

24/7 CYBERSECURITY MONITORING (SOC/ SIEM) SUCCESS STORY

Private transportation company

OVERVIEW

Our client was looking for a proactive approach in protecting their data and systems from cyberattacks. They were particularly wary of Apache Tomcat attacks on vulnerable servers. To prevent attacks like these, our client wanted to obtain more visibility on the activity that was happening within their systems and networks. To implement this strategy, the client decided to subscribe to our 24/7 cybersecurity monitoring service.



**Increased
Visibility**



**24/7 activity
monitoring**

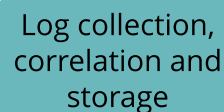
CHALLENGES

Working within the client's environment, we wanted to build a foundation for secure SIEM implementation that will meet the coverage needs of the client's growing infrastructure.

OUR CONTRIBUTION

Virtual Guardian onboarded the client and started monitoring with an industry-leading SIEM platform: IBM's QRadar. This client also wanted to reduce their attack surface further by engaging our vulnerability management service, also delivered by our SOC analysts using Qualys.

SERVICES



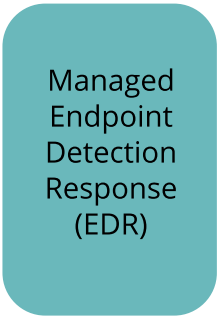
Log collection,
correlation and
storage



UEBA



Network
traffic
monitoring
and
Vulnerability
Management



Managed
Endpoint
Detection
Response
(EDR)

RESULTS

The client has continued to expand this effective SIEM approach with our team and continues to iterate the scope of their growing SOC needs. Today, the client has a reduced attack surface and 100% visibility on suspicious activities happening on their systems.