BANK OF ENGLAND

FinTech Accelerator Proof of Concept

Anomali- Threat Intelligence Knowledge Management Tool

Background

The Bank of England set up a FinTech Accelerator in June 2016 to work with innovative firms and new technologies. Cyber Security is a key area that the Accelerator is examining. With an increasing number of cyber threats to identify and respond to, the Bank has been keen to explore solutions that allow it to stay ahead of the rapidly evolving cyber landscape. To evaluate these technologies, the Bank undertook a Proof of Concept (PoC) to test them as part of its day to day work.

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.

After running for a period of two month, the proof of concept demonstrated the benefits of applying a combination of established and emerging technologies to threat intelligence knowledge management, improving situational awareness, accelerating the time required to adjust defences and making more efficient use of resources.

The Proof of Concept

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. 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. 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.

The Bank sought to explore methods to consolidate threat information and intelligence into a searchable repository that can optimise collation, correlation and enrichment efforts in support of 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

Anomali's Threatstream platform works to collect, integrate, hunt and investigate cyber security intelligence data in a highly automated fashion, with integrations into existing security tools.

The Bank found that the platform was intuitive; it integrated well with existing sources of information and allowed highly efficient, automated ingestion and sharing of data. The threat model and overall workflow was a good match to established and well-rehearsed processes, with the ability to associate threat actors, their activities and campaigns and to automatically seek links and patterns in the data while automatically corroborating and enriching the data with relevant context in real-time and against live systems.

In terms of future applications, the technology could be leveraged to enhance the sharing of high quality and validated threat information within trusted circles of peer organisations.

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. The Bank has agreed to extend its working relationship with Anomali.