# USE CASE

## Investigating a Potential Malware Threat

At eSentire, we are committed to helping our clients optimize their security posture. We often go above and beyond our standard service if it means that our clients' networks will be safer as a result.

### A Client Request

A client contacted the eSentire Security Operations Center (SOC) to inquire about a suspicious file that was flagged by their antivirus system. A reported Microsoft Excel spreadsheet from a workstation was flagged as malicious and they wanted us to investigate.

### Initiate Human Investigation

Upon evaluating the situation, the file scanned positive for Microsoft Office malware. The client requested additional information to understand where the file and email originated. While reviewing the quarantined file, analysts discovered it contained emails between select employees and external firms. Using open source intelligence, it was also discovered that Microsoft recently released a related patch.

### A Timeline of Events

Through building a timeline, the SOC was able to confirm that the emails were sent months before the vulnerability disclosure. The client's antivirus solution recently received a new signature and, as a result, marked the old message as malicious.

### A Comprehensive Response

Offering a detailed timeline enabled the client to fully understand how the incident occurred. Their response: *"This is an awesome and comprehensive response. Thank you for the diligence and thoughtfulness."*

While investigating employees in detail isn't our focus, we take the security of our clients seriously and always strive to go above and beyond for our clients. No threat is too big or too small, and should never go unnoticed. Let us do the same for you. Contact us to learn more about how eSentire Managed Detection and Response™ service can help protect you.


© 2017 eSentire, Inc. All rights reserved.