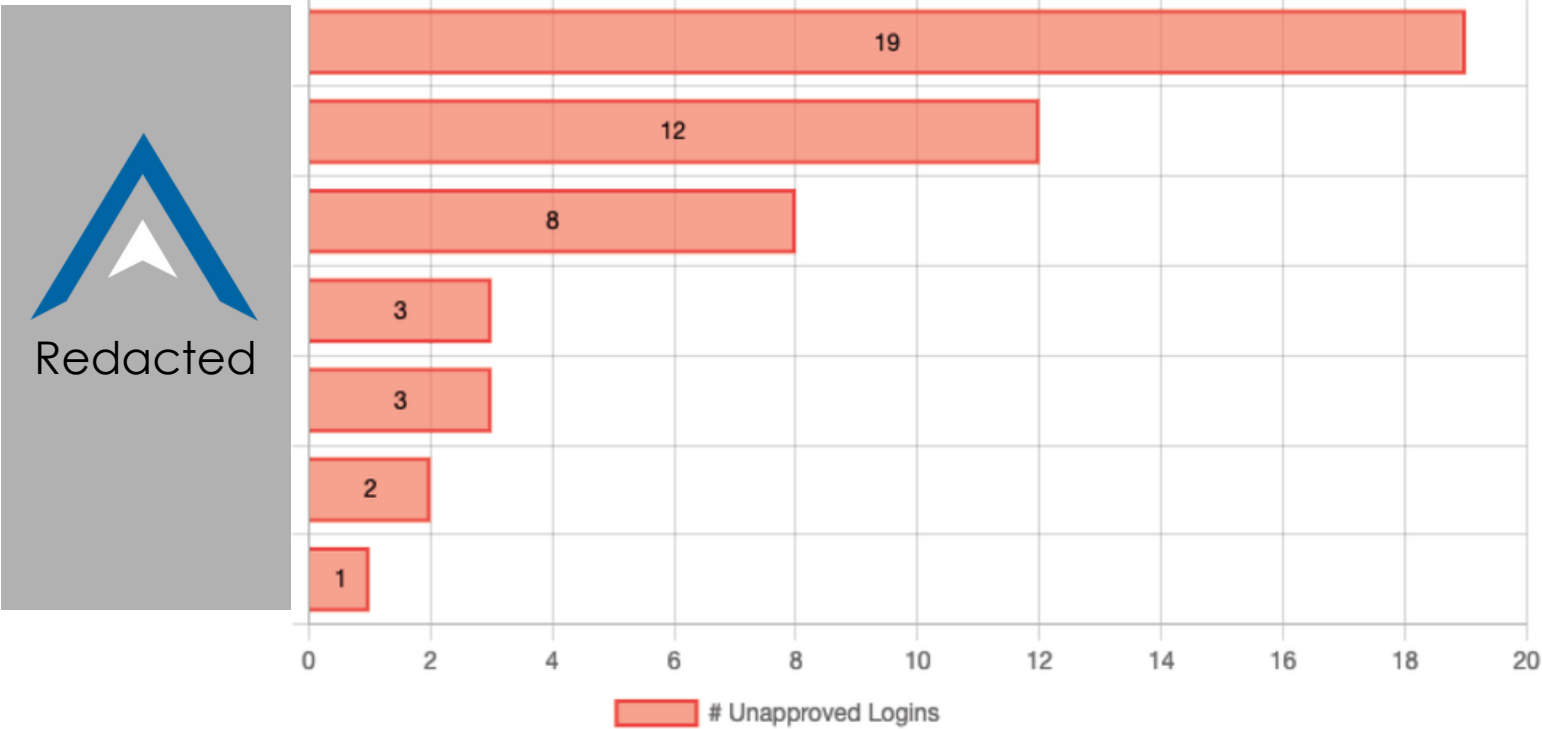
The chart below displays the number of successful and failed login attempts on a daily basis during the report period.



This data provides insight into your employees application usage and bad actors attempting to take over their account.

Unapproved logins

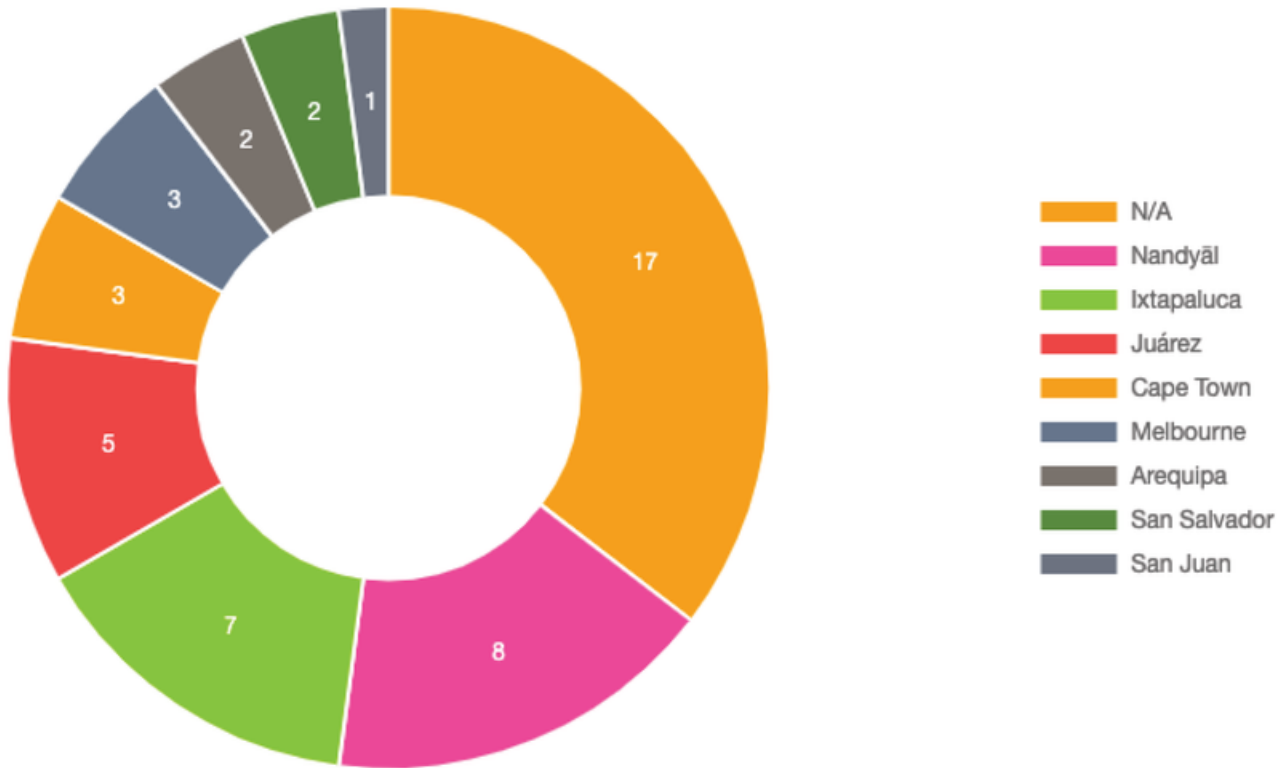
The chart below shows the top 10 accounts with the most successful logins from unapproved countries.



If a login from an unapproved location is present, a critical alert is generated in our system so we can coordinate with your organization to prevent further harm.

Unapproved locations

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



We continually monitor these events and are constantly evaluating threats from new locations so we can assist you in preventing unauthorized access to your accounts.