


# How to Guide Your Company To Test its POC

---



Lidia Giuliano  
October 17, 2017

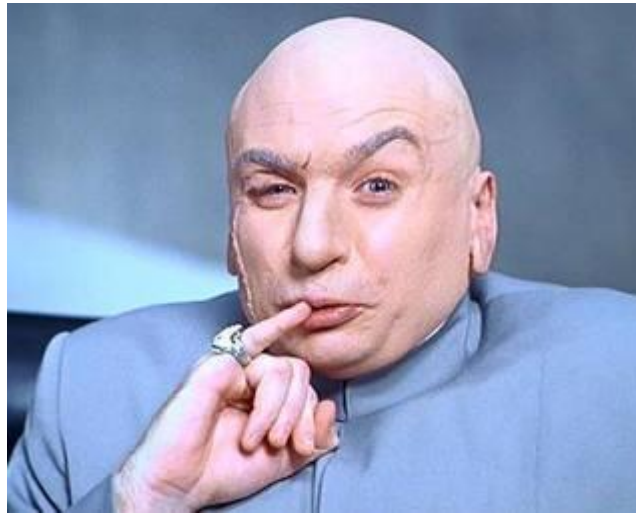
 pink\_tangent

# Understand Business Objectives for the POC

---

## More of the Benefits:

- Reduction of Incidents
- People Costs
- Reputation
- Keep the business running
- Protect PII data



## Less of the Problem:

- Ransomware
- Insider Threat
- Malicious Outsider
- Threat Hunting

## Requirements:

- Functional
- Non-Functional

## Measurements:

- Must's + Should's + Nice to have's
- Weighting + Scoring

# Some non-functions to consider

---

Most people get lost in the functional testing, but these should be considerations in your testing:

- Importance of 2FA support for SaaS solutions
- AD integration
- SIEM integration (in-house or managed service). Are there extra costs involved, storage, people, or vendor monitoring
- APIs available for other systems integration
- Large scale deployment
- Storage of logs, is there an extra cost
- Backwards capability of older systems
- Does it require a reboot

# Preparation of Your Test Environment

---

Recommend to build your own test environment consisting of:

- Victim machine
- Attacker machine
- Malware machine
- Victim machine II which is connected to Victim 1

Considerations for virtual environments:

- Not all VMs will execute malware in the same way
- VirtualBox (for example) compared to KVM, AWS or VMWare will all behave differently
- Consider vendor cloud setups, convenience yes, ability to compare solutions side by side no.

# Testing Variables

---

Recommended inputs / scenarios to consider:

- Test the different layers of the software, and then disable each layers to determine tight-coupling constraints
- Connected agents and non-connected agents
- If your organisation has different user profiles for different roles, consider testing these to check for different results
- When testing malware, as it's the easiest scenario, choose a variety, new, old, grey and don't just mutate them x1, do it a few times different ways
- Test more than binaries try other file types such as .zip, .jar, .com, .vbs, change an ext, rename a file, .ps, false-positive directories

# What to test?

---

Classic Malware Testing (a file exists):

Static Malware Detection / No Process is Running / Dormant

- Importance of background scanning
- File changes (on-write, modify, delete)

Note: Much of the solutions focus on static testing against PEs. Scripts and other file-types are not in-built as yet, unless you are using sandboxing technology

Is this a must or should requirement?

# What to test?

---

Classic Malware Testing (a file exists) cont...:

Dynamic Malware Detection / Process is Running

- Detection and Prevention of those processes being stopped

Note: Older mutated malware caused many headaches, with no real learning.

Memory Resident / File-less Malware (no disk write):

- Detection of Abnormal Actions
- Indicators of Attack –

Mitre ATT&CK [https://attack.mitre.org/wiki/Technique\\_Matrix](https://attack.mitre.org/wiki/Technique_Matrix)

# What to test?

---

Finally, run the solution in your environment for a few weeks:

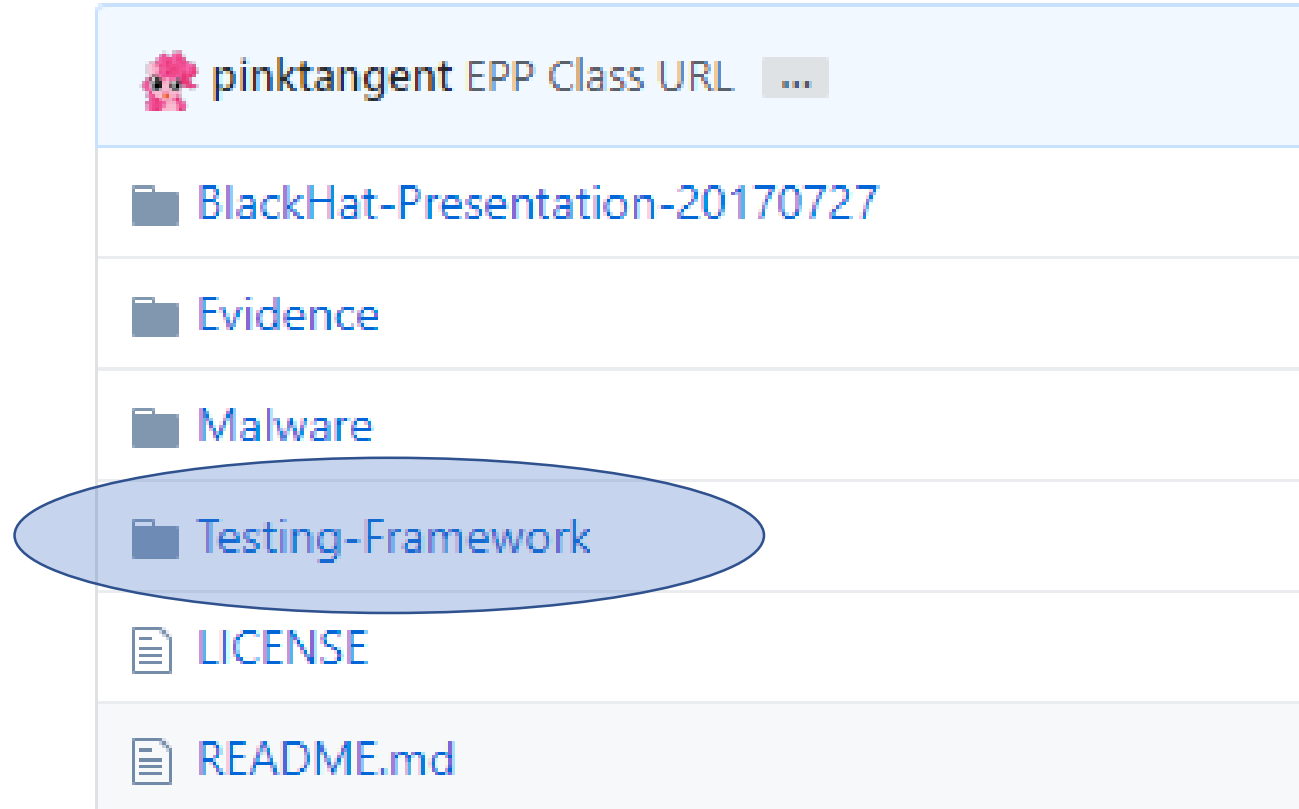
- Don't test malware in this scenario
- Agent sitting in silent mode on a few workstations or systems of importance
- Testing malware is important but how compatible is it with your actual work environment
- How many FPs are being generated and its not because the solution is not good, but perhaps it's the way your company pushes packages, or writes admins script
- If vendors push you to a tight testing timeline, then reconsider



# Testing Guides

---

<https://github.com/pinktangent/Endpoint-Testing>



# Testing Workshop

---

<https://pinktangent.github.io/> - In Progress

## Pink Tangent

twitter: [@pink\\_tangent](#)  
personal blog: [PinkTangent](#)



[View My GitHub Profile](#)

Hosted on GitHub Pages — Theme by [orderedlist](#)

## Welcome

Thanks for visiting. The goal of this site is to share my information security experience with others in the community.

One of the many hot topics of 2017 and will continue into 2018 is Endpoint Protection and how to test the different solutions on the market. If my BlackHat USA talk highlighted anything to me, more organisations and the people that work in the defensive space are challenged knowing where to start. While working for a client on this initiative, I developed in the background a reusable [testing framework](#) that others could use for themselves and their organisation.

In addition to the framework, I wanted to be able to share the process involved, all the different testing scenarios and how-to's. I hope to accomplish this by writing the first online / self-paced Endpoint Protection POC workshop.

- **Endpoint Protection Testing Workshop**

Good luck and enjoy. [Email me](#) with any questions.

# Questions

---

