

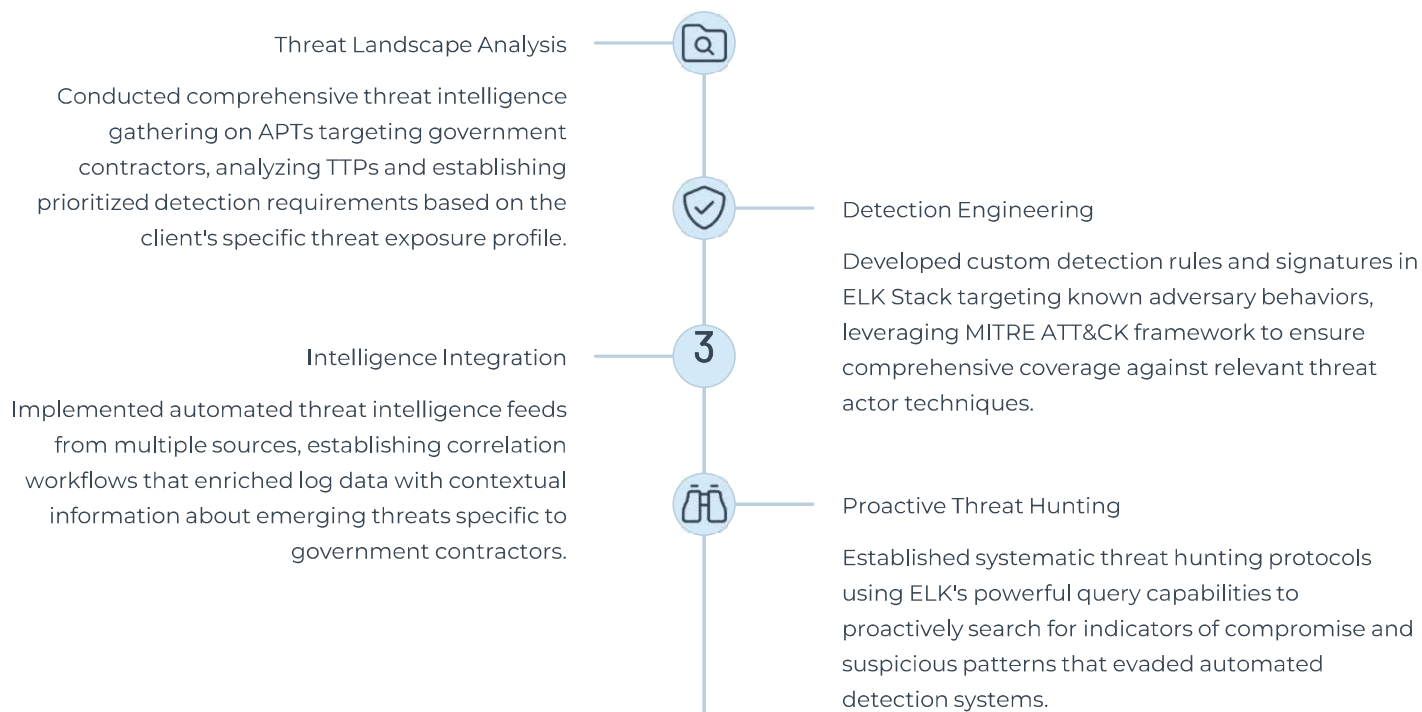
# Case Study: Migrating from LogRhythm to ELK



## Client Background

A mid-sized federal contractor providing critical infrastructure services to multiple government agencies faced significant challenges with threat detection after experiencing several security breaches. With 800 employees operating across both classified and unclassified environments, the organization needed enhanced security intelligence capabilities to safeguard sensitive government data and systems.

Recent security incidents exposed the organization to advanced persistent threats (APTs) specifically targeting government contractors. Their existing LogRhythm implementation proved inadequate for providing the comprehensive monitoring and threat hunting capabilities required. Both the security operations center (SOC) and incident response (IR) teams lacked the sophisticated detection tools necessary to identify and counter advanced threat actors. Furthermore, escalating licensing costs constrained their ability to implement a robust threat intelligence program that met their security objectives.



## Results Achieved

The contractor successfully transformed their security operations with a threat-intelligence driven approach while building cost-effective detection and response capabilities within budget constraints. The ELK solution delivered comprehensive visibility across their environment with specialized detection rules tailored to known adversary techniques. Their security operations team now proactively identifies threats similar to those responsible for previous breaches, leveraging enhanced detection engineering and rapid response capabilities.

Since implementation, the organization has successfully detected and contained multiple sophisticated attacks matching patterns of previous government contractor compromises. Their revitalized SOC and IR teams have prevented three potential security incidents bearing hallmarks of nation-state actors, demonstrating the effectiveness of their enhanced security posture while maintaining federal compliance requirements and optimizing operational costs.