BANK OF ENGLAND

FinTech Accelerator Proof of Concept

ThreatConnect- Enterprise Threat Intelligence Platform

Background

As announced in the Governor's June 2016 Mansion House speech, the Bank has set up a FinTech Accelerator. The Accelerator works in partnership with new technology and firms that use innovative ways of working to help the Bank harness FinTech innovations for central banking. Cyber Security has been and continues to be a priority area for the Bank and hence we have chosen to undertake this Proof of Concept (PoC) to understand how we might conduct our work more efficiently and effectively.

For this project, the Bank sought a solution which would consolidate threat intelligence into a searchable repository that can optimise information collation, enrichment and sharing in support of a proactive, intelligence-led defence strategy.

The PoC ran for a month and was used to understand, the benefits of applying a combination of established and emerging technologies to threat intelligence knowledge management, the ability to improve situational awareness, accelerating the time required to adjust defences and making more efficient use of resources.

The Proof of Concept

Security threats come in different forms. As the number and variety of information sources continue to grow, quick and effective correlation of disparate data feeds is essential to produce actionable intelligence that security teams can rely on to enhance an organisation's network defence.

Most network defence models and technology solutions in use today continue to focus primarily on aggregation of tactical indicators which, when collected and processed in isolation, are limited in the value that they are able to provide to security teams seeking to prioritise detection and remediation efforts. In addition, threat intelligence teams need the ability to perform link analysis in order to identify relevant patterns and provide context to threat information that can be operationalised for proactive defence purposes.

Hence, the Bank wanted to identity a system to easily aggregate and normalize threat data from any source. We were seeking to consolidate the information into a repository that could be effortlessly

recalled to identify patterns, optimize correlation and support a proactive defence strategy. In particular, the Bank wanted to explore how such technologies can support cyber security teams' efforts to optimise intelligence collation and enrichment; automate threat information dissemination into existing network defence solutions; and enhance workflow, intelligence sharing and collaboration (both internal and external) for proactive hunting, quick detection and effective mitigation.

Reflections and Next Steps

The Bank found that the ThreatConnect system enabled effective and open communication between and within teams and the compartmentalisation of information was straight forward. It was quick and easy to share information and to process it, usually using automatic functions to seek, find and describe patterns. The system was able to ingest existing data feeds and then to collate and analyse that data and draw actionable outcomes from it while corroborating findings against live systems.

Currently, the adoption of tools that allow for automated ingestion and exchange of actionable threat information is far from uniform across the financial sector. However, a number of initiatives are taking shape in this area in an effort to promote an integrated collective defence stance.

As such, the Bank is supportive of solutions that support the sharing of strategic, operational and high quality tactical threat intelligence to achieve an informed and rigorous understanding of the cyber threat landscape across the financial sector.