DevBlue

Applying Software Engineering Practices to Blue Teaming for the Win!

March 3, 2020

Ismael Valenzuela | Sr. Principal Engineer
Lucía Coppes | Detection Engineer
Alejandro Houspanossian | Manager, Software Engineer
About us

- Enterprise Products – Detection Engineer at McAfee (Argentina)
- Experience as Software Engineer and Computer Forensics
- Twitter: @lucoppes

- Sr. Principal Engineer at McAfee
- SANS 530 co-author and instructor
- 20 yrs. defending all the things!
- GSE #132
- Twitter: @aboutsecurity
Meet DevBlue, the merge of two worlds

Developers
- Software Engineering Practices
- Agile Practices
- Software Quality
- Release Management
- Automation

Blue Teamers
- Cybersecurity
- Hunting & SecOps Tools
- SOC Operations
- Networking
- Forensics
- Adversarial Emulation
- Incident Response

DEVBlue
- Adversarial Attack Emulation
- Atomic Red Team Automation
- Hunting and Research
- Continuous Delivery
Challenges & Learnings

- How we track our tasks and show our progress
- How we assure the Quality of our Detections
- How we achieve Continuous Delivery
- What Purple Team Exercises we do
- What our Training plan is
Issue Tracking System

Benefits:
- Clarify scope
- Leverage research
- Understand available resources
- Improve communications

EPIC (New feature / Improvement)

- Story
- Story
- …
Creating our backlog

We need more granularity
## How we map the ATT&CK Matrix into the Issue Tracking Tool

### Option #2

### EPIC

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Tactic</th>
<th>Persistence</th>
<th>Payload Delivery</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
<th>Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Envelope Compromise</td>
<td>Application</td>
<td>bash/itm and Jail v</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Access Token Manipulation</td>
<td>Account Discovery</td>
<td>Application Window</td>
<td>Application Access Token</td>
<td>Authorized Connection</td>
<td>Communication Thru Removable Media</td>
<td>Data Exfiltration</td>
</tr>
</tbody>
</table>

### STORY

**Epics never end!**
Best Practice #1: Issue Tracking at Sub-Technique level!

Epic → Sub-Technique

Story → Detection Rule

Tags → Tactic / Technique

Tracking at sub-technique (aka Procedure – as in TTP)

Relevant tags enables filtering

Multiple teams collaborate to achieve the Security Outcome
Detection as Code: JIRA workflow for Detection Engineering teams

https://medium.com/@ateixei/jira-workflow-for-detection-engineering-teams-a7433f4c2a9f
Detection as Code: JIRA workflow for Detection Engineering teams

https://medium.com/@ateixeijira-workflow-for-detection-engineering-teams-a7433f4c2a9f
Best Practice #2: Managers do like charts...

(Note: This example is used for illustration purposes. It does not represent actual product coverage.)
Best Practice #3: Building Quality from the inside

At Pull Request level
- Tests
  - Unit Test
  - Atomic Red Team Test
  - Re-play Test

At build level
- Atomic Red Team Tests Suite (529 tests)
  - Customized open source and internals
- Unit Tests Suite
- Goodware Suite
- Report generation

At release level
- Smoke test
- Release Communication
Best Practice #4: Continuous Delivery

Cadence is everything

EDR Content Release Flow!
Best Practice #5: Purple Team Exercises to break “silos”

- Adversary Attack Emulation roadmap
  - Internal and external
  - Keep engineering in the loop
  - Which teams should participate?
    - Everyone: Including IT, UI, PM…
Best Practice #6: Training Plan

- SOC rotations
- Customer calls
- SANS courses
- Research
- Defend The Flag!
Key Takeaway

1. Choose tools used in your organization to track your progress.
2. Consider how you can show your progress.
3. Think ways to assure the quality of your detections.
5. Train and look for new sources of knowledge.