FINANCIAL COMPANY ASSESSES INTEL CAPABILITIES USING CYBER THREAT INTELLIGENCE SERVICES

OVERVIEW

A large US-based financial services company engaged Mandiant to help establish core intelligence capability and set them on a path toward intelligence capability maturation. They had unfocused, ad-hoc intelligence practices in place, some of which was documented, but only addressed certain daily operational tasks. Intelligence communications were not repeatable. It was determined that the state of capability was not representative of a holistic program or set of capabilities.

Foundational buildout

Initial discussions and deliverables provided via "Threat Intelligence Foundations" helped the client step away from daily operations and understand what should be focused on to build and mature capability. Consultants provided guidance on how to effectively identify intelligence consumers or stakeholders, within the organization, spending extra time on approach for reaching out across the business to determine intelligence appetite and consumption needs. At the end of these activities, the customer's intelligence team was on its way to implementing the basic building blocks of their program via a repeatable process.

Assessment and planning

As the Mandiant team dove deeper into analysis and assessment, we began to measure capability maturity in a variety of areas with a special emphasis on core intelligence capabilities or the minimum set of practices we see as necessary for a successful program. Through the Intelligence Capability Assessment, we identified a set of strengths, weaknesses and recommendations. Collectively, we used this to form a strategic roadmap that captured all results and prioritized a set of initiatives that could be reasonably achieved within twelve months with the resources available to the customer. This provided the customer with a key baseline of capability and roadmap to addressing the areas where the customer was having difficulty:

1. Self-identifying weaknesses
2. Compartmentalizing daily operations from maturation initiatives
3. Prioritizing and focusing efforts

The assessment and strategic roadmap left the client with a clear and achievable path towards an effective cyber threat intelligence (CTI) program.

MANDIANT®
A FireEye® Company

Threat Intelligence Foundations

Threat Intelligence Foundations (TIF) establishes basic building blocks for developing threat intelligence practices and capabilities. It identifies stakeholders and provides a framework for prioritizing threat intelligence practices, communications and use cases.

FireEye®

Mandiant set this customer up with foundational components critical to maintaining a sustainable threat communications workflow as well as a clear strategic roadmap for program growth.

Threat communications: Strategic threat briefing and workflow

A key need for the customer was establishment of efficient, repeatable threat communications. The Mandiant team pivoted to address this following the completion of the assessment and planning work. Together, with the client, we defined the following:

- Specific intelligence communication types, with a focus on strategic briefings
- Format, frequency and content requirements for communications
- Proper messaging, verbiage and branding
- How best to capture stakeholder feedback and incorporate feedback to continuously tune communications to their needs
- How to scale communication activities and communications to operations, by prioritizing stakeholder needs and intelligence communications within boundaries of available resources

Mandiant consultants defined a straightforward, pragmatic threat communications workflow with special interest paid towards Strategic Threat Briefings targeting executive-level audiences. The intelligence team was able to immediately apply this to operations, delivering a briefing product to the CIO based on the template, approach and support we provided. Overall, the customer understood who should be served within the organization along with how, why and with what.

Ultimately, Mandiant set this customer up with foundational components critical to maintaining a sustainable threat communications workflow as well as a clear strategic roadmap for program growth. This set the customer up for immediate wins as well as longer term growth and maturation of the CTI program.

WEEK 1-2

- Foundational Components
  - Identified key consumers of intelligence
  - Identified intelligence concerns and needs
  - Determined proper form of intel consumption for consumers

WEEK 3-6

- Assessment and Planning
  - Assessed core intelligence capability
  - Identified gaps and provided recommendations for addressing
  - Formed strategic roadmap

WEEK 7-10

- Threat Communication
- Built communications executive plan and related workflow
- Customer able to show immediate value of intel program to strategic stakeholders while continuing to grow their capability.

For more information on FireEye, visit:
www.FireEye.com

About FireEye, Inc.

FireEye is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye