Leveraging Red for Defense

Presented by:
David Kennedy, Founder and CEO
@HackingDave

BINARY DEFENSE

TrustedSec

DAVE KENNEDY

OSCE, OSCP, CISSP, ISO 27001, GSEC, MCSE

Dave Kennedy is a computer hacker and the founder of TrustedSec and Binary Defense. Dave has helped with the Mr. Robot TV show as well as being directly mentioned on the show and others. Dave also served on the board of directors for the $(ISC)^2$ organization, is the co-author of the best-selling book “Metasploit: The Penetration Testers Guide“, the creator of multiple widely downloaded open-source tools, frequent keynote speaker across the world and on the news, and an avid gamer.

Red Teaming

- Red teaming is a concept of simulations and emulations towards an organization in order to identify weaknesses.
- Involves threat modeling and understanding capabilities.
- Traditionally used as an effectiveness measure of controls and security program.

- This rationality of thought has changed over the years.
- Red is no longer just an effectiveness test, it’s a way to work with blue teams in order to strengthen security programs.
- Ability to simulate adversaries in a way that allows security programs to grow.

Traditional SOC

- Ingestion of log data and difference sources with correlations that are built.
- Possibly some EDR capabilities but limited visibility into the endpoints.
- Controls are largely misunderstood and frequent testing of detection capabilities are not always there.

Prevention takes a long time. Detection can be much faster and results even better.

TrustedSec

BINARY DEFENSE

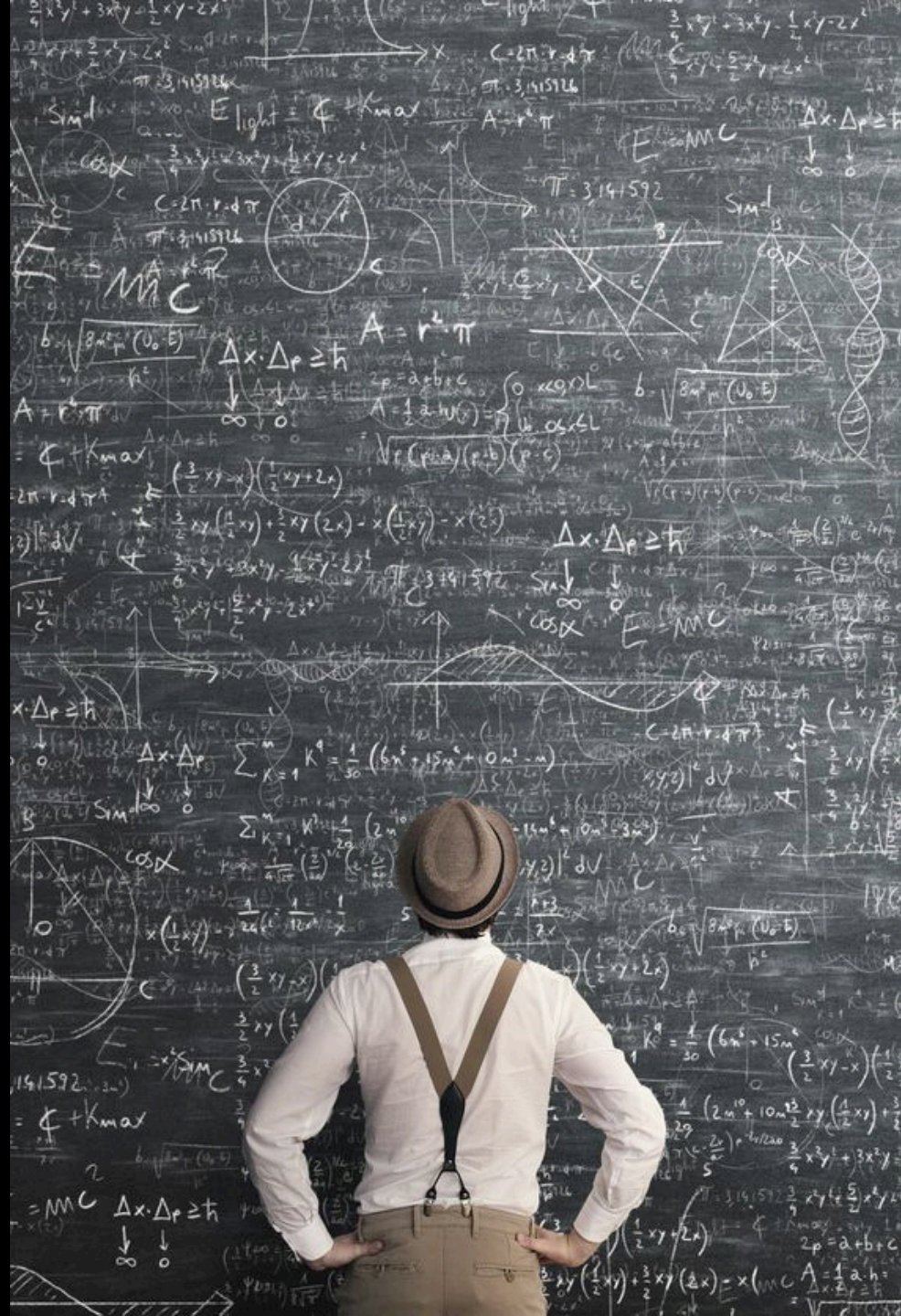
The basics are still a problem.

Some Basics

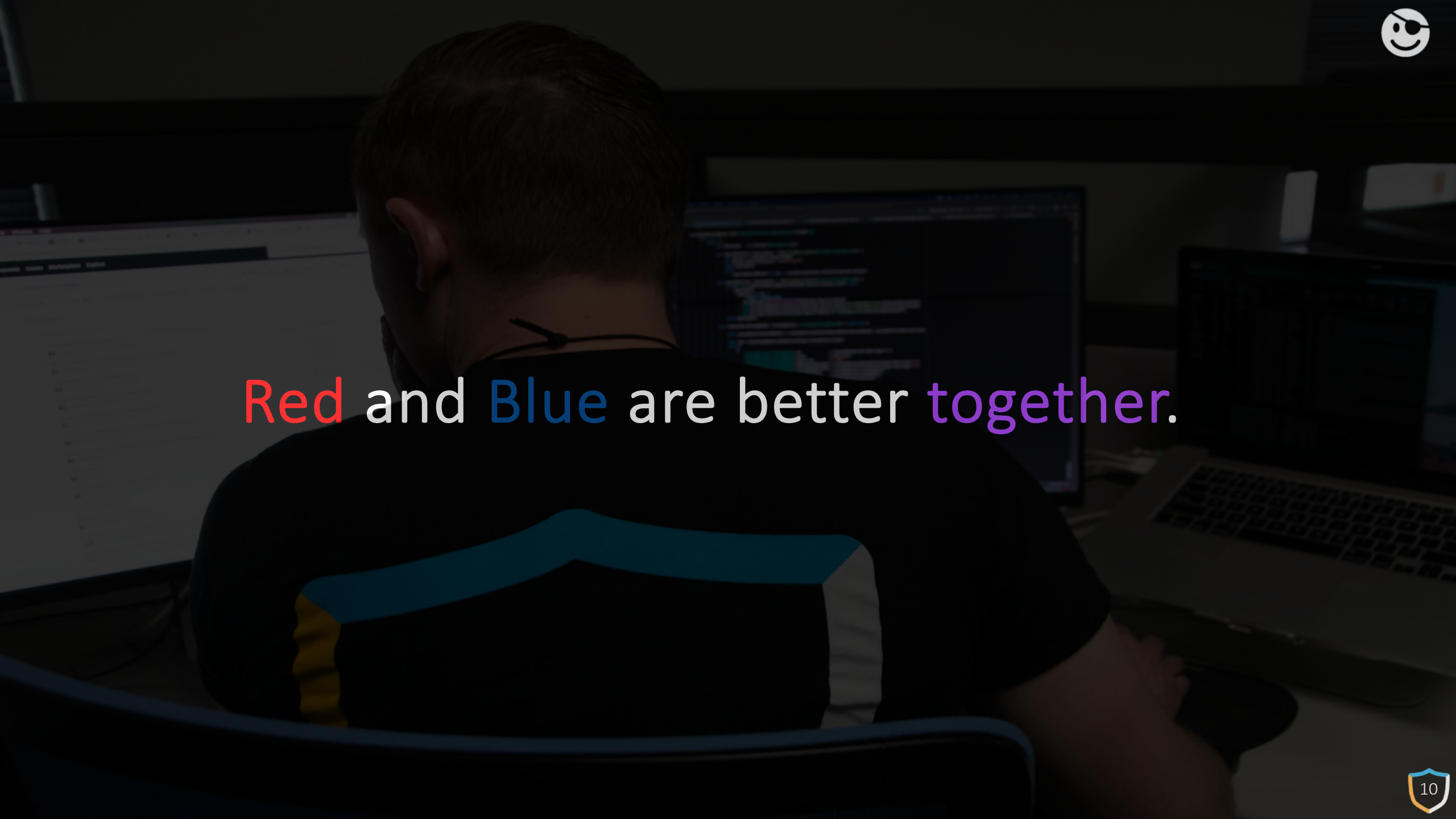
- Prevention takes time however some high value ones:
  - Blocking unsigned executables in user profile directories as a start.
  - Constrained Language Mode.
  - Disallow regular users from PowerShell access.
  - PowerShell v6 and above.
  - Leverage ETW (Sysmon is a great start).
    - https://github.com/olafhartong/sysmon-modular
  - **Please, please, please** enable the Windows firewall internally.
- Detection can move faster:
  - You must, repeat must have endpoint logs.
  - Other sources such as DNS, east/west/north/south, command line auditing, script block logging, and more make a huge difference.
  - Visibility first, then improve on more visibility.
  - Understand the tactics and procedures attackers operate by vs. the techniques.
  - Threat hunting can help reduce the time window of a breach.

Simulations and Emulations

- Tool releases are great for simulations.
- Without simulations, red and blue can’t work together well.
- Working through identifying gaps in programs help put priority on what really matters.
- Usually companies don’t even have the foundation for a building to build on this.



TrustedSec BINARY DEFENSE

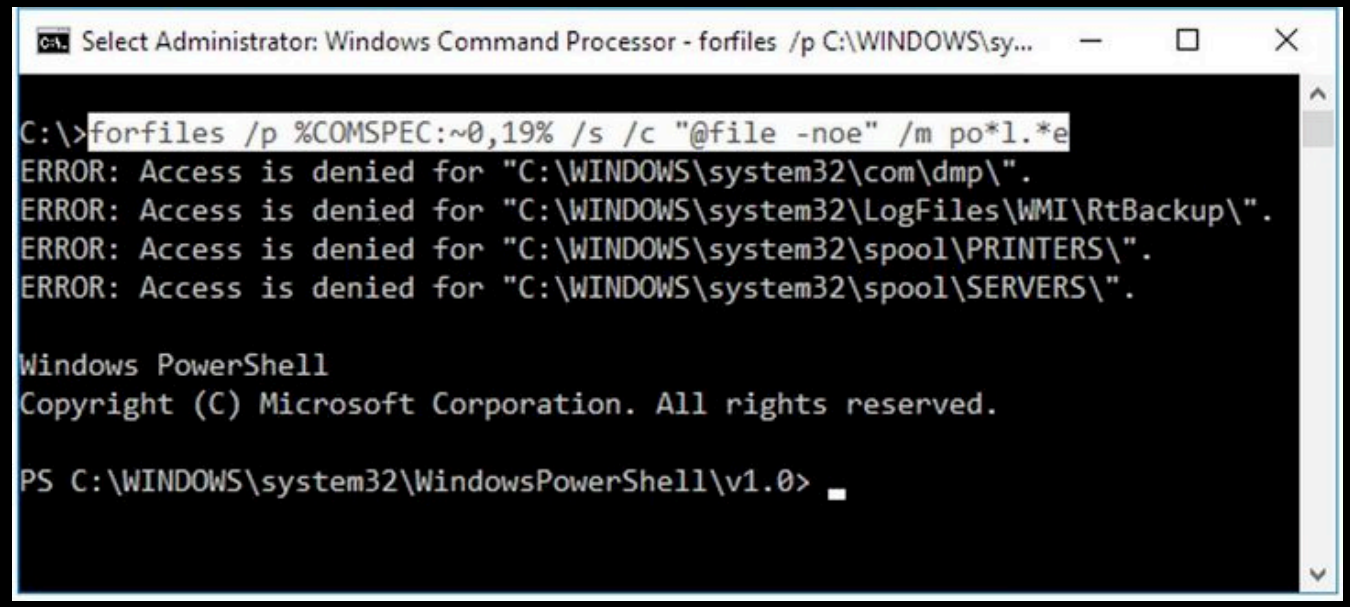

Red and Blue are better together.

The industry changed.

- Red no longer designed to own everything and walk away.
- The red team's customers are the blue team.
- Penetration testing is not Red Teaming.
- A lot of this is legacy thinking of years ago much like the "rock star" mentality which rarely applies today.
- Used to paint an ugly picture due to years of neglect.

Collaboration and Sharing

- More information shared now than ever.
- Still concerned about crowdsourced TTPs.
- Some Red Teams do their own research and customize tooling to compete.
- Red teaming has gotten harder.
- Research is a good thing.
- Releasing tools is a good thing.



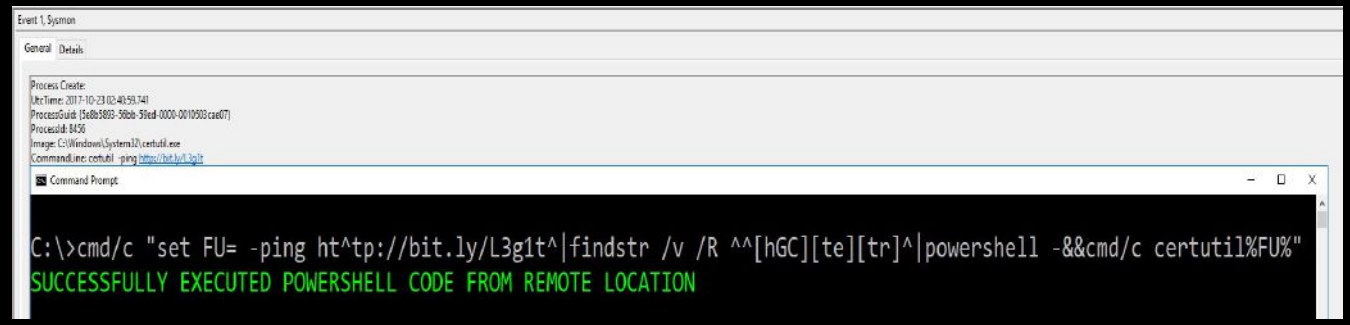


Image Sources: Daniel Bohannon @danielhbohannon (<3)

Sharing Knowledge Between Groups

- Threat Hunting
  - Intelligence capabilities and unusual behavior.
- Red Teaming
  - Understanding capabilities of attackers and applying threat models and simulations.
- Security Operations Center
  - More than just alarm generation and responding to false positives.
- Blue Team
  - Working with a number of different teams to coordinate detection, response, or prevention.
  - While may not understand offensive capabilities, when given access to offense, substantially increases security of organization.
  - Vulnerability management probably these most important security program in an organization. (CMDB anyone?)

Focus on Behavior

- We are focused on techniques, not tactics or procedures.
- Behavior creates too many false positives.
- Allocating appropriate resources for detection becomes challenging.

Visibility is Critical

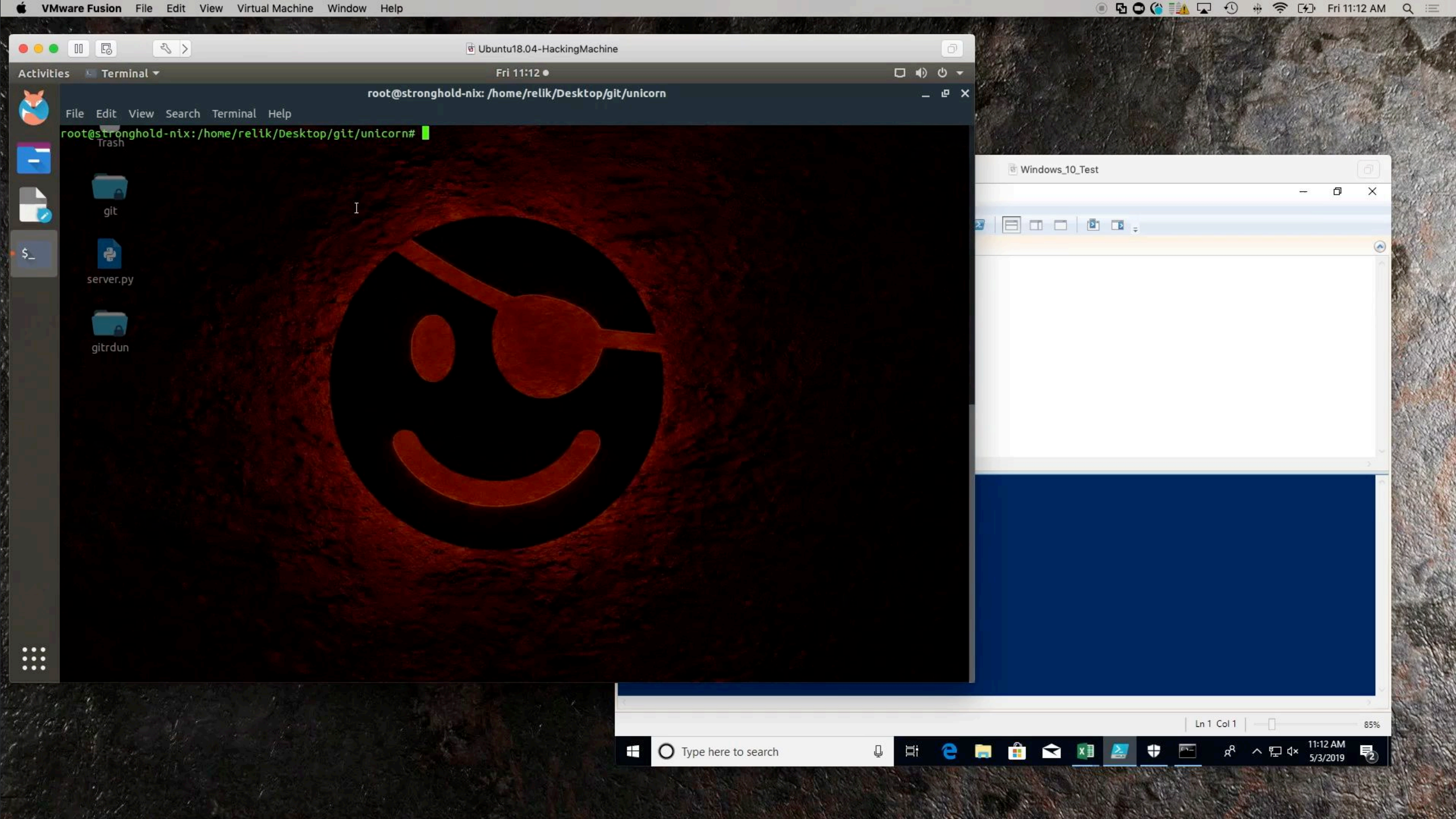
- Protection takes time.
- Detection vs. Protection
- Visibility is first step and the most important one.
- This has to include endpoint logs.

If an attacker customizes, they largely go undetected.

Customized Stuff

- Take a technique and modify it in anyway and you can usually circumvent all detection criteria for an organization.
- Build your own, you are sure to evade detection substantially longer than ever before.
- Leverage a technique through your own research almost ensures little to no detection.

DEMONSTRATION


VMware Fusion File Edit View Virtual Machine Window Help
Fri 11:12 AM
Ubuntu18.04-HackingMachine
Activities
Terminal
Fri 11:12
root@stronghold-nix: /home/relik/Desktop/git/unicorn
File Edit View Search Terminal Help
root@stronghold-nix:/home/relik/Desktop/git/unicorn#
Trash
git
server.py
gitrdun
Windows_10_Test
Ln 1 Col 1
85%
Type here to search
11:12 AM
5/3/2019


Closing Remarks
TrustedSec
BINARY DEFENSE

Thank you all!

Presented by:
David Kennedy, Founder and CEO
@HackingDave

BINARY DEFENSE

TRUSTEDSEC