vade
FOR M365

DATA SHEET

Threat Intel & Investigation

Threat Intel and Investigation is an add-on for Vade for M365 that provides the integrations, intel, and tools to investigate and respond to email-borne threats transiting through your networks. Export Vade for M365 email logs to any SIEM/EDR/XDR, conduct a forensic examination of emails and attachments, investigate and remediate user-reported emails, and integrate Vade for M365 into your XDR strategy.

Detect, investigate, and respond

Email is a rich source of information about ongoing threats against your networks, but SOCs are challenged to monitor and analyze security data from an array of endpoints. Threat Intel & Investigation provides the threat intelligence that SOCs need to gather forensic evidence, cross-check threats across their networks, and develop incident response processes.

Threat Intel & Investigation also provides access to key components of Vade's filtering technology that allow your SOC to dig deeper into malicious emails and attachments in your Vade for M365 Email Logs.

As the cybersecurity landscape evolves and the attack surface broadens, Threat Intel & Investigation will evolve with new features and enhancements to empower your SOC and limit the need for additional technology investments.

KEY FEATURES

- **Export** Vade for M365 email logs to any SIEM, XDR, or EDR.
- **Inspect files and attachments** to find forensic evidence of malware and phishing (URLs, hashes, decoded data, objects, embedded files).
- **Investigate and respond** to user-reported emails and similar, unreported emails.
- **Download** emails and attachments for investigation.

BENEFITS

- **Integrates** email into your XDR strategy.
- **Unifies** disparate email security data.
- **Improves** threat visibility and SOC productivity.
- **Elevates** threat investigation capabilities.
- **Improves** defensive posture.
- **Decreases** time to respond to security events.

Log Export

Vade for M365 email logs feature an array of intelligence about the threats targeting your business. With Threat Intel & Investigation, you can export your Vade for M365 email logs to any SIEM, EDR, or XDR with Vade's REST API.

Integrating your Vade for M365 email logs with your SIEM, XDR, or EDR converges your email and other endpoints under a single pane of glass. Get a real-time view of data-rich email logs that empowers your SOC to investigate threats, cross-check threats across your networks, and respond with precision.

File Inspector

File Inspector reveals details about malicious characteristics and elements of the attachments, including hash, URLs, objects, decoded data, and JavaScript. The evidence collected can be used to cross-check threats and determine whether they have spread to other areas of the business. Inspect files and attachments from the Email logs or upload PDFs and Microsoft Office files for inspection. Accepted file types include PDF, doc, docx, xlx, xlsx, ppt, and pptx.

Reported Emails

Emails reported as either phishing or spam by end users via the Outlook add-in must be reviewed by Microsoft 365 admins so they can be quickly triaged and remediated. Reported emails provides an aggregate view of user-reported emails in a single interface in Vade for M365. Admins can set alerts for user-reported emails and quickly investigate and remediate both user-reported emails and similar, unreported emails. This action will also remediate emails that have been forwarded to other users.

Download Emails/Attachments

The ability to analyze email conent and attachments is essential to understanding email threat typologies and characteristics. With Threat Intel & Investigation, you can download emails and attachements from the Email Logs to inspect the content.

Samples of emails and attachments enable your team to understand Vade's filtering rationale, collect visual evidence of malicious emails and attachments, and retain the samples for user training.*

*End-user approval workflow included.

About Vade

Vade is a global cybersecurity company specializing in the development of threat detection and response technology with artificial intelligence. Vade's products and solutions protect consumers, businesses, and organizations from email-borne cyberattacks, including malware/ransomware, spear phishing/business email compromise, and phishing.

Founded in 2009, Vade protects more than 1 billion corporate and consumer mailboxes and serves the ISP, SMB, and MSP markets with award-winning products and solutions that help increase cybersecurity and maximize IT efficiency.

Contact Vade

sales@vadesecure.com

Request a demo

vadesecure.com

vade