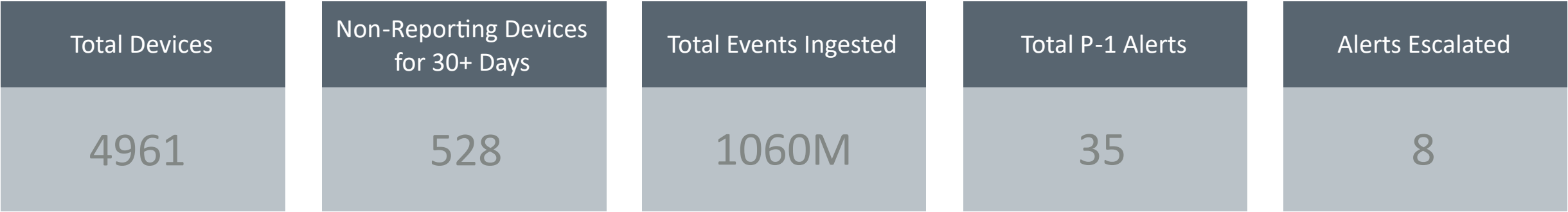


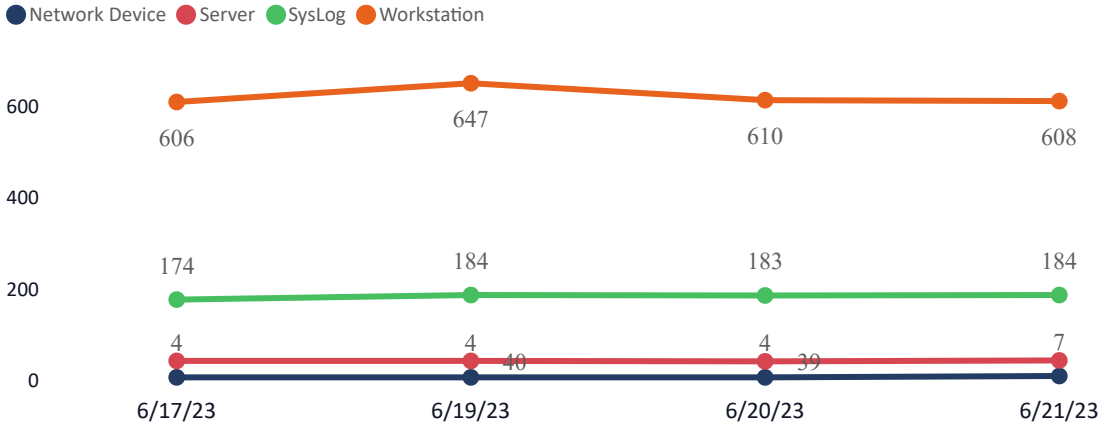
Executive Summary	Threat Insights	P1 Alerts	AD Login Failed	AWS	M365 Azure Login Activities	Windows Admin Activities
-------------------	-----------------	-----------	-----------------	-----	-----------------------------	--------------------------

Netsurion's SOC escalated a major security alert to the customer noting suspicious activity originating from Contososrv01, please refer to the AD Login Failed tab for more information. Netsurion's SOC also discovered suspicious activity coming from a malicious process masquerading as legit. Please refer to the Threat Insights page for more information.

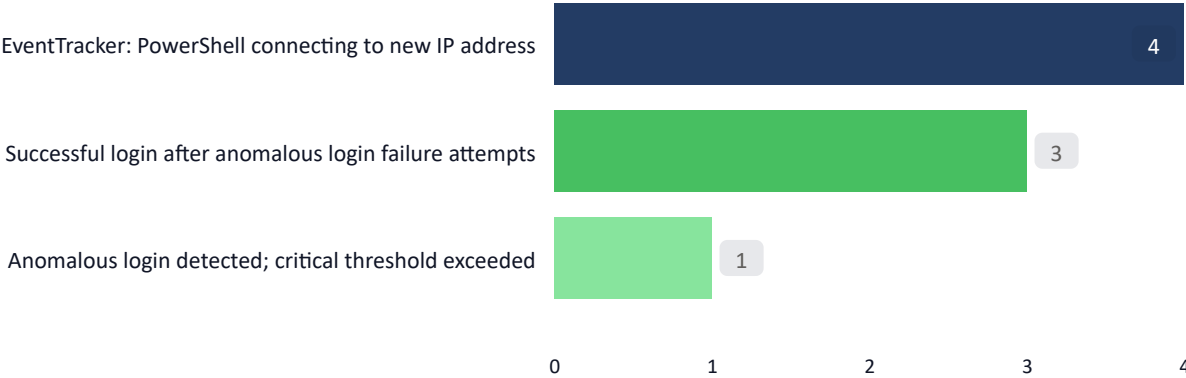
Service Summary: Managed XDR Enterprise Edition, Daily TIR report, Daily Threat Hunting, Incident and Audit Support
Result Summary: Netsurion's SOC generated 35 **P1 Alerts** in your environment of those, 8 were escalated to you



Non Reporting Device Trend



Escalated to Customer Alerts



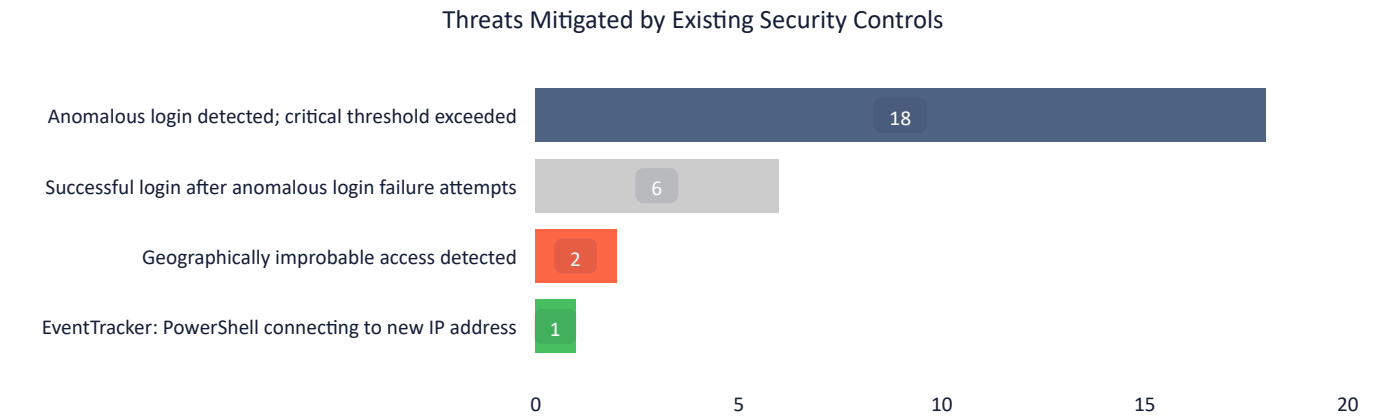
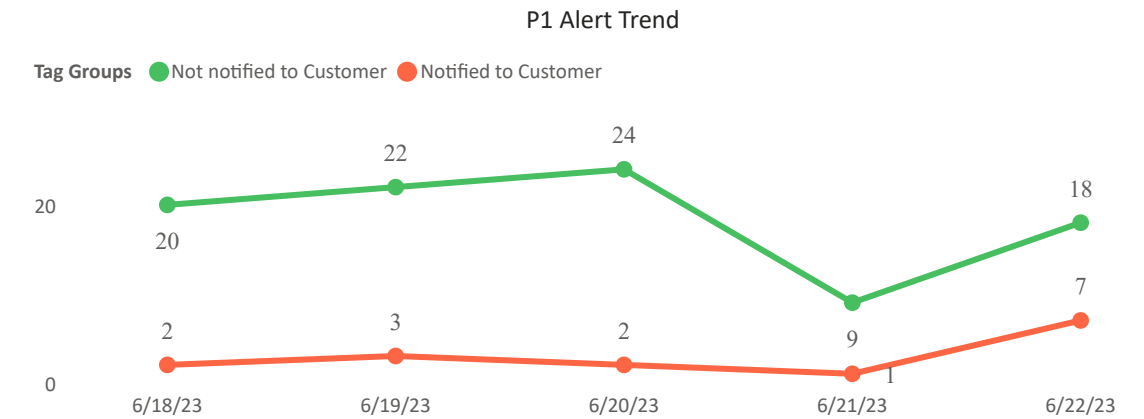
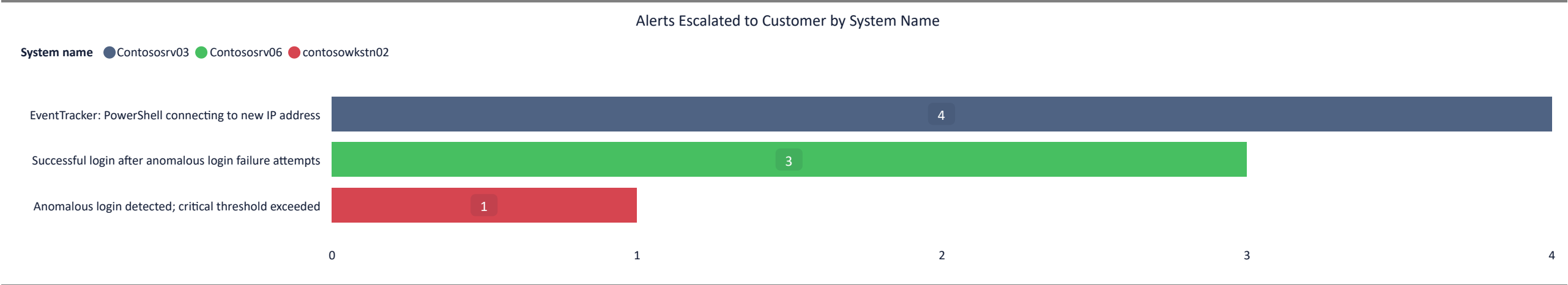
Executive Summary	Threat Insights	P1 Alerts	AD Login Failed	AWS	M365 Azure Login Activities	Windows Admin Activities
-------------------	-----------------	-----------	-----------------	-----	-----------------------------	--------------------------

Additional findings based on Netsurion's SOC review are listed below. For a complete description and recommendations to address the findings please see <link to additional information>

Threat	Severity	Observations	Actions
Brute force attempt	Critical	"Netsurion SOC has observed multiple failed log-in attempts on Contososrv02. The usernames used for logins are guest, builtin, backuponly and anonymous and so on. Mention in the below table. There is around 3K+ login attempts have been made and all of them are network-based logins."	
Dictionary attack detected	High	Netsurion SOC detected an unknown process with Bad Hash on the system Contososrv03. We observed two unsafe processes from the same product Lavasoft Software Canada Inc. with bad Hash executed on the system Contososrv03 by the user SEQUEL\sqadmin1.	
Email account compromise	High	SOC observed email traffic from the external IP addresses 102.221.237.43(Nigeria) and 47.201.115.180(US) delivered to several recipients within the organization and outside as well within a short interval of time.	
Emotet Trojan detected	High	SOC observed Suspicious Net logon Attempts on the below-listed domain controllers with the hostname Mimikatz and Emotet Trojan behavior activities are exhibited on DT5000181	
Malicious process masquerading as legit:	Critical	Netsurion SOC observed Suspicious Network logon failures from multiple external IP addresses using multiple usernames, all the login attempts were from outside United States on the system Contososrv01 due to the multiple reasons. Note: Soc observed that during this event the system was assigned public IP 75.70.201.44 and we observed successful login from this user Smith on the svstem Contososrv01.	

Executive Summary	Threat Insights	P1 Alerts	AD Login Failed	AWS	M365 Azure Login Activities	Windows Admin Activities
-------------------	-----------------	-----------	-----------------	-----	-----------------------------	--------------------------

Netsurion's SOC escalated 7 P1 alerts to the customer noting suspicious activity. Netsurion's SOC also reviewed 11 additional P1's that were analyzed by the SOC and determined to be false positives.



Executive Summary

Threat Insights

P1 Alerts

AD Login Failed

AWS

M365 Azure Login Activities

Windows Admin Activities

Netsurion's SOC observed Suspicious Network logon failures from contososrv01 which exhibited the brute force/dictionary login patters, Upon performing further log search, we didn't any successful logins (or) Upon Performing log search, we observed a successful access gaining activity followed by credential dumping.

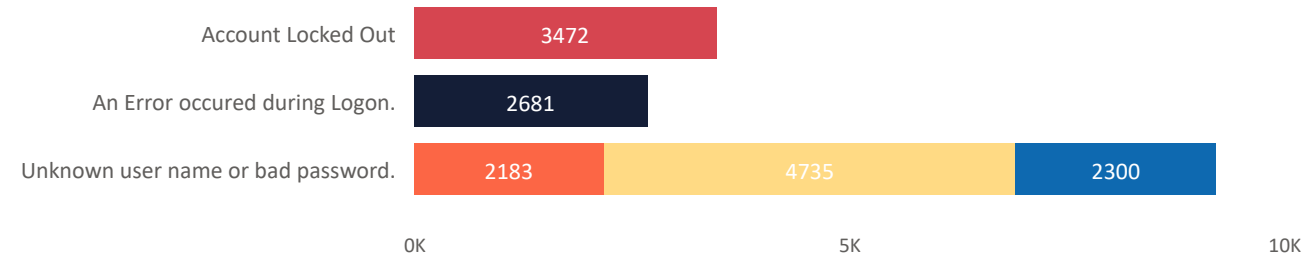
Netsurion's SOC identified lateral movement activities and sent a separate notification on the activities performed.

Recommendations:

Netsurion's SOC recommends changing the password for the compromised account.

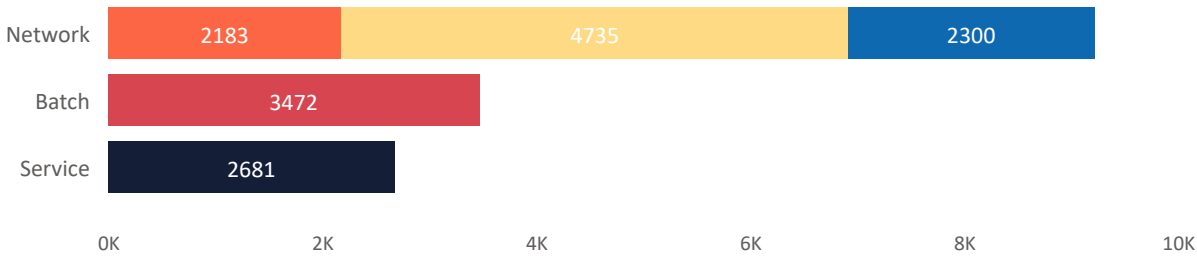
Top Reason

User Name Ava Emma Ethan Liam Olivia



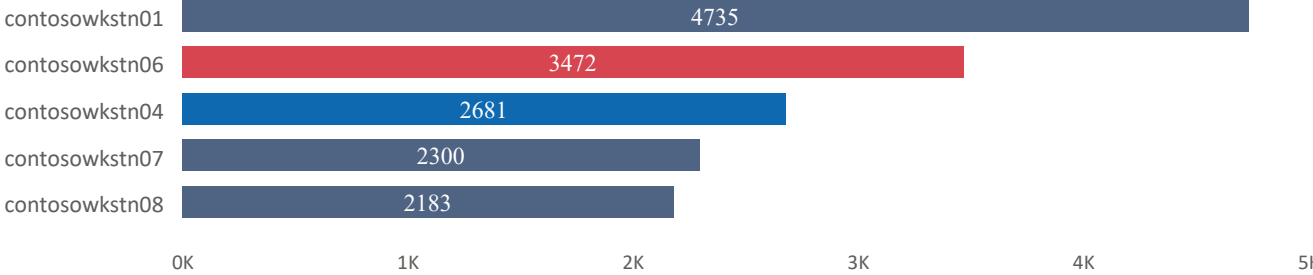
Logon Type by Username

User Name Ava Emma Ethan Liam Olivia



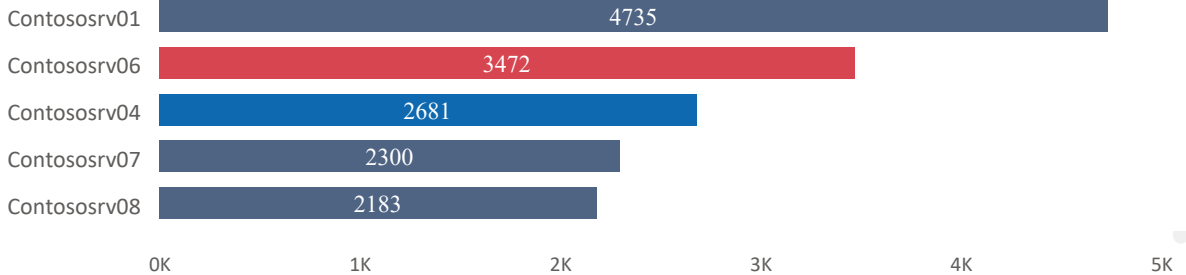
Destination - Workstation Name

Reason Account Locked Out An Error occurred during Logon. The specified account's password has expired. Unknown user name or bad pa.



Source Computer

Reason Account Locked Out An Error occurred during Logon. The specified account's password has expired. Unknown user name or



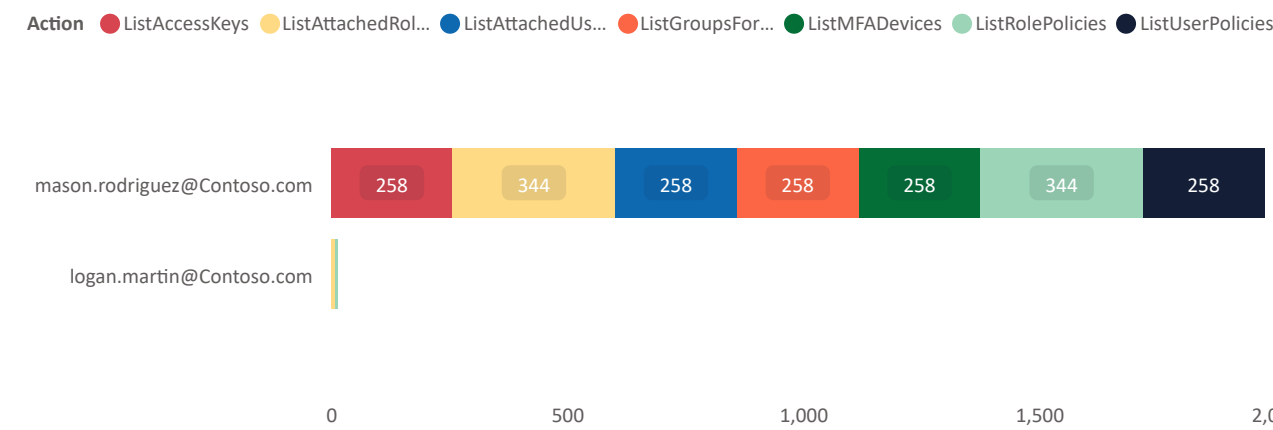
Executive Summary	Threat Insights	P1 Alerts	AD Login Failed	AWS	M365 Azure Login Activities	Windows Admin Activities
-------------------	-----------------	-----------	-----------------	-----	-----------------------------	--------------------------

Netsurion's SOC researched the actions across IAM, EC2 security group and EC2 VPC change activities. Netsurion's SOC did not observe any unusual activity.

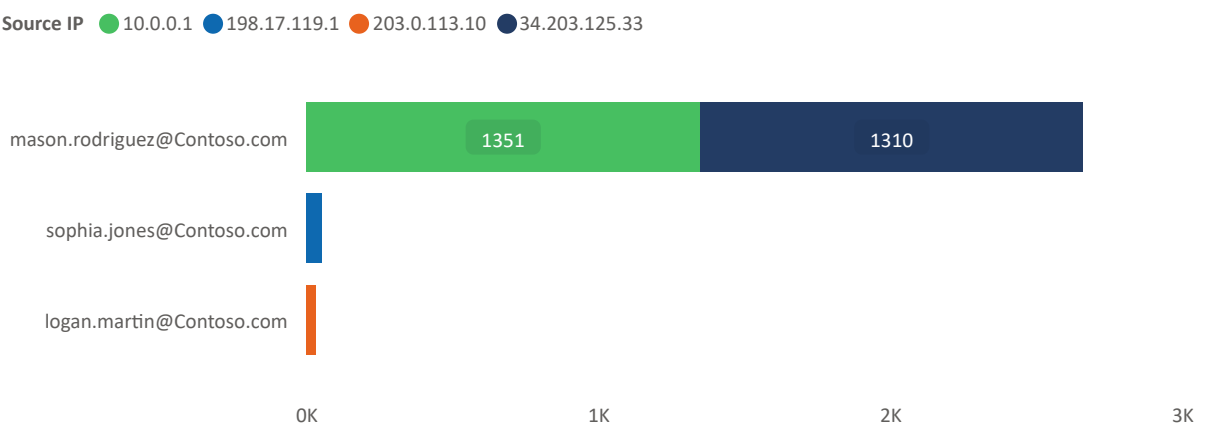
Recommendations:

Netsurion's SOC recommends to verify whether the activities below are approved and authorized.

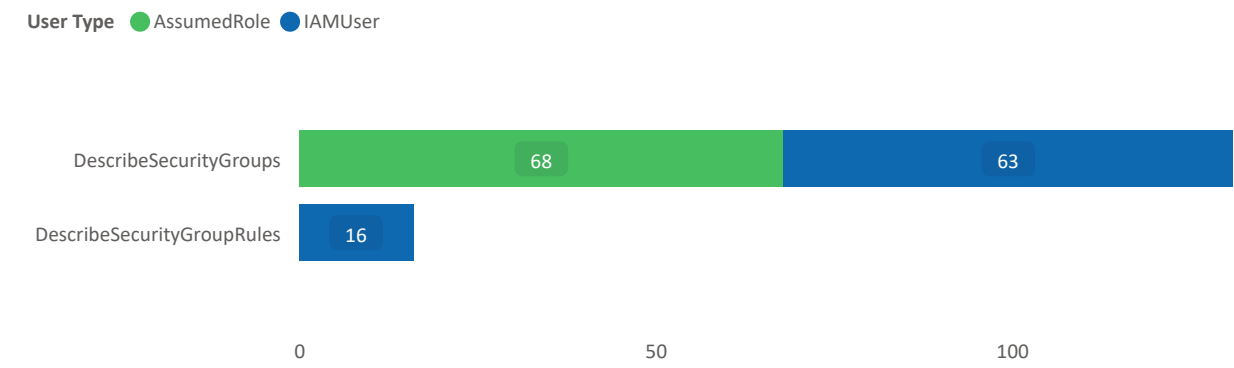
AWS IAM Activities - User Name by Action



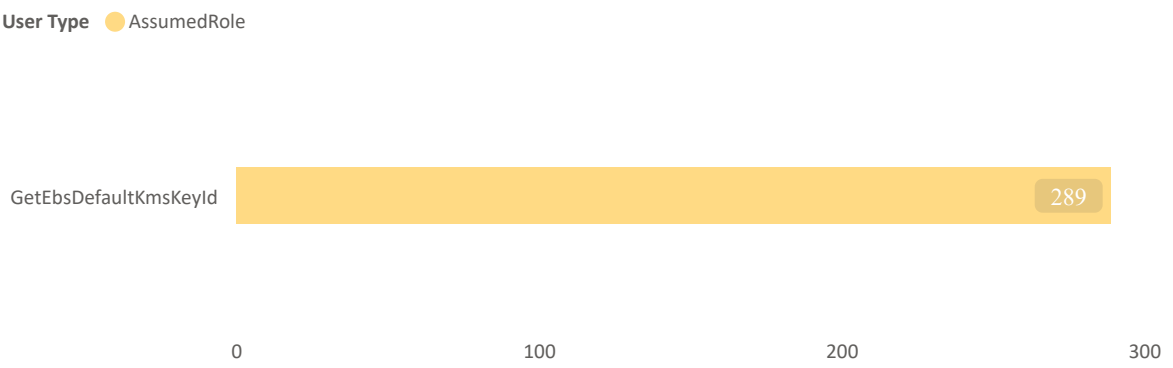
AWS IAM Activities - User Name by Source IP



Amazon EC2 Security Group - Action by User Type



Amazon EC2 VPC Changes - Action By User Type

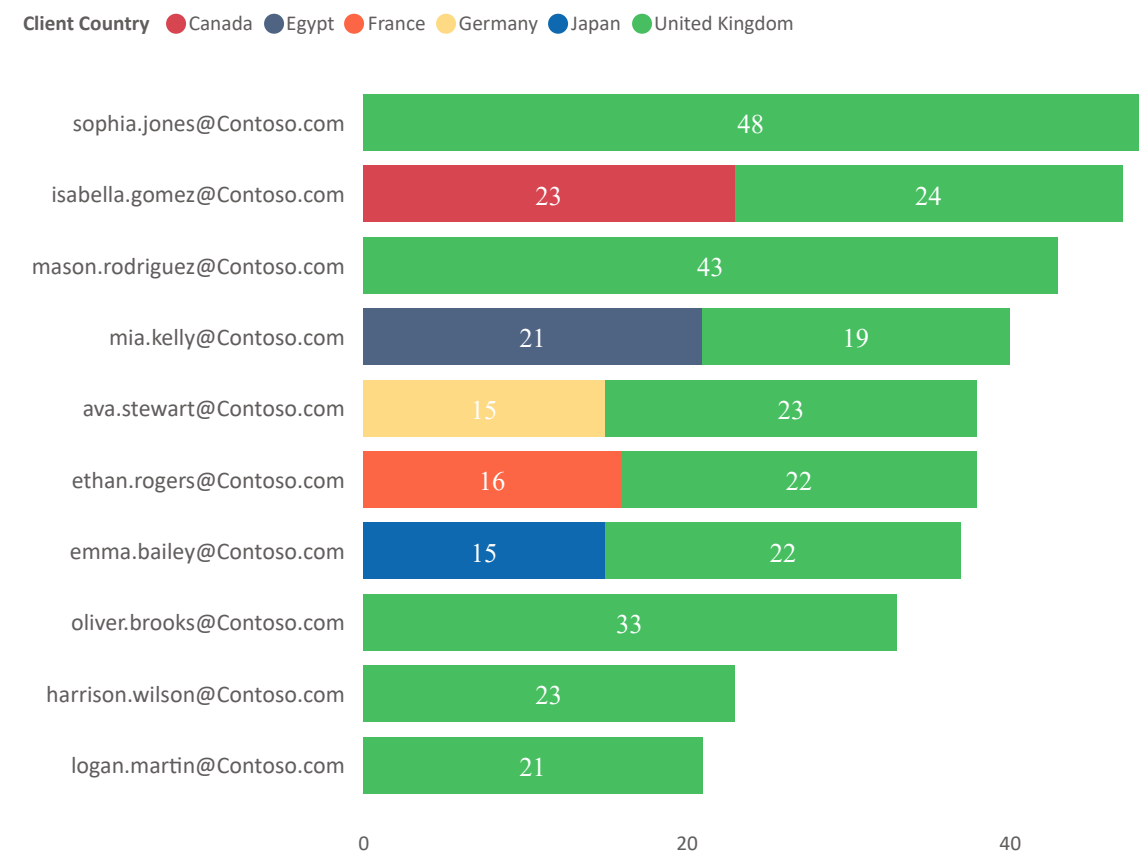


Executive Summary	Threat Insights	P1 Alerts	AD Login Failed	AWS	M365 Azure Login Activities	Windows Admin Activities
-------------------	-----------------	-----------	-----------------	-----	-----------------------------	--------------------------

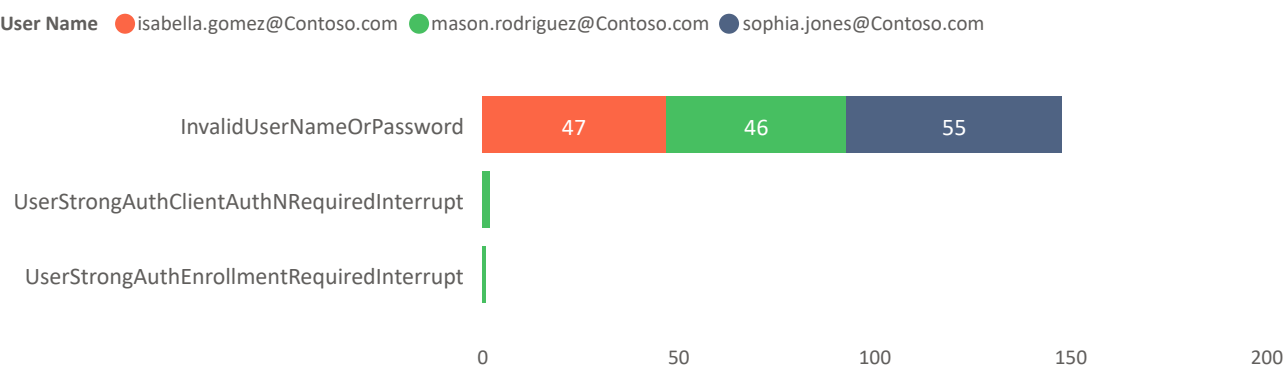
Netsurion's SOC observed successful logins from non-business countries Canada & Germany. Netsurion's SOC performed further analysis on the activities performed by the suspected use accounts and not other critical actions performed by the users.

Recommendations:
If this is not a legitimate login, reset the password for those users immediately, validate the permissions assigned and ensure that the MFA is enabled.

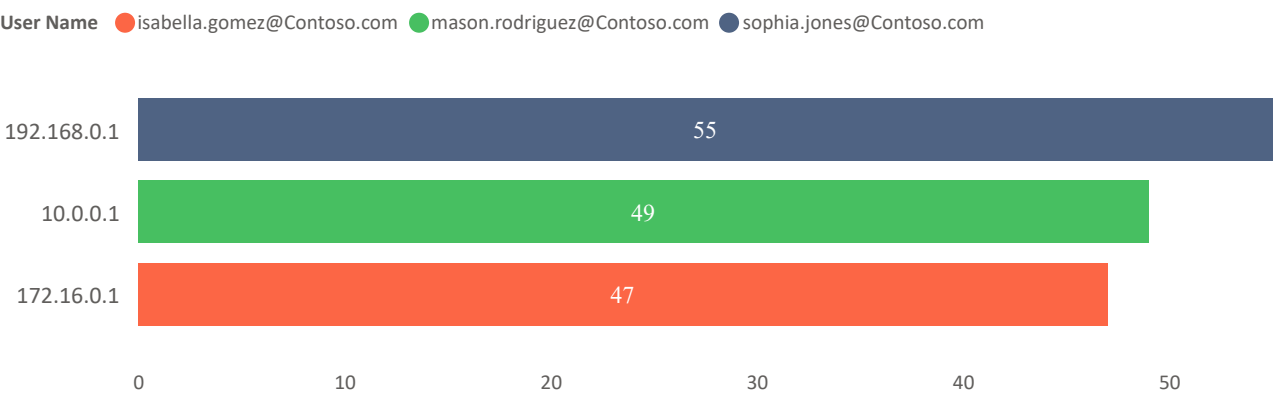
Top Login Failure by Users



Top Login Failure Reasons



Client IP by Username



Executive Summary	Threat Insights	P1 Alerts	AD Login Failed	AWS	M365 Azure Login Activities	Windows Admin Activities
-------------------	-----------------	-----------	-----------------	-----	-----------------------------	--------------------------

Netsurion's SOC observed the following active directory administrator activities as listed below. Major activities are associated with unlocking operation by user Smith. Netsurion's SOC performed further analysis on the activities performed by user Smith and identified no critical active directory changes performed by user Smith.

