TLC TECH
WE SPEAK HUMAN

Office 365 Threat Analytics

TLC Tech offers the **Threat Analytics Service** to provide our partners with proactive threat analytics by leveraging A.I. driven SIEM and 100% US based security analysts. This service will detect and alert on known and new cyber threats inside **Microsoft 365** using advanced machine learning, behavioral analytics. and dynamic threat models.

Key Features

- 24x7 Cloud Monitoring
- Customized rules tailored to your business
- 1 year log retention
- Response within minutes to prevent the escalation of threats

The Indicators of Compromise *(IoCs)* that this service looks for:

User Login Anomalies

- **Impossible Travel** - Two user activities originating from geographically distant locations within a time period shorter than the time it would have taken the user to travel from the first location to the second, indicating that a different user is using the same credentials.
- **Foreign Logins** - Logins from outside the country or state of the user's origin.
- **Risky IP Addresses** - This detection identifies that users were active from an IP address identified as risky.
- **Brute-Forced Successful User Login** - This alert will trigger when a bad actor tries multiple attempts on account passwords with the hopes that one of them will be valid and is successful on logon.

User Activity Anomalies

- **Email Forwarding Rules** - Monitoring for rules that will forward emails to outside of the domain.

Admin Activity Anomalies

- **Account Creations & Deletions** - Visibility into when an account is created or deleted.
- **Admin Role Changes** - Notified when a user is added to an admin role.
- **Multi-Factor Authentication Changes** - Notification if a user's MFA is disabled due to a compromise or verification if an admin is abusing their role.

(916) 441-3838 | www.tlctech.com | info@tlctech.com