# 10 STEPS FOR CONDUCTING



# OPERATIONALTHREAT INTELLIGENCE RESEARCH

Operational threat intelligence research is essential for organizations to proactively address cyber threats, adapt to evolving risks, and respond effectively to incidents. Follow these 10 steps for successful research with your team.

#### START HERE

#### **Define the Objectives**

- · What are you trying to achieve?
- Is it understanding industryspecific threats or investigating a specific incident?

# **Data Collection**

- 1. Security blogs and websites
- 2. Public forums and communities
- 3. Free threat intel providers 5. Industry groups and alliances
  - 6. Honeypots and honeynets
- 7. Logs from IDSs and IPSs
- 8. Firewall and proxy logs

#### **Analysis**

- **1. Correlation:** linking data, such as IOCs or TTPs, to identify patterns or campaigns
- 2. Trend Analysis: anticipating threats and tracking their evolution
- **3. Attribution:** identifying cyber attackers, for example, by analyzing TTPs, malware, or language

#### **Data Processing**

4. Paid threat intel

providers

- 1. Normalization standardizing diverse
- data formats

  2. Deduplication
  removing redundant

information

- 3. Enrichment adding context to raw
- threat data
  4. Filtering
- retaining only relevant intelligence

#### Dissemination

- Sharing findings with stakeholders within the organization.
- This might include IT teams, executives, or other relevant departments.

# Feedback Loop

Incorporating gathered stakeholder feedback to refine the intelligence collection and analysis processes, aligning them more effectively with the organization's specific needs.

# Operationalization

- Converting intelligence into actionable items.
- Updating the firewall rules, training the staff, or recommending further investigations.

# **Review and Iteration**

Reviewing and refining the threat intelligence process and conducting regular operational threat intelligence research.

#### ONGOING EFFORTS

# **Tooling and Automation**

Leveraging threat intelligence platforms (TIPs) and other tools to automate data collection, processing, and analysis.

#### **Training and Collaboration**

- Training the threat intelligence team on adversaries' latest TTPs.
- Collaborating with other organizations, industry groups, and government agencies to share intelligence and best practices.