USE CASE

Mock Incident Investigation

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 our Security Operations Centre (SOC) to inquire about initiating a mock incident investigation that would allow them to identify exfiltrated data, should a breach ever occur. Although not part of our standard service, we wanted to help them in their efforts to be prepared for a potential breach.

The Mock Incident

On the same day the request came in, our SOC team went into action preparing a mock incident. Leveraging our experience investigating numerous malware attacks, a SOC analyst prepared a fictitious scenario where a computer connected to the client's investment network showed signs of an active infection. The client performed numerous antivirus scans but the activity persisted. They contacted us for a detailed report of the machine to determine what happened.

The Mock Report

We created a mock report of the malware investigation using realistic data, timestamps, and an IP name and address true to one of the client's workstations. We noted a Poweliks malware infection in a highly detailed manner that also included a Magnitude Exploit Kit that was served to the machine. In addition to a timeline, we provided an explanation of the incident, summaries of the activity, and a report regarding the exfiltrated data.

Having these discussions with the client, we had the opportunity to give them a list of items to provide us with that would expedite the investigative process should a real incident occur.

Building Trust

Offering a thorough, realistic response helped build trust and confidence in our service. It gave the client an opportunity to witness our incident response capabilities, and what to expect if a breach occurred.

At eSentire, we take security seriously and always strive to go above and beyond for our clients. Let us do the same for you. Contact us to learn more about how eSentire Managed Detection and Response™ service can help protect you.