MITRE ATT&CK TRAINING

* Using ATT&CK for CTI Training
* Module One - Introduction
  + Understanding ATT&CK
    - Tough Questions for Defenders
      * defense effectiveness
      * worth of collected data
      * toll coverage overlaps
      * are the products being used, effective?
      * preparedness for APTs?
  + What is ATT&CK
    - knowledge base of adversary behavior based on real world observations
      * not theoretical, simulated, red team based
    - common language framework for threat identification, community driven and open source
  + Bianco Pyramid – effort for attackers to change their MO’s
    - Hash Values – Trivial Difficulty
    - IP Addresses – Easy
    - Domain Names – Simple
    - Network/Host Artifacts – Annoying
    - Tools – Challenging
    - TTPs – Tough
  + Breaking Down the ATT&CK Matrix
    - Tactics Rows – High Level Technical Goals
      * Technique Columns – how the goals are achieved
        + Procedure Examples – specific implementations of said techniques

highly detailed

textbook definition of activity, why, how

Metadata

Mitigations

Detection Methods

Specific examples of particular actors carrying out said TTPs

* + - Group Information
      * Group ID, Group Descriptions, Aliases
      * Techniques used, Software used
  + Uses Cases
    - Detection
      * behavior analytics
    - Threat Intelligence
      * track adversaries, compare/contrast behaviors between and amongst groups, store intel
      * inform defenders
    - Assessment and Engineering
      * determine security engineering priorities
    - Adversary Emulation
      * red team emulation, coordination with blue team
* Module Two – Mapping to ATT&CK From A Finished Report
  + Difficult to Map CTI
    - shift in analytical thinking from indication to behaviors
    - sheer volume of ATT&CK techniques and their detail
  + Mapping Process
    - * Understand ATT&CK
      * Find the Behavior
      * Research the Behavior
      * Translate behavior into a tactic
      * Figure out what technique applies to the behavior
      * Compare results to other analysis
    - Two key sources
      * finished reporting
      * raw data
  + Understand ATT&CK
    - watch presentation
    - read the Philosophy Paper and Getting Started Series
    - read Tactic descriptions
    - skim Technique list
    - do weekly Technique presentations
  + Find the Behavior
    - Look for what the adversary or software does
    - initial and/or post-compromise details
      * not all information will be useful for mapping
        + static analysis
        + infrastructure registration information
        + industry/victim targeting information – diamond model
      * verbs, tools commonly used, processes
  + Research the Behavior
    - do additional research
      * internal and external resources
    - understanding core behavior
  + Translate the Behavior into a Tactic
    - intent, context from finished intelligence
    - twelve options
      * initial access
      * execution
      * persistence
      * privesc
      * defense evasion
      * credential access
      * discovery
      * lateral movement
      * collection
      * c2
      * exfil
      * impact
    - Review summary of malware and apply to the above twelve
  + Figure Out What Technique Applies
    - toughest part
      * not every behavior maps
    - Look at list of Techniques for the ID’d Tactic
      * search attack.mitre.org
        + key words
        + procedure-level detail
        + command strings specifics
        + differing levels of granularity amongst techniques
    - be careful when looking to skip steps – may increase biases and will not always work
* Storing and Analyzing ATT&CK-Mapped Data
  + Considerations for Intelligence Storage
    - Human/Machine
    - Requirements, Context, Detailing
    - Technique and/or Procedure
    - How is this intel linked with other intel
    - Formatting
  + Examples
    - MISP Threat Sharing
      * Galaxies
      * Link indicators and files
    - Anomali
      * Summary
    - McAfee
      * Summary
      * Techniques
      * Procedures
    - Crowdstrike
      * Techniques
      * Summary
    - Recorded Future
      * Timestamps
    - Unit42
      * Indicator Patterns (machine readable)
      * atomic indicators linked to techniques
  + Once Intelligence is Stored – What Can Be Done With It?
    - Overlay TTPs between groups to detect overlap, commonalities
      * Threat-Informed Approach
    - ATT&CK Navigator
      * visualize attack data
      * github – ATT&CK Matrix
        + TTPs
      * Toolbar
        + Multi-Tactic Technique Selection

Search Menu

Multi-Select

Groups or software

Deselect

* + - * + Layer Information

Naming, Description, Metadata

Download Layer in JSON for export

Export to Excel

Render to SVG for image type

Filter by Platform (OS) or Stage (Pre/Post)

Sort Options – ascending/descending

Coloring Options

low/high values from Scoring below

Toggle View Mode

* + - * + Technique Controls

Disable Certain Options

Show/Hide Certain Options

Background Color

Scoring

Comments

Clear Annotations on Selected Techniques

* + - * Create Layer from Other Layers
* Making Defensive Recommendations From ATT&CK-Mapped Data
  + Applying Technique Intelligence to Defense
    - * + making intelligence actionable
    - Process for Making Recommendations from Techniques
      * Determine Priority Techniques
      * Research How Techniques Are Being Used
      * Research Defense Options Related to Technique
      * Research Organizational Capability/Constraints
      * Determine What Tradeoffs Are for Organization on Specific Options
      * Make Recommendations
  + Determine Priority Techniques
    - Data Sources – what has already been collected
    - Threat Intelligence – what are adversaries doing
      * Spearfishing
      * Scheduled Tasks
      * Scripting
      * User Execution
      * Registry Run Keys/Startup Folder
      * Network Service Scanning
    - Tools – what can current tools cover
    - Red Team – what can red teams be capable of emulating
  + Research How Techniques Are Being Used
    - what specific procedures are being used for a given technique
      * ensure response overlaps with activity
  + Research Defensive Options Related to Technique
    - many sources provide defensive information indexed to ATT&CK
      * ATT&CK
        + data sources
        + mitigations
        + detection
        + references
      * MITRE CAR
      * ThreatHunter-PlayBook
      * Atomic Threat Coverage
      * Windows ATT&CK Logging Cheat sheet
    - supplement with self-research
  + Research Organizational Capabilities and Constraints
    - * what data sources, defenses, mitigations are already being collected
        + new options may be inexpensive
        + possibly new analytics on existing sources
      * what products are already deployed that may have additional capabilities
      * is there anything that may preclude responses
  + Determine What Tradeoffs Are for Organization on Specific Options
    - highly specific, options need to fit into organization
      * budget, culture
  + Make Recommendations
    - Technical
      * data sources, analytics, configurations, tools
    - policy
      * technical/human prep
    - risk acceptance
      * tradeoff/cost, undetectable, unmitigable
    - management, SOC, IT, etc.