ASCERIS

# Microsoft 365 Proactive Assessment

One of the most common cyber incidents we see today is a result of insecurely configured Microsoft 365 environments. To help solve this problem, we built proprietary software to support assessments focused on the risks we see in our cyber response investigations.

We use our proprietary technology to evaluate environment configuration and user behaviour on Microsoft 365 to help prevent business email compromise attacks

Our assessment is focused on:

- Environment level configuration
- User level configuration
- Suspicious behaviour
- Unexpected user activity

The assessment is delivered in a high quality report with a view of the system configuration, activity as well as key recommendations. We check the below information.

| | |
|---|---|
| Multi-factor authentication configuration | Anonymous / VPN activity |
| Legacy protocol configuration and activity | Suspicious mailbox rules |
| Audit logging configuration issues | Unexpected consent grants |
| Shared mailboxes allowing direct sign-ins | Failed login activity |
| Connections from unusual countries | Known abusive IP addresses |
| | |

Some benefits to our approach are:

- We look at every account in the environment to identify unusual behaviour
- We are adding new checks all of the time, based on feedback from our insurance partners
- We only require a subset of administrator permissions to carry out the review, not the Global Administrator role
- We gather all of the information we need via an online form, saving time and offering a smooth customer experience

beazley