“Threat Intelligence” – evidence-based knowledge – including context, mechanisms, indicators, implications and actionable advice – about an existing or emerging menace or hazard to IT or information assets. It can be used to inform decisions regarding the subject’s response to that menace or hazard.¹

“Threat Mitigation” – the elimination or reduction of the frequency, magnitude, or severity of exposure to risks, or minimization of the potential impact of a threat or warning.²

“Risk” – the possibility that something bad or unpleasant (such as an injury or a loss) will happen.³

²http://security.stackexchange.com/questions/tagged/threat-mitigation
³Webster’s Dictionary
The Threat Landscape...

- Technical (not people)
- People who are not good at computers
- People who are good at computers
- People who are good at computers, organized & experienced
- People who are good at computers, organized, experienced & kinetic

Which threat level do you face?
Intelligence Lifecycle

Define Needs With Organization
Configure Collection Management System
Review and Fine Tune System Tasking
Sort, Filter, Vet & Prioritize Data
Analyze Relevant Data
Production
Analysis
Tools
Platform
Collect Data
Vetting/Exploitation
Draft and Deliver to Intelligence Product Organization
Dissemination
Discuss Impact, Manage Follow Up Actions
Take Action
Assess changes to requirements
Information Requirements
Analyzers

Intelligence
Intelligence Efforts Focus

• Identify intelligence efforts that protect the following

• Priority #1: **Self**

• Priority #2: **Third Party & Supply Chain**

• Priority #3: **Indirectly Connected**
The Need For Cyber Assessment...

“An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak”


“Verizon’s Data Breach Fighter Gets Hit With, Well, a Data Breach”


“Hackers Threaten to Release 30GB of Stolen Data From San Francisco’s Municipal Railway”

Threat Intelligence Program Framework

- **Requirements** - What you need
- **Roles** - Who you need
- **Team** - How they’re organized
- **Process** - How the program works
- **Systems** - What the program uses
- **Metrics & Reporting** - How it’s measured
- **Connections** - What & How it delivers

7 Parts
Intelligence Program Part 1 Continued

**Phishing Examples**
- Honeypots, spam email, and links
- Customer Abuse Box Feed/Monitoring
- Org Web Logs
- Phone/SMS messages
- Domain Name Registrations and “Go Live” Alerts
- Phishing Sites Detection System

**Brand Protection Examples**
- Logos and Visual Marks
- Impostor Social Media Accounts
- Copyrighted Image Search
- Claimed Relationships

**Takedown Services Examples**
- Malware
- Imposters
- Confidential Files
- Phishing
- Phone
- Email
Cyber Assessment: Requirements

- Provide to security executives, assessment on either self or Third Party & Supply Chain systems and assets

- Build program to continuously assess and report

- Areas to consider
  - Network Footprint
  - System Compromises & Infections
  - Account Compromises
  - External Facing Vulnerabilities
  - Domain & Spear-Phishing Risk
  - Intelligence Indications & Warnings
Intelligence Program Part 2

- Tip: Focused On Specific Deliverables

- Program
  - Planning
  - Architecture
  - Strategy

- Security Subject Matter Experts (SME)
  - Cyber Analysts
  - Social Analysts
  - Phishing Analysts
  - Malware / Forensic Specialists
  - Incident Response Specialists
  - Brand Protection Analysts
  - Rogue Applications
  - Third Party Risk Analysts
  - Physical Security Analysts
  - Language & Translation Specialists

- Network System SMEs
  - Network Security Operations
  - Network Integration Specialists

- Systems Development SMEs
  - Software developers
  - Data processing
  - Data analytics
  - Data visualization
Cyber Assessment: Roles

- Roles required
  - Planning
  - Architect
  - Manager
  - Cyber Analyst
  - Social Analyst
  - Third Party Risk Analyst

- Software developers covering
  - Data processing
  - Data analytics
  - Data visualization
Intelligence Program Part 3

- **Tip: Consider Tiered Structure**
  - Support 24x7 Operations

- **Structure**
  - Manager
  - Tier 1 Cyber Threat Analysts (junior)
  - Tier 2 Cyber Threat Analysts (senior)

- **Typical Work Schedule**
  - 12 hour shifts 4on/4off with relief support

- **Tiered Structure Essential**
  - Tier 1 Example: 24 full-time Cyber Analysts
  - Tier 2 Example: One full-time Senior Cyber Threat Analyst and Three full-time Cyber Threat Analysts

- **Backup/Resiliency**
  - Have permanent remote team members as geographic backup and resiliency support
Cyber Assessment: Team

- **Structure**
  - Manager
  - Cyber/Social/Third Party Analysts
  - Software Development

- **Work schedule**
  - On demand
  - 9-to-5
Intelligence Program Part 4

• **Tips:**
  - Functional Area Specific
  - Keep It Current
  - Invest in Technology Improvements
Intelligence Program Part 4: High Level Process

24x7 Real-Time Intelligence Processing

**Tier 1: Rapid Alerting**
- Feed Vetting/Noise Reduction
- Data Tagging
- Review Criteria Relevancy
- Additional Capture (e.g. Screenshots)
- Alert

**Tier 2: Contextual Alerting**
- Data Verification
- Adding Context – 5Ws
- Additional Tagging for Data
- Lake/Threat Landscape
- Quality Review
- Hotline

**Response 10 to 30 min after collection**

**Average alert 1 to 3 min after collection**

Ingest → Escalation → Relevancy Feedback

Quality Feedback

Organization Threat Response & Reporting

Local Telemetry
Local Org Data
Third Party Data
Industry Data
Global Actor Data
Global Cyber Data

© 2017 LookingGlass™ All Rights Reserved.
Intelligence Program Part 4: Phishing Detection Specific Workflow

Start
Assign Ownership
Site Review
Action Needed
Yes
Close Incident
End

Update Status
Create Action
Initiate Action
Determine Action
Type Required

Status Options
Not Reviewed
Under Review
Call - Waiting for Response
Email - Waiting for Response
C&D - Waiting for Response
No action needed
Monitor
Closed

Incident Target Issues
Claimed Relationship
Domain Name Violation
Image Use
Multi-Issue
Objecti onable Content
Traffic Diversion
Threat

Roles
System
SOC Manager
SOC Analyst
Analyst
Manager

Requirements
Operations
Team
Systems
Metrics & Reporting
Connections

© 2017 LookingGlass™ All Rights Reserved.
Cyber Assessment: Process

- **Gather**
  - Domains & Systems
  - User Accounts
  - Applications

- **Assess**
  - Network Footprint
  - System Compromises & Infections
  - Account Compromises
  - External Facing Vulnerabilities
  - Domain & Spear-Phishing Risk
  - Intelligence Indications & Warnings

- **Report**
Intelligence Program Part 5

• **Tips**
  - Identify system based on functional requirements
  - Best-in-class focus

• Systems to support process include
  - Threat Intelligence Platform
  - Response Management
  - Cyber Intel Workflow
  - Phishing Workflow
  - Social Media Intel Workflow
  - Help Desk
  - Time Management
Intelligence Program Part 5

- **Custom Web Application for Analysts**
  - Enter profile data
  - Monitor and review status of automated pipeline
  - Connects set of collection systems

- **Systems Used**
  - Vulnerability Scanner
  - Both Open Source and Commercial Network Footprinting
  - Domain Analysis
  - Dark and Surface Web Crawlers
  - Database and Spreadsheets
  - Threat Intelligence Platform (and aggregated MRTI)
  - Internet Intelligence
Intelligence Program Part 5

System Process

- Requirement
- Roles
- Team
- Process
- Systems
- Metrics & Reporting
- Connections

Plugins
- Infection Records
- Compromises
- Network Intelligence
- Open Source
- Vulnerability Scan

Settings
- From
- To
- Max. Limit Total Results per Plugin
- Max. Limit per Footprint

After the scan is completed you can see the results and remove them individually before preparing the final report. When you restart a scan all results for the plugins are deleted.
Intelligence Program Part 6

**Tips:**
- Who are reports for
- Expected outcomes of reports

**Including**
- Daily/Weekly Metrics Reporting
- Threshold Alerting
- Event Notifications
- Visual and Electronic Event Triggers
- Workflow/Time analysis
Intelligence Program Part 6

- Reports
  - Specific
  - Segmented
  - Actionable
  - Business Relevant
Intelligence Program Part 6: Report/System & Account Compromises

- Analysis & Summary on
  - Total Records Analyzed
  - Recent Breaches Listing
  - Unique Users Covered
  - Malware Infections Found
  - High-Recurrence Users
  - Reputation Risks
  - Executive Credentials

EVIDENCE OF SYSTEM COMPROMISE OR INFECTION

0: Low
Key Takeaways: Out of the 92 queryable network elements discovered in the footprinting process for AcmeTech, no active malware, botnet, or other suspicious campaigns were found associated with the target in 2016 or 2017.

By leveraging the LookingGlass ScoutVision™ threat intelligence repository, we correlated more than 100 internal, commercial, governmental and third party data feeds with the indicators associated with AcmeTech’s publicly accessible network footprint. This process identified no threatening indicators associated with AcmeTech networks. No derogatory information was uncovered in this module. Similarly, no history of infection was discovered either. This is a very positive indicator, as a completely “clean” report in this section is relatively rare in LookingGlass’ past experience.

COMPROMISED ACCOUNT CREDENTIALS

60: Medium
Key Takeaways: LookingGlass identified 97 total records associated with 45 unique users. In each area of analysis - recency, recurrence, source, leadership team, etc. - AcmeTech was generally in line with our typical findings except for the relative number of users found compared to the size of the company workforce (approximately 9%, or double our 4-5% average.)

Since the majority of systems and websites now use the user’s email address as the username, any account credentials or breach data found that contain an email address and password where the email is tied to the Target Entity indicate a significant potential risk. The most obvious risk from such breached account data is direct access to company systems. For example, it is simple to check for Outlook Web Access (“OWA”) or other Web-based mail services associated with each domain, potentially allowing a hacker access to the user’s work email account, and possible viewing or exfiltration of all the sensitive information it may contain.
Intelligence Program Part 6: Report/Vulnerabilities

- Listing sites analyzed
- Assessment of active vulnerabilities found
- Number of instances

VULNERABILITIES IN EXTERNALLY-FACING APPLICATIONS

Key Takeaways: Despite the small size of its outward-facing network footprint, AcmeTech is at risk for a number of common cyber attack vectors, including Cross-Site Scripting (XSS), BREACH, Denial-of-Service (DoS), cookie hijacking, and password brute-force cracker attacks.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Vulnerability</th>
<th>Identifier</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>Clickjacking</td>
<td>CWE-693</td>
<td>3</td>
</tr>
<tr>
<td>Medium</td>
<td>BREACH attack (CVE-2013-3587)</td>
<td>CWE-310</td>
<td>1</td>
</tr>
<tr>
<td>Medium</td>
<td>Slow HTTP DoS Attack (Apache-Based)</td>
<td>N/A</td>
<td>1</td>
</tr>
<tr>
<td>Medium</td>
<td>Host header attack</td>
<td>CWE-20</td>
<td>1</td>
</tr>
<tr>
<td>Medium</td>
<td>Apache 2.x version older than 2.2.6 (CVE-2007-3842)</td>
<td>CWE-20</td>
<td>3</td>
</tr>
<tr>
<td>Medium</td>
<td>Apache 2.x version older than 2.2.8 (CVE-2008-0006)</td>
<td>CWE-79</td>
<td>3</td>
</tr>
<tr>
<td>Medium</td>
<td>Apache 2.x version older than 2.2.9 (CVE-2008-2364)</td>
<td>CWE-399</td>
<td>3</td>
</tr>
<tr>
<td>Low</td>
<td>Apache 2.x version older than 2.2.10 (CVE-2010-2271)</td>
<td>CWE-79</td>
<td>3</td>
</tr>
<tr>
<td>Low</td>
<td>Ruby on Rails CookieStore session cookie persistence</td>
<td>CWE-284</td>
<td>3</td>
</tr>
<tr>
<td>Low</td>
<td>Login page password-guessing attack</td>
<td>CWE-307</td>
<td>4</td>
</tr>
<tr>
<td>Informational</td>
<td>Password Type Input with auto-complete enabled</td>
<td>CWE-200</td>
<td>4</td>
</tr>
</tbody>
</table>

Potential False Positives:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Vulnerability</th>
<th>Identifier</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>Backup Files</td>
<td>CWE-538</td>
<td>150</td>
</tr>
<tr>
<td>Medium</td>
<td>Application Error Message</td>
<td>CWE-200</td>
<td>1</td>
</tr>
</tbody>
</table>
Intelligence Program Part 6: Report/Domain & Spear-Phishing Risk

- Company owned domains
- High risk domains

**DOMAIN PORTFOLIO AND SPEAR PHISHING RISK**

Key Takeaways: The review of AcmeTech-related domains discovered only one site of concern. However, this one site, HR-AcmeTech.com displays numerous characteristics that lead the LookingGlass team to believe that there already is, or soon will be, an attempted spear phishing campaign aimed at AcmeTech.

A review of known registered domains related to the AcmeTech brand and website found a total of 17 registered domains of potential interest, 9 related to the AcmeTech brand/string, and 8 additional domains identified based on common and look-alike character substitutions of the type typically used in successful spear phishing attacks. Specifically, the strings matched in the analysis were:

1. acmetec  
2. amcetec  
3. acmteec  
4. acmteec  
5. acmteec
Intelligence Program Part 6: Report/Intelligence & Warnings

- Aggregated view of threat intelligence reports
- Context and background to support analysis
- Analysis and prioritization
- Recommendations on critical intelligence to act on
• **Use Case**

Intelligence Program Part 6: Report/Exec Summary

- Provide to security professionals...
  - **Insight** into application vulnerabilities
  - **Information** on potential leaks, theft of sensitive data
  - **Identify** holes in internal security posture to ensure compliance
  - **Identify** latest data breaches and compromised user accounts
  - **Reduce risk** of high impact exploits such as ransomware, website defacements or malicious injection
Intelligence Program Part 7

- **Tip:** Empower rapid response to incidents and maintain goodwill

- Internal Systems and Groups
  - SecOps/NetOps
  - IT, Compliance, Third Party Risk

- Supply Chain
  - Infosec/SecOps

- Industry Connections
  - Data Feeds (Open, Commercial)
  - Technology Learnings
  - Trusted Sharing

- Law Enforcement Connections
Intelligence Program Part 7

• Final report influences and updates connected teams

Requirements
Roles
Team
Process
Systems
Metrics & Reporting
Connections

Use Case

Systems Patched
Vulnerability Mgmt Teams

Policy & Password Changes
IT Team

Supply Chain Updates
Policy and Enforcement
Third Party Risk Team

Security Rules Update
NetOps & SecOps Teams

- Provided Inputs
- Network Footprint
- Target Profile
- Final Report

Endorsement of System Compromise or Infection
Compromised Account Credentials
Vulnerabilities in Externally-Facing Systems
Domain Portfolio and Spear-Phishing Risk
Threat Intelligence: Online Indicators and Warnings
Recommendations

**Justify** Threat Intelligence Program to reduce **business risk**

**Define** program across
- Requirements
- Team
- Roles
- Process
- Systems
- Metrics & Reporting
- Connections

**Focus** intelligence
- Self
- Third Party
- Indirect

**Protect** business leveraging threat intelligence