CONTROL IT SOLUTIONS

Security Monitoring

bluedog SECURITY MONITORING

Strengthen your organisation with bluedog

Office 365 security monitoring

Many businesses are now using Office 365 for all business emailand productivity. These businesses thenrely upon anti-virus and basic anti-malware solutions for their security which will never be triggered should an account be compromised.

With bluedog O365 security monitoring, bluedog can track the way an attacker navigates through the network: picking up on the unusual location of login, lateral movement within a network and data exfiltration. By correlating this data and more, the patterns of attackers are easily spotted. As soon as an incident is identified, action will be taken by the bluedog first responders to eliminate the threat from your organisation. Whether this is blocking the user, isolating a device or closing off full network segments; the incident is resolved, quickly and accurately.

Working from home?

How do you monitor devices that are not on company premises? Many businesses have seen a huge benefit in using Office 365 as it improves collaborate working practices. March 2020 saw an increase in phishing emails of over 660% compared with the previous month. The saddest thing about this is that almost 40% of untrained users are susceptible to phishing, making many businesses more vulnerable than ever before. bluedog Office 365 monitoring delivers peace of mind: should any malicious activity appear within your environment, you will be alerted to it immediately, providing you with the ability to act before too much damage is done.

Bluedog can effectively monitor Office 365 by looking for “weird behaviour” such as

- unusual sign-in locations
- failed and successful login attempts from unusual locations
- data extractions from SharePoint or OneDrive
- logins to mailboxes on Exchange
- behaviour inside Exchange
- emails with suspected phishing etc
- device updates
- user account changes such as user password changes, user updates, new users, deleted users.

Working with the data stream from Office 365 (including event logs from the Active Directory), active users and locations can be seen, and their work patterns learnt. Anomalies are detected and strange behaviour, which could be malicious, is scrutinised and acted upon.

Contact

Tel: 01738 310 271 email: info@controlitsolutions.co.uk web:www.controlitsolutions.co.uk
3 High Street, Kinross, Scotland, KY13 8AW

Frequently Asked Questions

Can we trace if someone extracted information from the network when they for example put in their resignation, to validate they didn't breach any of the non-competition clauses in a contract?

Yes, this capability is certainly present inside the bluedog Office 365 monitoring solution. It is possible to have a full overview of what actors have been doing. The ability to review files, folders and emails that have been accessed, downloaded, deleted, etc, gives this overview in time and place. This is a great benefit to identify any data that may have been stolen or leaked, drilling down to the user and IP address.
Important note The contents of files or emails themselves are not visible to bluedog, only the filenames and locations of files inside SharePoint/ OneDrive and the subject of email or filename of the attachment.

Can we find out if someone is in a different location than where they claim they are?

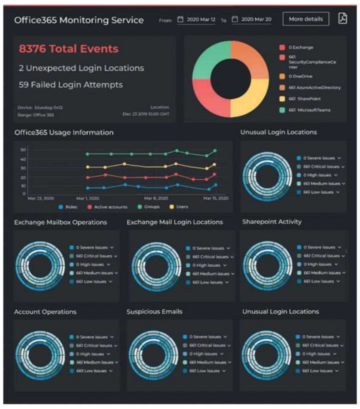
Yes, this is possible as the IP address of user activity is stored with the location at the time of the activity. This allows the bluedog team to determine where actors are located while performing their activities.

Can we see if a certain office location is working more proactive than other locations are?

Yes, the capability of grouping data sets based on geolocation, country and city are present in the bluedog Office365 monitoring solution. This gives the ability to check on performance or make other geographical correlations from the data.

Would this offering be able to provide a report to show the number of external (only) emails sent by each user over a period, i.e. seven days?

Yes, this is possible. The Exchange dashboard provides insights into email behaviour from within the company. It also shows how email is treated, showing the types of email a user sends and receives. This provides great insights on any targeted attacks on the company. Identifying which users are receiving most phishing attacks and looking at the kind of malware.
With this information, bluedog can provide recommendations on what action to take that will improve security measures for the business.



8376 Total Events

2 Unexpected Login Locations

59 Failed Login Attempts

Contact

Tel: 01738 310 271 email: info@controlitsolutions.co.uk web:www.controlitsolutions.co.uk
3 High Street, Kinross, Scotland, KY13 8AW