Cisco Threat Analyzer for Office 365

What is the Cisco Threat Analyzer for Office 365?

The Cisco Threat Analyzer for Office 365 is a tool that Cisco sellers and partners can use to demonstrate why Office 365 security is not sufficient. It can identify security vulnerabilities present in select Office 365 email inboxes and help prove the value of using Cisco Email Security and AMP to better secure those inboxes.

How does it work?

The Cisco Threat Analyzer for Office 365 leverages the Graph API from Microsoft. By making a read-only call via the API, the tool will ingest, scan and then discard messages. During the scan, the verdicts from the message scans are used to build the summary report.

What is the Cisco Threat Analyzer for Office 365?

The Cisco Threat Analyzer for Office 365 is a tool that Cisco sellers and partners can use to demonstrate why Office 365 security is not sufficient. It can identify security vulnerabilities present in select Office 365 email inboxes and help prove the value of using Cisco Email Security and AMP to better secure those inboxes.

How does it work?

The Cisco Threat Analyzer for Office 365 leverages the Graph API from Microsoft. By making a read-only call via the API, the tool will ingest, scan and then discard messages. During the scan, the verdicts from the message scans are used to build the summary report.

Is there a cost to use the Cisco Threat Analyzer for Office 365?

The Cisco Threat Analyzer for Office 365 is free of charge to use.

What impact Cisco Threat Analyzer for Office 365 have on the customer environment?

The Cisco Threat Analyzer for Office 365 uses the Graph API, thus does not impact Exchange Online or the user access to mailboxes. If running the tool in dCloud, no local compute resources are required.

If running in the customer premises, then a VM is required to run the tool. The requirements for the VM would follow the same used for a C300 image.

How do I use the tool? How do I set up an appointment for my customer?

Log into dCloud and schedule a session to use the tool – dcloud.cisco.com, alternatively an independent Virtual Machine can be used on customer site.

Firewall Considerations:

If a local VM is required, the tool will require HTTPS connectivity to the internet, and the tool runs on port 8080 on the VM. An IP on the management interface must be assigned.

Who from the customer should I contact to participate in the scan?

You should contact your customer's Office 365 Administrator to participate in the scan as their user credentials will be required to configure a secure binding between the tool and their environment

What does the customer need to do to participate?

The customer needs to work with you to share their Office 365 Administrator passwords and be willing to share access to their mailboxes in a read only mode.

Is there a security risk for my customer to allow an API call to their Office 365 Instance? How can I reassure my customer this is secure and doesn't risk their compliance requirements?

We do not read any information contained within the emails, we operate in a scan only mode, any information that is scanned is then immediately discarded with all message tracking removed once the scan is complete. Nothing is stored in NVRAM (Non-Volatile Random-Access Memory) post power either.

What is actually being scanned?

Mail within the selected mailboxes is being scanned in read only mode.

How many mailboxes and messages should I scan and how long will the scan take?

You want to get a sample, not scan every mail message or mail box as the tool is designed to showcase the value of Cisco Email Security. In order to augment the chances of success the recommendation is to scan 50 densely populated mailboxes to begin with. Scan times can vary, however expect to leave the scan running for 48-72 hours.

What does my customer get after the threat analyzer runs?

Your customer will be given a high-level one page report that graphically shows what has been scanned by their Office 365 instance. The report highlights how many mailboxes scanned, how many emails were within those mailboxes. It also highlights how many infected mailboxes were found with spam, malicious URLs and malware.

What is it purpose of the Cisco Threat Analyzer?

The Cisco Threat Analyzer has been designed to scan mailboxes and to look for threats which Microsoft has failed to detect. The tool is not mean to replace an existing Email Security incumbent product or is it to be used as a forensics tool. The customer will get a report detailing the findings at the end of the scan which will highlight to them the need for increased Email Security from Cisco.

What should I do after I run the scan for my customer?

You should talk to the Cyber Security contacts at your customer about how Cisco Email Security can mitigate against the security risks highlighted in the report. You should discuss running a full proof of Value or evaluation of Cisco Email Security so that they can understand the full Cisco Email Security solution and the value it can bring to their organisation. Alternatively if the customer is already convinced that they need Cisco Email Security, we can provide them a quotation through their preferred channel partner.

What is the maximum size of a mailbox that can be scanned?

The upper limit of a mailbox is 25GB. Large mailboxes can lead to long scan times with inconsistent results.