Vade for M365

Threat Intel & Investigation

Threat Intel and Investigation is a premium add-on for Vade for M365 that allows SOCs to export Vade for M365 email logs to any SIEM, conduct a forensic examination of emails and attachments, and integrate Vade for M365 with their XDR (extended detection and response) strategy.

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.**
- **Analyze email attachments with Vade's PDF and Microsoft Office document parser.**
- **Download emails and attachments from the Email Logs for investigation.**

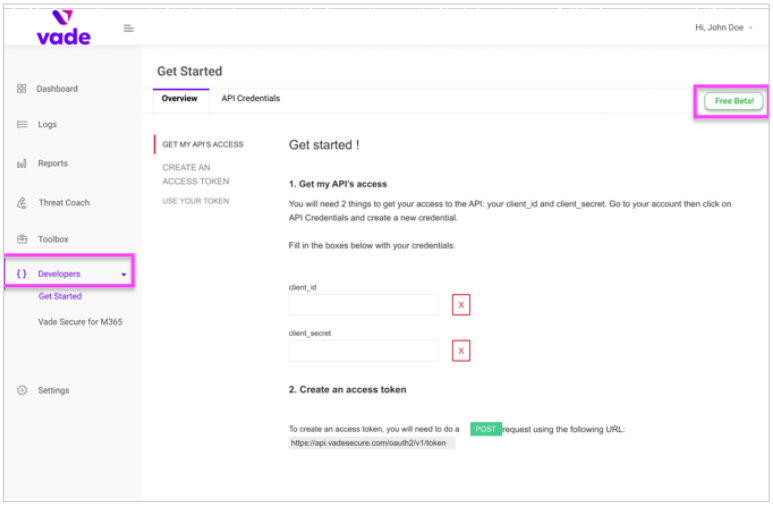
BENEFITS

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

SIEM Integration

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 in just moments with Vade's REST API.

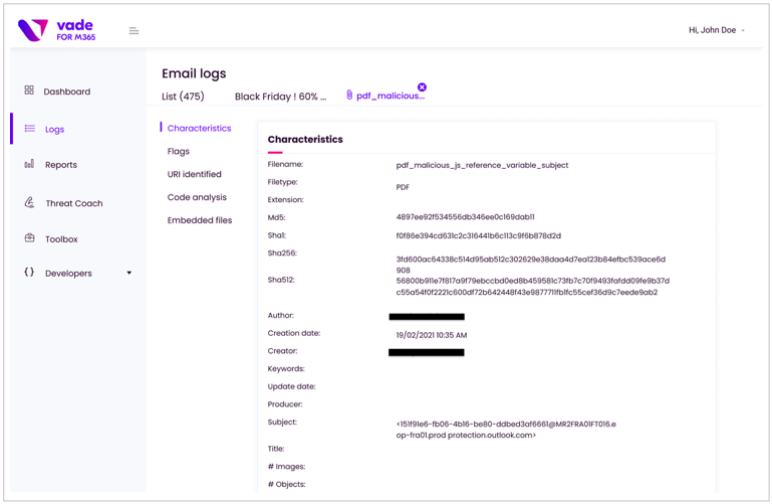
Integrating your Vade for M365 email logs with your SIEM converges your email and other endpoints under a single pane of glass. SIEM integration provides a real-time view of data-rich email logs that empowers your SOC to investigate threats, cross-check threats across your networks, and respond with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



Attachment Analysis

For a deeper analysis into attachments, Threat intel & Investigation is equipped with an advanced tool developed by Vade R&D. Vade's PDF and Microsoft Office document parser is a key component of the core filter engine's attachment analysis, offering deep insights into how threats are built and the evidence you need to investigate and respond.

The PDF & Microsoft Office parser 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.



Email/Attachment Download

The ability to analyze email content and attachments is essential to understanding email threat typologies and characteristics. With Threat Intel & Investigation, you can download emails and attachments 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.*

Vade
sales@vadesecure.com

Request a demo of Vade for M365 at

www.vadesecure.com