Blue Team 101: Building Defensible Systems

A series of short poems

by Daniel Griggs of cmdSecurity


dan — Hogwarts
Last login: Sat Apr 23 14:18:05 on ttys000
dan@Hogwarts: ~
$ whoami
• Daniel Griggs, CEO and founding partner: cmdSecurity
• Worked for the US DoD and other government agencies on security for Apple devices
• Specializing in security and management at scale for more than 10 years
• Currently working on multiple security standards

Security and management should
NEVER destroy the user's experience

Continuous Diagnostics and Mitigation (CDM)

How to win friends & influence people

General Problems

- Security is complex
- Users are focused on ease of use
- Threats and vulnerabilities change daily
- Compromise is nearly inevitable

Goals of security

- Know when something bad happens
- Facilitate easy workflows that are secure
- Train users to recognize security incidents
- Protect the data on the device

Attack Lifecycle

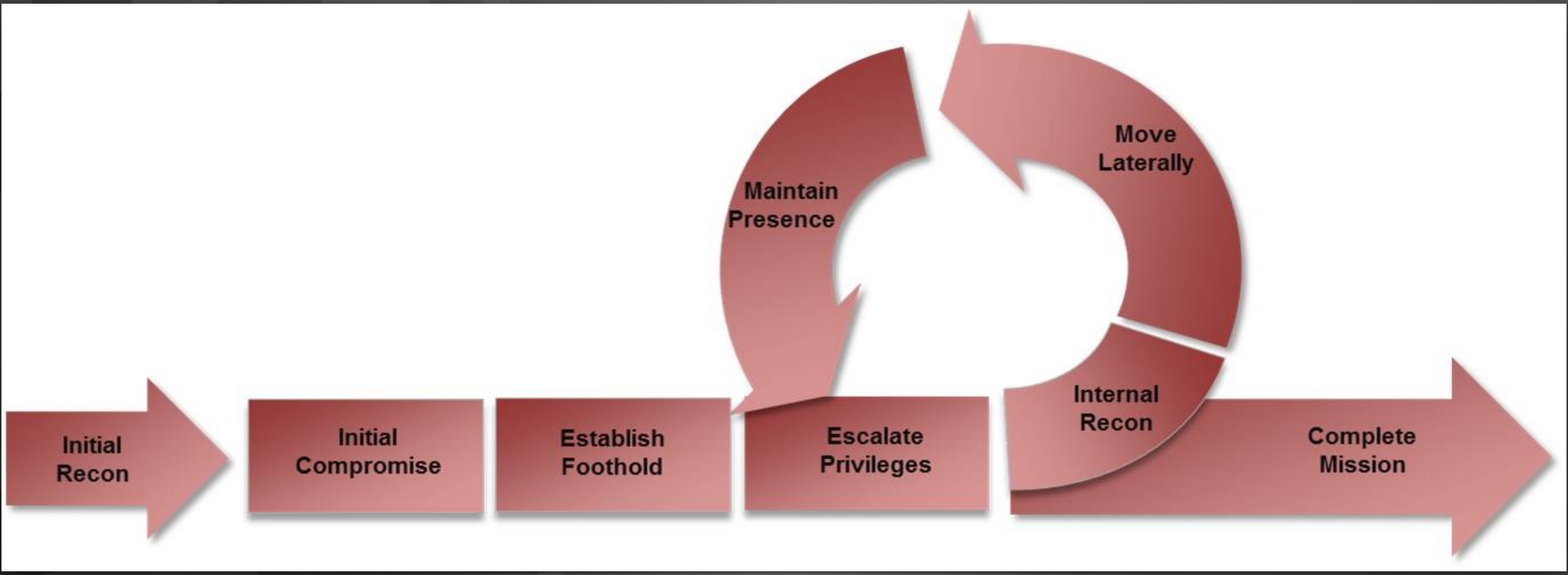


Image Source: Mandiant Consulting, see https://www.fireeye.com/services.html

Definitions

- **Vulnerability:** A mistake in software that can be directly used by a hacker to gain access to a system or network
- **CVE:** Common Vulnerabilities and Exposures
  - Gives a common serial number to publicly known cybersecurity vulnerabilities
  - https://nvd.nist.gov/

Definitions

Vulnerability -> Exploit -> Malware/Virus

- **Exploit:** A sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software
- **HOW** an attacker uses a vulnerability to gain access to a computer

Definitions

Vulnerability -> Exploit -> Malware/Virus

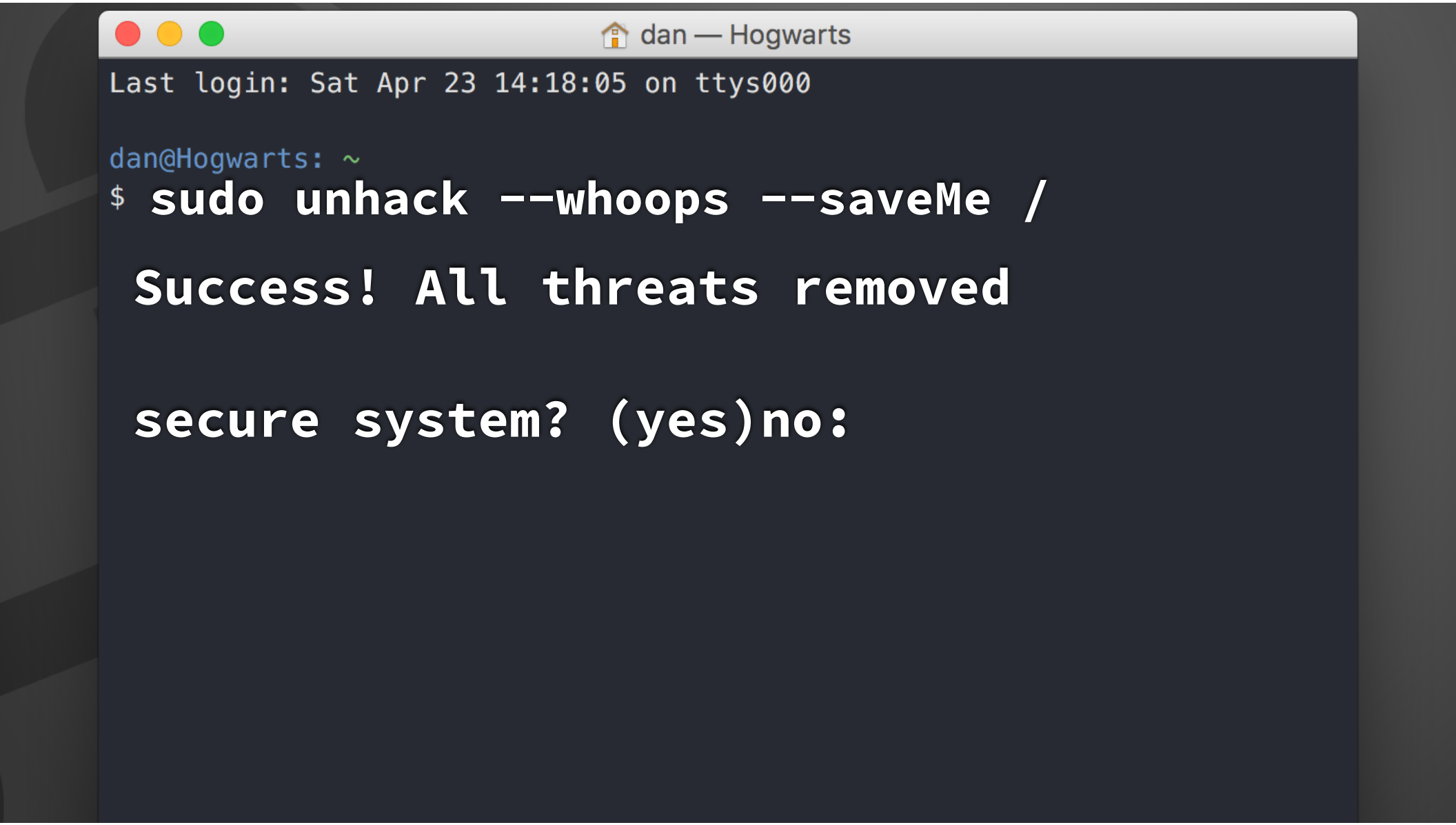
- **Malware/Virus:** A malicious program that, when installed, performs some form of harmful activity. These activities can be
  - Data corruption or exfiltration
  - Movement to other, more important systems
  - Denial of service(s)
- **WHAT** an attacker is using vulnerabilities and exploits to place on your computer

Macs are immune though, right?

CVE(s) in the past 3 Months

- Mac CVE: 283
- Windows CVE: 261
- Linux CVE: 183

https://nvd.nist.gov


dan — Hogwarts
Last login: Sat Apr 23 14:18:05 on ttys000
dan@Hogwarts: ~
$ sudo unhack --whoops --saveMe /
Success! All threats removed
secure system? (yes)no:

Basics of security practice

- No MDM == NOT secure
- Security is iterative, there is no ‘done’ state
- Focus on the endpoint
- Most of the problems in security have already been solved by teams of experts

Security Guidelines

- CIS Guidelines
- NIST Special Publications
  - SP 800-137 Continuous monitoring
  - SP 800-128 Security focused config management
  - SP 800-171 Protecting sensitive information
- USGCB
- STIG(s)

What NOT to do

Turn on every available security restriction

What NOT to do

“I am just trying to stay off the front page of the Washington Post”

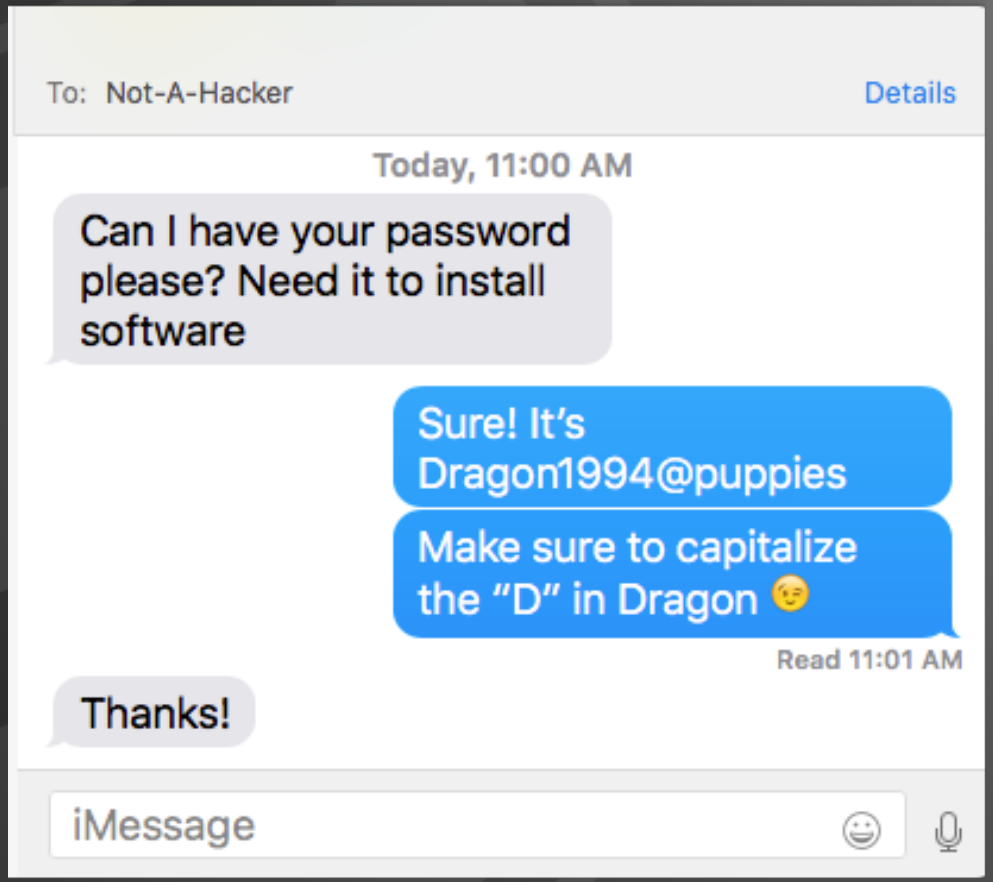
What NOT to do

Relying on “do everything” security devices or software

What NOT to do

Blame the users

Phishing



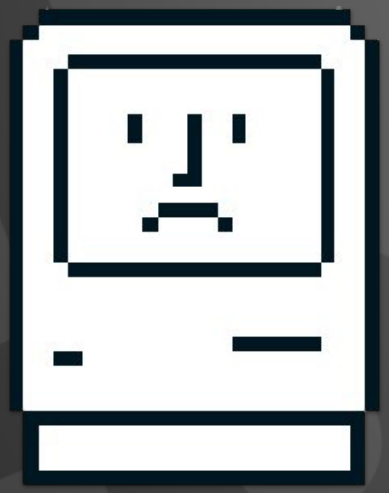
- All hope is lost
- This is the most common and most successful attack

The Good News

Company money is best spent training **YOU**

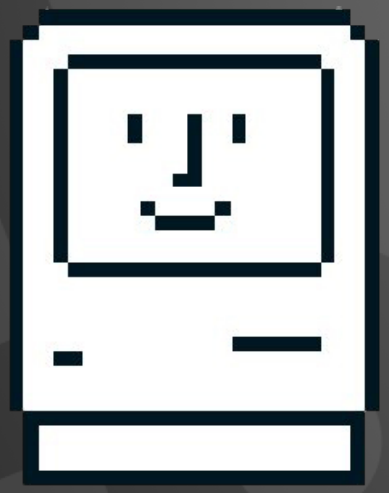
Any environment can be secured

What bad security looks like



- Machines are barely operational because of all the restrictions on them
- No record of software, services, or open ports
- Inconsistent configurations
- Users finding less-secure ways to do work

What a properly secured device looks like



- Attackers face obstacles at every stage of the attack
- Most of the system is open for the user to do work
- Computers continuously and completely inventoried
- Scan for known vulnerabilities

How to Get there

- Design to find results of malicious actions
- Standardize across your organization where possible
- Collect as much meaningful signal about your devices as possible

Design for change

- Modular IT Stack
- Clear assignment of IT duties
- Training systems for non-IT employees
- Clear incident response duties and timelines

Log Aggregation

- Splunk, Logstash, GrayLog, loggly, etc…
- **ENSURE** that all of your log transmissions are encrypted
- Get as much data off-device and searchable

Risk

Risk = Likelihood * Impact

What are you worried about happening

How likely is it to happens

What constitutes a breach

- Illegitimate computer access of any kind
- Any situation where protected data has **POTENTIALLY** been viewed by unauthorized personnel

Baselines “Known Good”

- What is normal behavior for a machine
- What are the expected settings for critical services
- How you detect when something changes
- How to determine if that change is bad

Change Detection

- Attention to detail
- Alert on deviation from baselines
- Start tuning out false positives slowly

Putting It All Together

Anatomy of a Security Decision

Define What To Protect

Stop users from running low-level systems configuration commands

Lock Down Access

Only allow designated management users to ‘sudo’

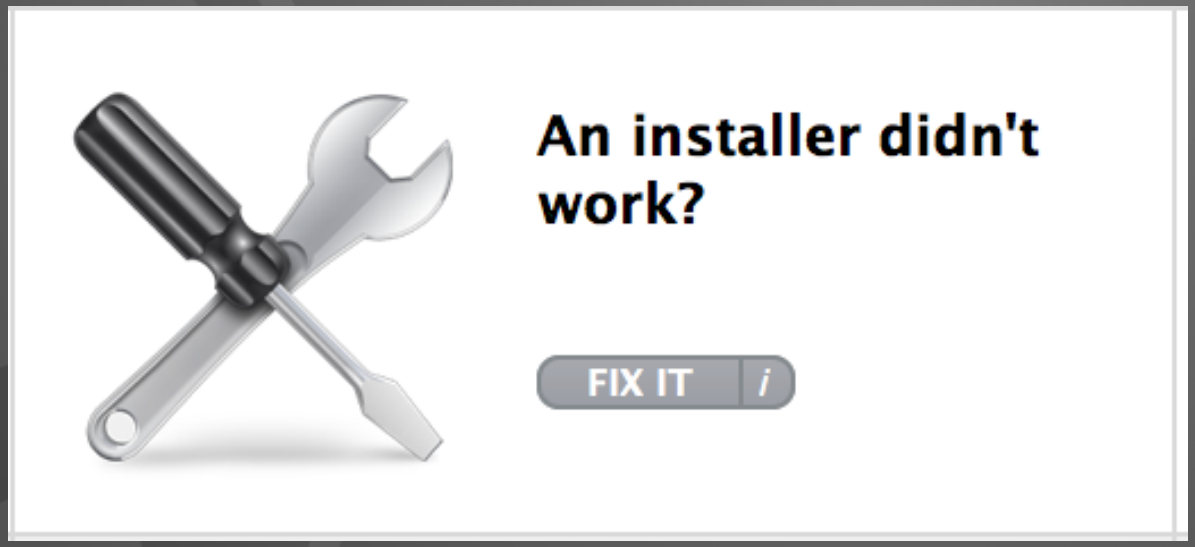
Apply Moderate Security

Users are still able to be admins and install software

Monitor Everything

Know when malicious activity is happening by attempted ‘sudo’-ing

User Support



Passwords and Complexity: A Holy War

- XKCD “correct horse battery staple”
- entropy vs cracking machines vs attack models
- Perfect world vs Real world
- Scope of use
- Rotation frequency (90 days vs Almost Never)

Config Profiles vs Scripts

Profiles

Always configured, never change

(Password Policy)

Scripts

Controls that have some flexibility

(File Shares)

Antivirus: Friend or Foe?

What Would Apple Do? (WWAD)

Free Tool: RansomWhere?

https://objective-see.com

- Detects when an non-apple process starts encrypting lots of files
- Has its limitations, but overall very good tool

Free Tool: osQuery

https://osquery.io/

```
osquery> SELECT uid, name FROM listening_ports l, processes p WHERE
l.pid=p.pid;
```

osquery gives you the ability to query and log things like running processes, logged in users, password changes, usb devices, firewall exceptions, listening ports, and more.
You can perform ad-hoc queries or schedule them. More details can be found here

Enterprise Ready

CentOS, Ubuntu LTS and OSX are supported with no dependencies. osquery powers some of the most demanding companies, including Facebook.

Differential Changes

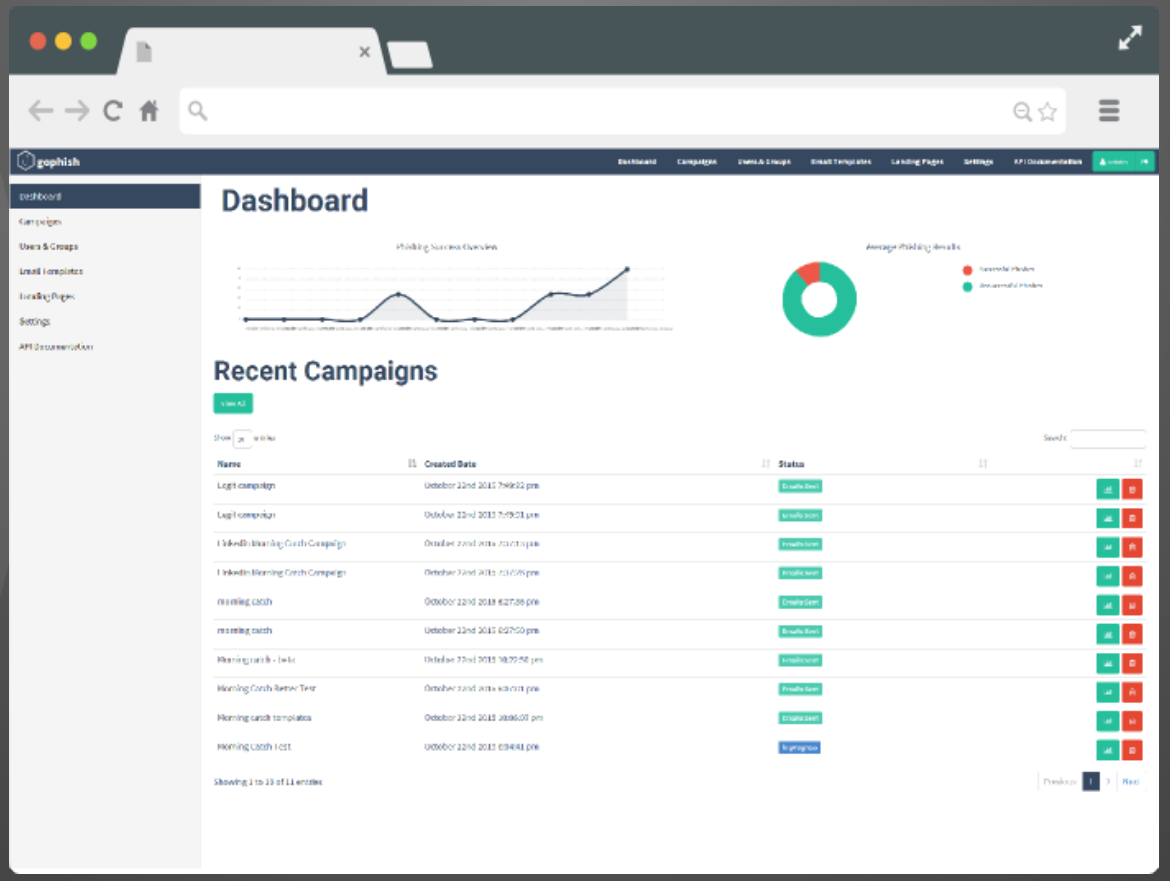
Know when critical objects are added, modified or deleted from a system.

Feature Velocity

You control the roadmap. Developed in the open, by the community, for the community.

Free Tool: Simple Phishing Toolkit

https://github.com/gophish/gophish



Where to learn more

- SANS.org
- CEH, CISSP, CompTIA certs
- Read the security publications
    - NIST SP 800-XXX, USGCB, CIS
- Apple Security talk tomorrow 9am