EXPERTISE ON DEMAND USE CASES

Expertise On Demand can bring a lot of value to your organization. Review the some real-world use cases.

An Endpoint Alert Investigation Through Expertise On Demand

A Mandiant Automated Defense customer received an alert and quarantined several attacker utilities, including Mimikatz. However, questions remained. How did these malicious utilities get on the system? Was there a human attacker involved? If so, what was the scope of the intrusion? The customer invoked their Expertise On Demand service to investigate.

The customer initiated the collection of a Standard Investigation evidence package and provided the Mandiant analysts access to their security console. Mandiant was able to determine the earliest evidence of attacker activity, how the attacker was able to access the host, the malicious executables that were used by the attacker, local accounts that were created on the system, and that the system was quarantined before the attacker could move laterally. Mandiant also provided recommendations on how this type of incident might be avoided in the future.

This service was provided to the customer at a cost of 4 Units. If you are concerned about an alert you are seeing in your environment as well, reach out through your Expertise On Demand subscription to see how our experts can assist.

Leveraging Custom Threat Reporting to Increase Security Controls

A financial organization reached out to Mandiant looking to expand their operational footprint in several areas, including technology, products, and business partners. We took note of their specific concerns and scoped a tailored report that gave them

- Visibility of the threat landscape (i.e., which threat actors were operating in their space and what tactics, techniques, and procedures they use)
- Their threat profile within that landscape (I.e., identifying possible exposures related to people and assets that could be targeted) and detailed case studies of relevant activity.

With this information, the customer was able to proactively implement security controls for valued assets (infrastructure and personnel) and ultimately pass the report up the stakeholder chain to inform the calculus for corporate risk decisions.

If you are looking for specialized Intelligence based on your business needs, purchase a Custom Threat Intelligence report through your Expertise On Demand subscription.

Not an Expertise On Demand Subscriber yet?

If you are not an Expertise On Demand subscriber but are interested, contact **eod@mandiant.com** ().