Clearwater Digital

Horizon

OUR ONBOARDING **PROCESS**

Clearwater Digital

HORIZON OVERVIEW

Horizon is a non-intrusive cloud security and compliance platform that works in conjunction with the Microsoft Office 365 Management and Microsoft Graph APIs. The Horizon code works seamlessly to ingest and structure data from these sources into the Horizon interface, to uniquely visualise your Microsoft Office 365 environment. Designed by leading CREST: The Council for Registered Ethical Security Testers professionals, we ensure our data management processes comply with Microsoft's Acceptable User Policies and United Kingdom and European Union data assurance standards.

Clearwater Digital

HOW DOES ONBOARDING WORK?

WE HAVE TWO METHODS OF DATA COLLECTION

The first utilises the official Microsoft Office 365 Management Activity API to obtain log data on a continuous basis, and Microsoft Graph to retrieve user details. To enable this method, we send an email link to your Microsoft Office 365 Global Administrator. Upon clicking this link, a Microsoft Azure Authentication prompt will ask if your administrator authorises the Clearwater Horizon platform to access your cloud audit data.

The API provides Clearwater with a consistent log data feed as well as up to 7 days* of data prior to the date of authorization.

For clients with historic auditing enabled (see Enable Auditing below), Horizon can support a second collection method using Microsoft's UnifiedAuditLog PowerShell Interface. This method allows us to retrieve up to 90 days of historic data* in a one-time deployment, enabling enriched Horizon insights from the start.

Both access methods are under full control of the client's administrators and access can be revoked at the end of, or during any engagement.

*Historic collection by API feed and/or PowerShell is only possible if a client has previously enabled auditing

Clearwater Digital

WHAT DO I NEED TO DO TO ENABLE HORIZON?

ENABLE AUDITING

By default, Microsoft Office 365 creates new tenants with auditing disabled. This means that there is very limited log data being stored for your organisation, severely impeding cyber incident response investigations or auditing. Effective Horizon monitoring requires auditing to be enabled.

This is a simple one click change to your Microsoft Office 365 tenant, which Microsoft do not charge for. The change will cause no impact on the functionality or performance of your Microsoft Office 365 tenant.

TO DO THIS:

1. As an Microsoft Office 365 Global Administrator, please browse to https://protection.office.com/unifiedauditlog.

2. If you see a box stating, “Turn on auditing”, auditing is not enabled. Please click the box.

3. If you do not see a box, auditing is already enabled, and you need take no further action.

4. Microsoft’s instructions are available at https://docs.microsoft.com/en-us/microsoft-365/compliance/turn-audit-log-search-on-or-off?view=o365-worldwide#turn-on-audit-log-search

Clearwater Digital

ENABLING API ACCESS

To complete this step, you must accept the Horizon application permissions, whilst logged into Microsoft Office 365 as a Global Administrator. Upon acceptance of these permissions, Horizon will begin collecting log data.

Clearwater will send you a URL directing you to our application permissions page. This page details the permissions requested by the application – please take time to read them and contact Clearwater if you have any questions about the extent of our data collection. Once you are happy, click **Accept.**

Additionally, please supply Clearwater with the name of your Microsoft Office 365 tenant by navigating to **Settings > Domains.** The domain name required is the *Initial domain.*

For security purposes, we support out-of-band confirmation that the email from clearwaterdigital.io is legitimate.

Clearwater Digital

Horizon

horizon@cwdynamics.com

00 44 (0) 1202 804 140