Bringing Red, Blue and Purple Teaming into Balance

By Tim Medin, IANS Faculty

Contributor: Dave Kennedy, IANS Faculty

Agenda

- Introduction to red teaming
- Introduction to blue teaming
- Building a purple team
- Identifying KPIs and metrics
- Using scorecards to track capabilities
- Where to go from here

Introduction to Red Teaming

What makes a red team valuable?

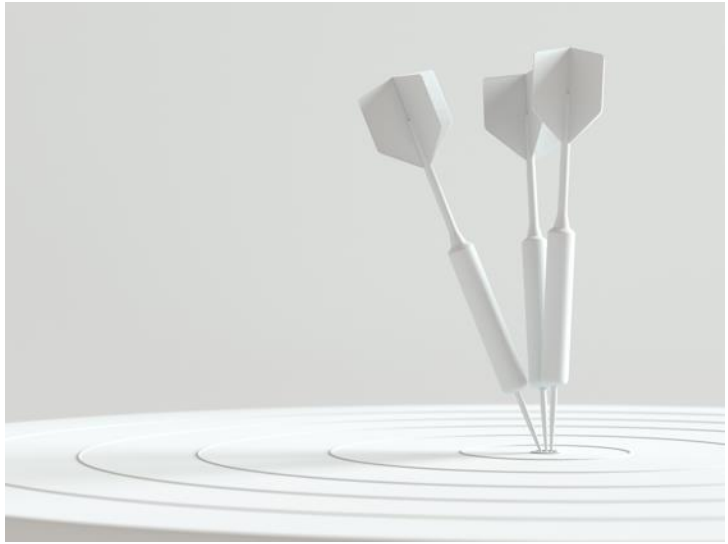
Definitions

- **Red team exercise:** The act of emulating a realistic attack specifically using an attacker's mindset
  - Red team exercises can be performed by an internal red team or a third-party
  - They are typically held annually

- **Red team:** An individual or group with highly specialized skills that acts as the attacker during a red team exercise

The Purpose: The Attack

- **Traditional penetration test:** Assesses either the entire organization or a selected business unit to identify specific vulnerabilities
- **Red team:** Assesses if a determined attacker can compromise an organization in any way



IANS

Benefits: Red Team

- Real-world attacks
  - Doesn’t just focus on exploiting a vulnerability
  - Uses methods that exploit multiple points in a security defense
  - Often chain-attacks to finally gain access
- Accurate assessment of security posture
  - Gain better insight into all your controls, not just the technical controls
  - Provides key performance indicators (KPIs) for scoring and helps align remediation efforts

IANS

Introduction to Blue Teaming

The defense

Definitions

- **Blue teaming:** The defense of an organization, including protecting against attacks and hardening systems
  - Blue teaming can be done by an internal team or a third-party
- **Blue teams:** An individual or a group with highly specialized skills that works to improve the overall security posture of an organization
  - Multiple groups can make up a blue team – threat hunting, forensics, firewalls and more

The Purpose: Detection

- Traditional defense
  - Designed around vulnerability management
  - Focuses heavily on patching and performing scans to establish KPIs
- Blue team
  - Designed to assess if other gaps could allow an attacker to gain unauthorized access to any system or physical location

Benefits: Blue Team

- Focuses on industry standards
  - Uses well-known and respected standards to create KPIs for a business unit
  - Recommends appropriate focus on specific vulnerabilities or security gaps for remediation
- Works with penetration testers
  - Collaborates with penetration testers to validate security controls and identify gaps
  - Uses penetration test results to guide remediation efforts

Building a Purple Team

Collaboration between offense and defense

Definitions

- **Purple teaming:** The process of performing attacks and analyzing them in real time using defensive controls
  - With purple teaming, both the red and blue team work together, often simultaneously
- **Purple team:** A group made up of both red and blue teamers with highly specialized skills that focuses on generating several attacks and evaluating defensive controls

Building a Team

- Ensure the correct ratio of red and blue
- Establish that it's one team; this is not about red **vs.** blue
- Have the team focus on non-standard and out-of-the-box attacks that go beyond simple vulnerability exploitation
- Include subject matter experts (SMEs) from all parts of the blue team along with highly skilled red team members

Get the Correct Ratio of Red and Blue

- How many red teamers?
  - Depending on the size of the organization, purple teams typically have two to four red teamers
  - There should be enough red to provide work for the blue, but not so many that it turns into just another penetration test
- How many blue teamers?
  - Purple teams should be more blue than red
  - Two to four blue team members is typical
  - Teams should have at least one SME from each security control

Size and Maturity

- How big should the team be?
  - Industry demographics play a large role
  - Financials usually have the largest purple teams
- Teams range from ad-hoc (non-dedicated) members to multiple individuals with different skill sets
- Some conduct ongoing engagements while others (smaller organizations) do annual exercises
- Leveraging third-party consulting can help increase maturity

Working as a Single Team

- This is not an us-vs.-them scenario
- The purple team leverages the skillsets of both the red and blue team members to improve the security posture of an organization

Non-Standard and Out-of-the-Box Attacks

- Send as many attacks as possible
  - The point of the purple team is not for the red team to remain hidden
  - Attacks should come in very rapidly
  - Use attacks that aren't already performed in normal penetration tests or during vulnerability scans
- Identify new techniques just released on social media
  - For example, try command line evasion techniques designed to avoid detection

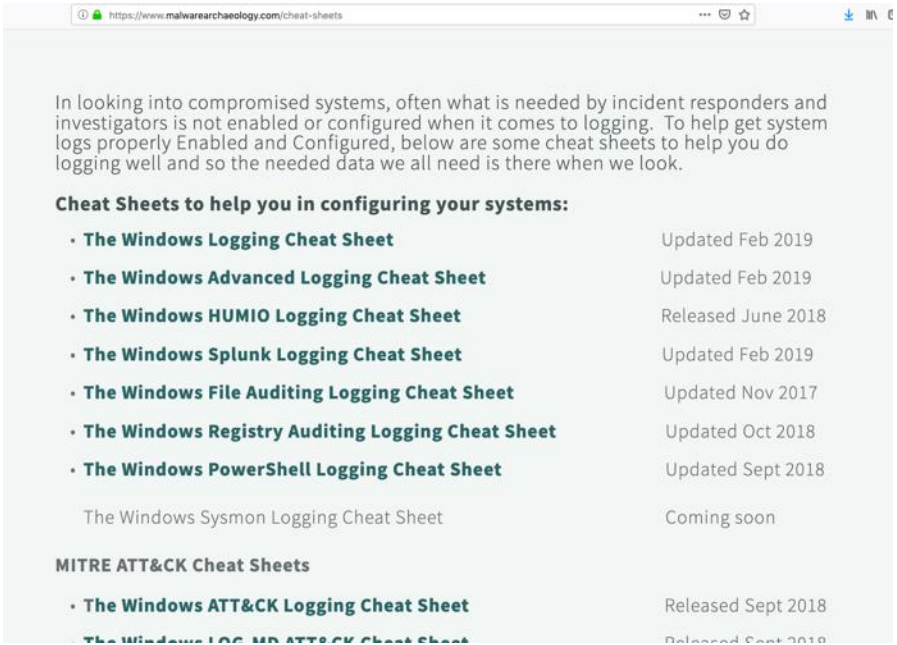
Team Skills

- Top skills include:
  - Red teaming and understanding attack tactics
- Top roles include:
  - Systems admins
  - Web application security
  - SIEM SMEs
  - Endpoint detection and response (EDR) SMEs
  - Network admins

What Should We Log? Everything?

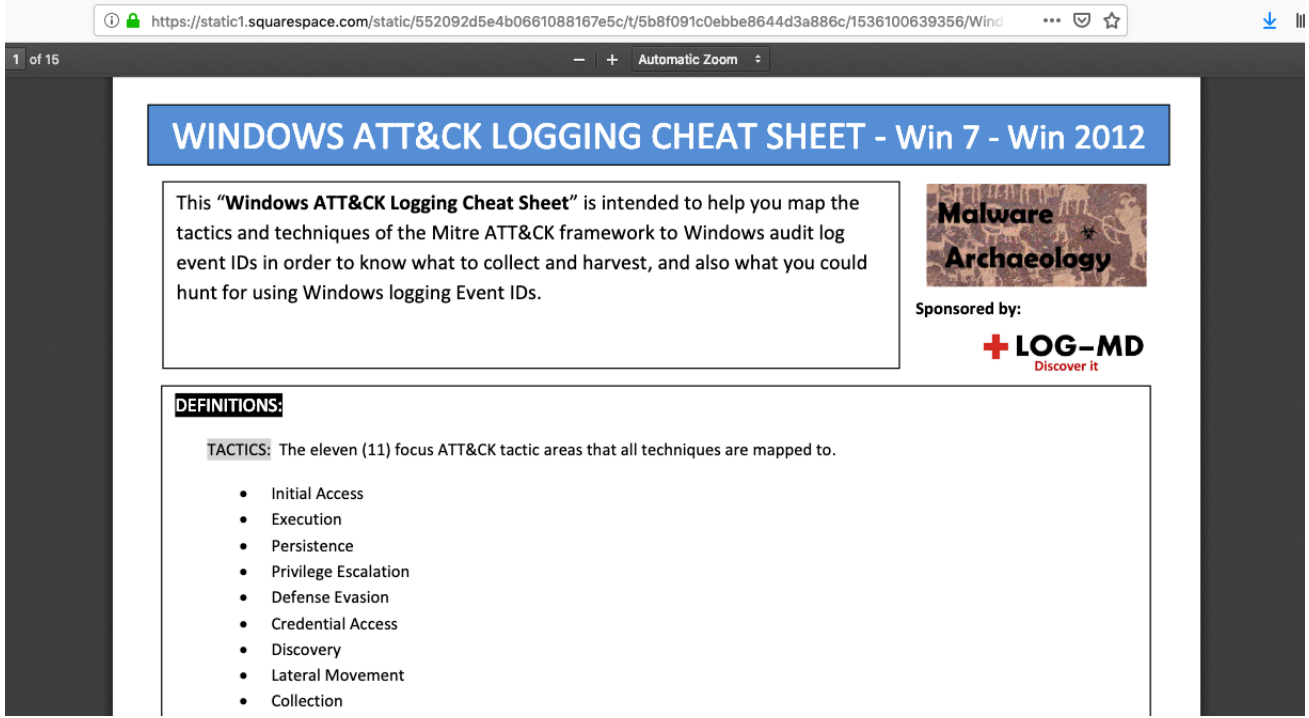
- We need endpoint logs (sorry)
- Endpoint logs tend to be one of the most fruitful for providing early warning of compromise
- You don't need them all, but you will need some

Good Reference Point



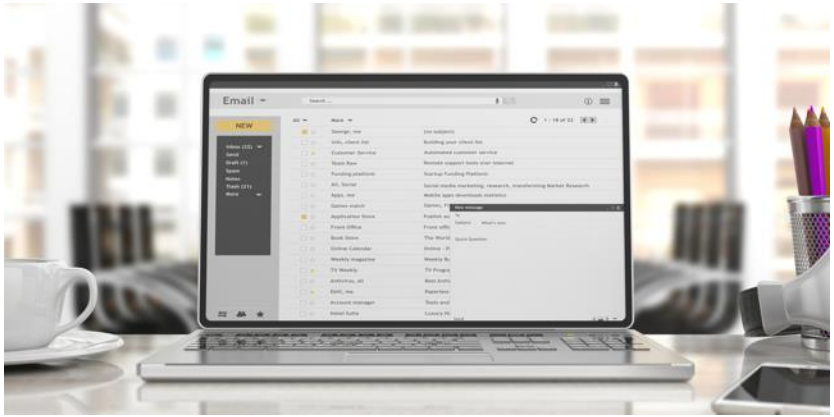
- https://www.malwarearchaeology.com/cheat-sheets

MITRE ATT&CK Integration



For Workstations – You Need Endpoint Logs!

- Endpoint logs are a must!
- Tools that can help:
  - OSQuery is great for Linux, OS X and Windows (https://osquery.io/).
  - For Windows, Sysmon is fantastic
    - Exposes kernel-level Event Tracing for Windows (ETW)
    - It's free from Microsoft



IANS

Sysmon Basics

- Can be customized based on data type
- Great community resource here:
  - https://github.com/olafhartong/sysmon-modular
- Lets you monitor several key areas to get an EDR-type visibility
- Allows you to monitor common and uncommon techniques, such as process injection, Mimikatz and more

Event Volume Concerns

- For those concerned about the sheer volume of events, consider using something like ElasticSearch
- ELK (ElasticSearch, LogStash and Kibana) is open source and can handle large scale
- Allows a substantial amount of information for your teamers to go through

Fostering a Team

- Fostering a healthy team is equally important
  - Manage knowledge using Confluence, Slack, etc.
  - Provide opportunities for training and growth
  - Consider automation; ensure you can conduct operations if someone leaves
- Budget for conferences and fun

KPIs and Metrics

- KPIs are often challenging in information security in general, but direct KPIs can be measured with a purple team approach
- No. 1: Mapping detection enhancements to detection capabilities
  - New detections should be integrated into the security operations center (SOC)
  - Ensure communication and knowledge transfer with/to the SOC
- Number of valuable log or intelligence sources, or refined hunting methods

Balanced Scorecard for KPIs

- The concept isn't just for security: https://en.wikipedia.org/wiki/Balanced_scorecard
- Great talk on this from Chris Nickerson and Chris Gates at BruCon:
  - https://www.youtube.com/watch?v=Q5Fu6AvXi_A
- Mapping to capabilities
  - https://attack.mitre.org/wiki/Main_Page
  - https://attack.mitre.org/wiki/Adversary_Emulation_Plans
- Balanced scorecard (example)
  - https://docs.google.com/spreadsheets/d/1pI-FI1QITaIjuBsN30au1ssbJAZawPA0BYy8Ip6_jV8/edit#gid=420971399

Knowledge Transfer Is Critical

- The main purpose of a purple team is to enhance the overall monitoring and detection program
- When new indicators of compromise are identified, getting new detections to the SOC for analysts is important
- Continual knowledge transfer from the purple team to the SOC is critical

Conducting a Purple Team Exercise

One team. One goal.

Step 1: Establish Baselines

- Establish a baseline of what can be detected or blocked
  - Perform attacks and check detections
- Good starting points:
  - Command line auditing (EventID: 4688)
  - User authentication (EventIDs: 4624 and 4625)
  - PowerShell commands (EventID: 4104)
  - Kerberos query (EventID: 4769)
  - New user added (EventID: 4720)

Step 2: Build Detections

- Look for abnormal patterns
  - Count the number of commas in a command line process
- Build the detection for an attack, even if you have a control that blocks it
  - The control may be removed or fail, or there may be a way to bypass it
- Try to perform the same attack multiple ways to ensure the detection catches all attacks

Step 3: Refine Detection

- Ensure detection controls are working and not too specific to a single attack
- Ensure the detection doesn't rely on a manual process for an alert
- Attempt to reduce the noise-to-signal ratio to increase the fidelity of the detection
  - It often takes some tuning to remove known systems that emulate an attack, such as a vulnerability scanner

Step 4: Replay the Attack

- Once the detections are created, updated or refined, replay the attack to ensure the detection is working as intended
- Adjust the attack slightly to ensure the detection isn't over-engineered or too specific
- Validate the fidelity on the alert to ensure you don't miss other systems adding noise to the detection

Good References

- Simulate different phases of the MITRE ATT&CK framework
  - https://attack.mitre.org/
- Leverage the Atomic Red Team framework to help augment detections and tests
  - https://github.com/redcanaryco/atomic-red-team
- Scenario-driven exercises can help keep things fun

Purple Team Output Deliverables

How to use an exercise

Strategy Roadmap 1

- After an exercise, you will come out with technical validation and areas for improvement
- Using the output as a method for validating your strategic infosec roadmap is huge
- Map deficiencies and the best ways to improve

Mapping Deficiencies

- During Purple Team Exercise 1, the organization finds additional logging is needed to identify a certain part of an attack
  - Low, moderate or high attack coverage is determined
  - This is mapped to an overall matrix to track coverage for multiple, different attack phases
- During the exercise, deficiencies are documented and remediation performed
  - Can we write a detection now?
  - What do we need to do so?

High-Level Communication

- Purple Team exercises help determine if a security program (and its technology) is effective
- Helps underscore the need for additional staffing and highlights weak areas in the program
- It's also important to leverage threat modeling to understand the overall risk from attackers and set priorities for the program

Reporting

- The coverage (mission/scope)
- Gaps identified
- Breakdown of both strategic and technical findings
- Project plan for remediation efforts
- After action: What can we do better? How can we improve?

Wrapping Up

Putting it all together

Success Is Measured in People

- People make a successful purple team
- Technology augmentation is important, but tools cannot keep up with the pace of attacks
- Investment in people is crucial

KPIs and Metrics

- Establishing clear outcomes and responsibilities for a purple team can drastically increase its value
- Using outcomes to both build a strategic roadmap and address technical findings is important
- Enhancing the SOC and building up the teams to be one unit is critical to success
- Designating clear owners of exercises and conflict resolution pays dividends

Purple Makes the World Better

- Organizations that conduct purple team exercises quickly find their overall security is *better*
- Groups tend to work more effectively with one another and communication becomes continual between groups
- Regular purple team exercises can help validate your program and its weaknesses, while improving it drastically

Questions?

Thanks for attending!