MITIGA

Threat Hunt

International Cybersecurity Software Company

A worldwide cybersecurity software company had sensitive data exfiltrated in the past, and suspected the attacker regained persistency within their AWS environment. They called Mitiga to perform a threat hunt for any malicious activity.

Mitiga's Role

Attacker Regained Persistency:

- Identified both old and new Tactics, Techniques and Procedures (TTPs) that the threat actor could have used to gain persistency
- Developed attack scenario variants based on the attacker's previous TTPs
- Performed a series of attacks specifically geared towards the organization's AWS environment

Threat Intelligence – Mitiga conducted threat intelligence efforts, including querying intelligence sources, dark web forums, and underground markets

Value Delivered

- Based on Mitiga's threat-likelihood rating system, we determined that it was Highly Unlikely that the attacker regained persistency
- Determined that no additional leaks or indicators of compromise had taken place before, during, and after the given timespan
- Mitiga completed the execution of this threat hunt within a week, exceeding the customer's expectations

Mitiga's technology and services lower the impact of cyber breaches and optimize readiness for cloud and hybrid incidents and accelerate both response and recovery times when incidents occur. Importantly, Mitiga's readiness prioritization also increases resiliency for future incidents. Mitiga's shared-responsibility model is unique. Unlike others, who charge additional fees for incident response and recovery, Mitiga subscribers face no add-on fees.

For more information, visit www.mitiga.io or email us at info@mitiga.io

US +1 (888) 598-4654 | **UK** +44 (20) 3974 1616 | **IL** +972-3-978-6654 | **SG** +65-3138-3094

MITIGA aws partner network