infotex

Microsoft 365 Log Monitoring

offerings.infotex.com

Microsoft 365 log monitoring can represent an effective strategy to achieve cloud security and ultimately compliance. Leveraging that log data to get insights about user behavior and insider threats. Microsoft 365 logs are generated by cloud-based Microsoft 365 applications, such as Azure Active Directory (AD), Office, Exchange, SharePoint, etc.

Benefits of Microsoft 365 Log Monitoring

Microsoft 365 can report about administrator-privilege accesses, end-point user behavior, user access, log-in history including log-in times and location, and user sharing behavior. This auditing offers a variety of benefits, including (but not limited to) increased security awareness and enhanced detection capabilities, all by monitoring and analyzing Microsoft 365 security logs in a structured way.

Examples of Microsoft 365 Log Monitoring

Azure AD: Logs generated by Azure AD, Microsoft's cloud-based identity and access management application, deliver information about user maintenance, group maintenance, and authority delegation. All activities an Admin wants to know about. In essence, it's an entire Windows network in the Cloud!

Exchange: Logs extracted from Exchange Online provide an audit trail of what Admins can do and much more. In this context, along with the knowledge that many attacks originate from phishing emails. Analyzing Exchange logs can help detect who is infected, how the attack spread, as well as reveal mailbox snooping, mailbox takeover, inappropriate activity, etc.

SharePoint: The web-based storage platform SharePoint, which is strictly linked with OneDrive, outputs logs that report any operation performed on files. They help to report any instance of file access, download, or sharing via a link with a person outside the organization; even logging the email address to which a file has been share.

Benefits of Engaging with infotex for Microsoft 365 Log Monitoring

As explained above, Microsoft 365 itself does a very good job in terms of auditing. Unfortunately, the Microsoft 365 portal to view logs has very limited functionalities when it comes to searching, exporting, and archiving. Microsoft 365 Log Monitoring services, like the **infotex** offering, address these shortcomings and enable Clients to search better, export more logs, and archive logs for longer periods. From a security and compliance perspective, it is considered best practice not to keep the logs within the same system that generated them because logs can be modified by users with privileged rights. By engaging with a third-party system to trace log data, your institution can overcome this shortcoming!

Conclusion

Microsoft 365 log monitoring represents an effective strategy to achieve cloud security and leverage that walled-off log data that would otherwise be left unwatched. **infotex** has built a Microsoft 365 Cloud Connector as part of our SIEM to empower our Clients and Data Security Analysts to meet the daunting challenge of remaining secure and protected against data theft, security breaches, and cybersecurity attacks. At the same time addressing today's sophisticated cloud security and compliance requirements.

If you are interested in our Microsoft 365 Monitoring, our SIEM, or any of our other services, please visit:

offerings.infotex.com