Red Teaming Anchors and Sails

CPE provided by Grant Thornton NASBA #108891

whoami

Today’s Objectives

1. Indicate the strengths and opportunities in operating and enhancing in-house Red Team capabilities at a global financial institution.

2. Identifying how value is measured and how this affects processes.

Today’s Agenda

The challenges (anchors) ⚓ and triumphs (sails) ⛵ of operating an in-house Red Team at a financial institution.

Where does the Red Team sit at Northern?

How do we define value?

What is our process?

What are our capabilities?

How do we execute and consume our work?

Q&A

Where does the Red Team sit at Northern?

- Sits in Information **Technology Security Risk Management** ⛵
- **Complements** other testing and assessment work ⛵ ⚓
- Maintain a level of **independence** from the rest of the organization ⚓
- **Not comprehensive** in coverage of the environment or identification of vulnerabilities ⛵ ⚓
- Operating with a **“forward-looking” adversarial mindset**, driven by **objectives** ⛵ ⚓

Key Takeaway: Appropriately positioning the Red Team organizationally to provide an objective assessment of protection, detection, and response capabilities is crucial for getting value out of the investment.

How do we define value?

Our Mission:

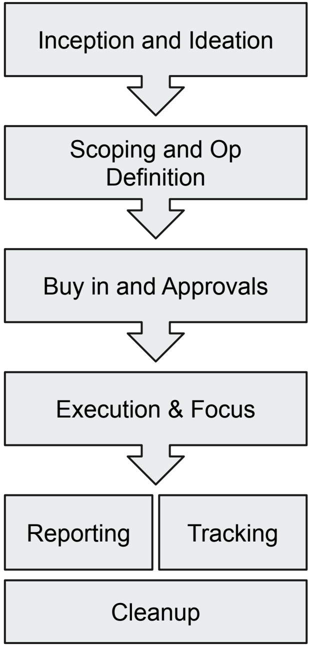
- Challenge assumptions and strategies at the strategic level ⛵ ⚓
- Challenge Internet posture at the operational level ⛵
- Challenge the effectiveness of detection and response ⛵ ⚓

Key Takeaway: Value of the Red Team is driven by a clearly defined mission. The mission should be communicated, understood, and appreciated by Internal and External customers. Delivering on the tenants of the mission can be met with challenges that need to be carefully managed.

Internal Customers
Executive Leadership
Security Operations
Vulnerability Mgmt.
Security & Technology Architecture
Business Units
Operations

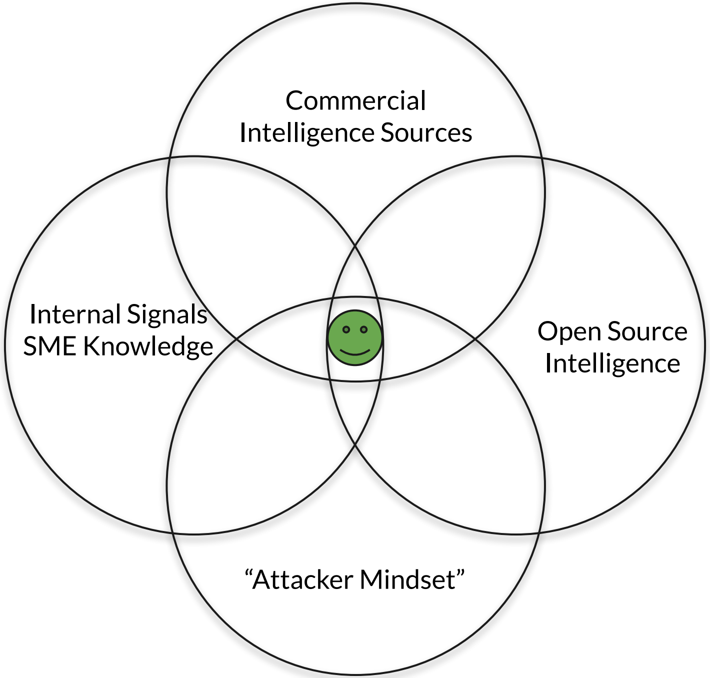
External Customers
Regulators
Clients

What is our process?



- Operate as a service to the organization ⛵
- Develop / create new requests / ideas ⛵
- Align to t**hreat intelligence** ⛵ ⚓
- **Deconfliction** of discovered / identified Red Team activity ⚓
- Sponsorship, buy-in, and ongoing **support** ⛵
- **Deliver** observations, recommendations, narrative, vulnerabilities ⛵
- **Drive** action ⛵ ⚓
- Time elapsed ⛵ ⚓
  - 6-8 months
- Post operation **cleanup**, data **archival**, and **look-backs** for ad-hoc requests ⚓

What is our process? Threat Intelligence


Commercial Intelligence Sources
Internal Signals SME Knowledge
Open Source Intelligence
"Attacker Mindset"

Key Takeaway: Multiple sources of TI can be a force-multiplier, but overuse can quickly lead to analysis paralysis.

What is our process? Exception Management

Deconfliction

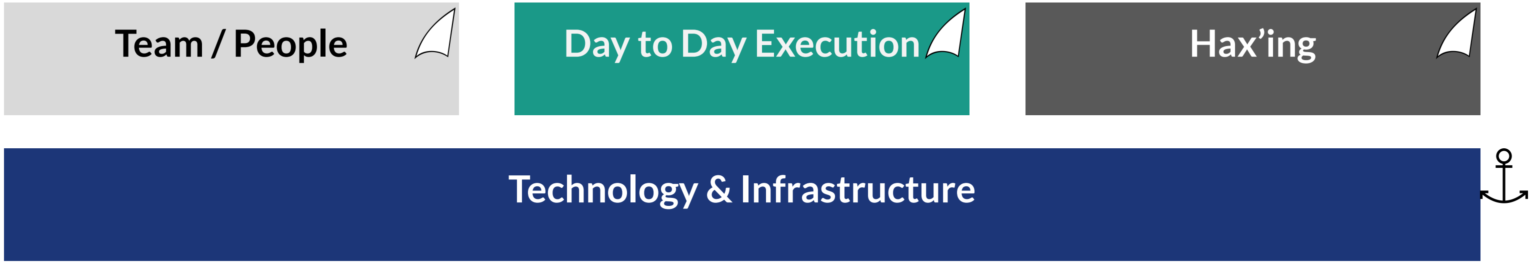
Ex: Red Team activity is identified, but not yet positively attributed. Incident response processes have kicked off.

When something goes ... not as expected

Ex: The team notices that an asset originally believed to be in-scope does not appear to be owned by the target.

Key Takeaway: Manage risk, but also maintain the integrity of the operation. Stakeholder buy-in / approval and clear scoping reduce the impact of exceptions.

What are our execution capabilities?



Team / People

Day to Day Execution

Hax’ing

Technology & Infrastructure

Key Takeaway: Manage risk, but also maintain the integrity of the operation. Stakeholder buy-in / approval and clear scoping reduce the impact of exceptions.

Red Team Operation (RTO) Execution Structure

Team Lead - Responsible for day to day management of people, point of escalation / deconfliction, setting overall team direction / strategy, and actively participating as an Operational Specialist or Operation Lead. Plays large role in team advocacy across the organization.

Operation Lead - Responsible for setting out the scope, designing, coordinating, and managing the lifecycle of an operation. Operates as a daily “decision maker” to ensure that actions taken during the operation are within the scope, objectives, and threat actor profiles as defined. Functions as an Operation Specialist as well.

Operation Specialists - Responsible for technical / tactical execution (hax’ing) day to day.

Logging, Monitoring Operations - Responsible for monitoring and escalating anomalies identified in Red Team attack infrastructure.

How do we report our work?

- Talking to and knowing our customer(s) ⚓
- **Structuring** readouts and managing tactical action(s) ⚓
- **Tracking** vulnerabilities, observations, and recommendations ⛵
- Managing **follow-ups** ⛵
- Measuring **Criticality**, **Risk, Impact, Effectiveness** ⚓

Key Takeaway: Writing reports that your audience can understand is a force-multiplier for obtain agreement to remediate or implement recommendations. Maintaining a capability to follow-up consistently to ensure that appropriate action is being taken is almost as important as the hax.

Q&A