Bootstrapped SecOps

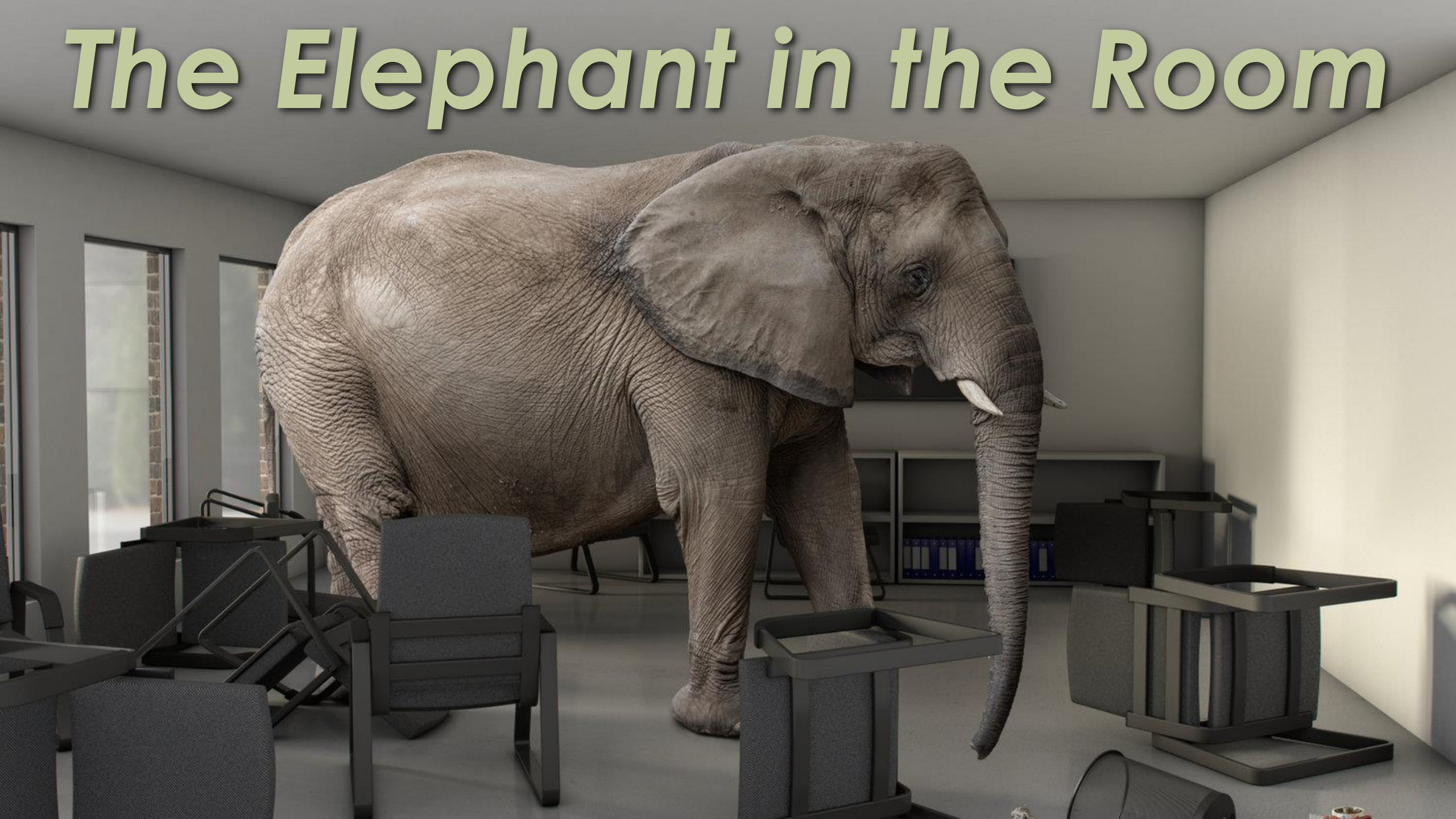
Practical Strategies for Starting with Minimal Resources

```
PS > Get-User | Select Name, Alias, Location, *Company, Role

Name                                : Hudson Bush
Alias                               : @HomeBrewedSec
Location                            : Chattanooga, TN
Company                             : Dragos
Role                                : Principal Security Engineer
SpeakingOnBehalfOfCompany           : FALSE

Name                                : Luigi Esposito
Location                            : Chicago, IL
Company                             : Dragos
Role                                : Principal Security Engineer
SpeakingOnBehalfOfCompany           : FALSE
```

Why Bootstrapped SecOps

- Most of us don’t work at Fortune 50s with unlimited resources
- “Living Below the Security Poverty Line” - @wendynather
- You don’t need to spend $$$$ to have a solid security program that stops real world attackers

The Elephant in the Room



Blog Post

Deconstructing a Cybersecurity Event

By Dragos, Inc. 05.10.23

On May 8, 2023, a known cybercriminal group attempted and failed at an extortion scheme against Dragos. No Dragos systems were breached, including anything related to the Dragos Platform.

The Elephant in the Room

- We’re a transparent company, so there’s not much more to say than was already said in the blog
- Give your incident responders a hug
- If you haven’t tested your IR plan, you don’t have one
- RBAC, RBAC, RBAC!!!

Phases

Phase 1 *Planning and Discovery*

Phase 2 *Analysis and Documentation*

Phase 3 *Mitigation and Remediation*

Phase 4 *Looking Forward*

Phase 1

Planning and Discovery

So you've started the Impossible

- Attitude is important – Friendly, Humble, Helpful, Optimistic
- Friends and allies are important – Don't make things harder for yourself
- Buy-in is important – Show the importance of what you are doing, and don't make people's jobs any harder than you have to.
- Project Competence and Professionalism (but not arrogance) – People want to trust you and your judgement

You Have to Start Somewhere

- **Track Your Work!**
  - Every week make sure you keep track of what you did, and what wins you had, if only to encourage yourself
- **Pick a Framework**
  - NIST CSF
  - ISO 27001 ($)
  - CMMC ($$$)
- **Become the expert in your environment**
  - Know what's normal
  - Understand business objectives
  - Figure out what can be simplified, standardized

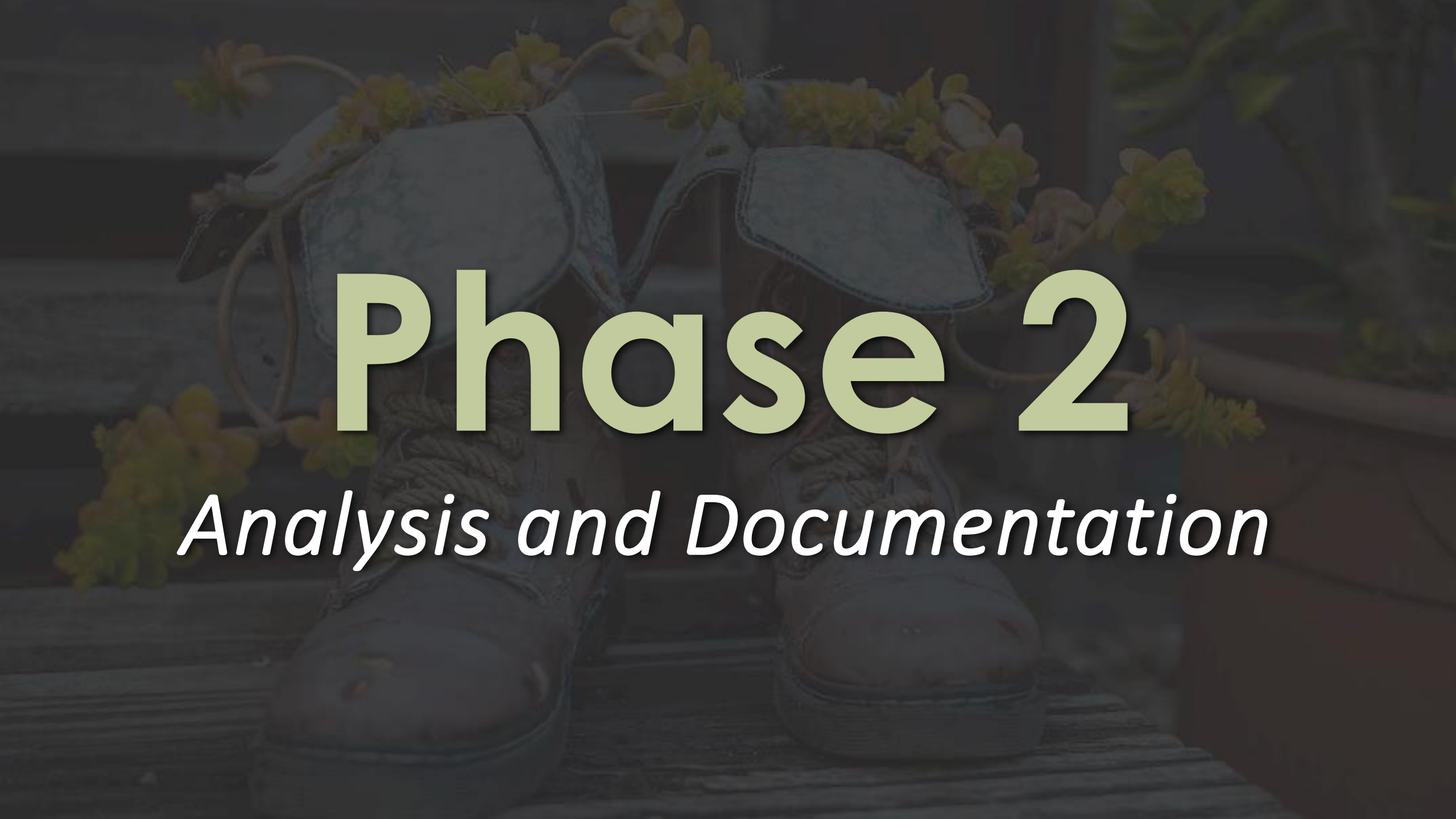
Threat Modelling

- **Know what you're protecting and know what you're protecting against**

- **Risk Assessment + Business Impact Assessment**
  - **Estimate what happens to the business** if X happens, and the likelihood of X happening

  - **Defender's Dilemma** *(old and busted):* An attacker only needs to exploit one weakness, a defender needs to protect all weaknesses

  - **Attacker's Dilemma** *(new hotness):* A defender needs to make it too expensive for an attacker to exploit a target given the value of that target



Phase 2

Analysis and Documentation


Should I Buy All The Things Now?


Should I Buy All These Things Now?
NO

Jake Williams
@MalwareJake

It floors me when (for instance), someone in a one-person security shop says to a group of infosec professionals "I want a SIEM and SOAR solution. What's the best in the business?"

And instead of saying "you aren't ready for that" they proceed to suggest million $$ solutions.

8:02 AM · May 17, 2023 · **83.1K** Views

Stop the Obvious Bleeding

- Role-based Access Control (RBAC)
- Secure your edge (ie. Don’t have port 22 or 3389 open to the internet)
- MFA
- Canaries
- Stale account cleanup
- Critical Vulnerabilities, Unsupported Software

Incident Response Planning

- If you haven't tested your IR plan, you don't have one
- Policies/procedures
  - Include timelines and regulatory requirements for breach reporting
- Create playbooks tailored to your team and tools
  - Scottish CERT playbooks are a great starting place
- Have a central place to track and document your response
  - TheHive is a free incident management system if you don't have an enterprise tool

Asset Management

- If you don’t know what you have, you don’t know what to secure
- Asset Management informs every other control you have
- Not just physical assets, includes:
  - Virtual machines
  - Software inventory
  - IP Address Management
  - Data inventory
  - Services Account Information and Renewals

Vulnerability Assessment

- Implement prior to patching to show reduction in vulns from patching
- Find a Vuln scoring (Critical / High / Med / etc) that works for your environment
- Generate differential reports that can track progress over time

- Open VAS is free / Shodan can scan external ports/vulns

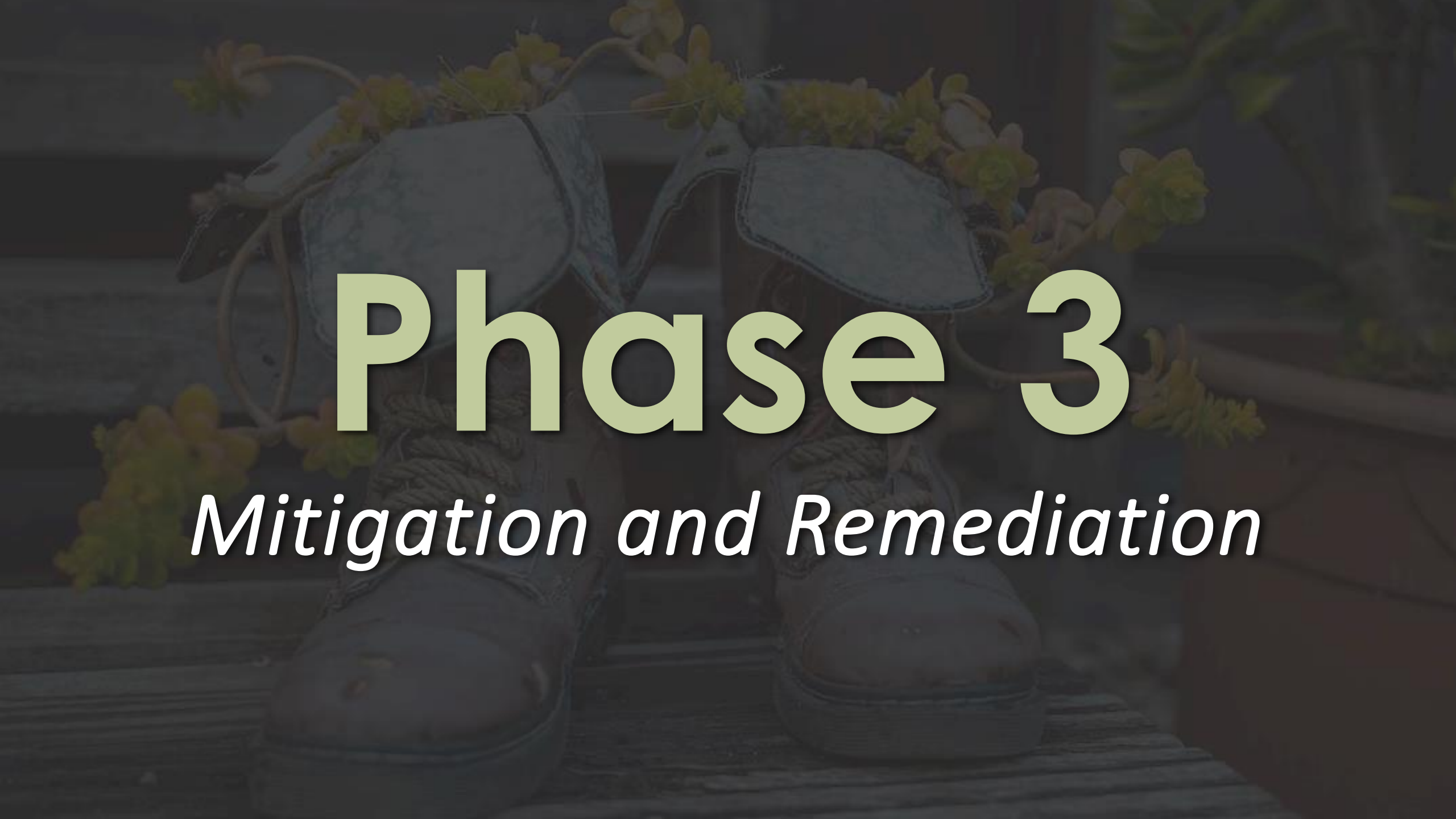
Patching

- Automated wherever possible (with exceptions as needed)
- You (probably) don’t have a team large enough for patch testing
- WSUS can be high-maintenance if you don’t have experience
- Every MSSP will have a patching software

- **Offload this to IT wherever possible**

Change Management

- Not necessarily your job…but it will be if it doesn't happen
- Even track changes that you don't think require approvals, these can be documented as "standard" changes
- Don't need a fancy tool, do it in your helpdesk software, or in Excel



Phase 3

Mitigation and Remediation

Key Purchases

- Firewalls
  - (No, Cisco or SonicWall doesn’t cut it in 2023)
  - Log it!
- EDR
- A proper Identity Provider
- WAPs that support WPA3

Backup

- Ensure each backup has an immutable (ie. Offline/out of band) copy
- This is another thing that is not necessarily your job, but will be if it doesn’t happen
- Like an IR plan, if you haven’t tested your backups, you don’t have backups
- Scale your backups to your needs based on RTO/RPO/MTTR

Least Privilege

- RBAC is not a sexy control, but it limits the success of real-world attacks
- Don’t need a fancy EPM, you can use ProcMon for removing Local Admin on Windows
  - LAPS on Windows
  - Privileges for Mac
- Reduction of privileged accounts

Detect

- Consider an MSSP/MDR if you don’t have the expertise or resources to manage a SIEM
- Only ingest what you need, what is actionable. If it isn’t actionable, stop ingesting it (log all the IMPORTANT things)
- Case study: Using firewall logs to do low-budget micro segmentation

Phase 4

Looking Forward

Show What You've Done

- Imagine you have no idea what security does or is good for
- Imagine you have no idea what all the money you spent on security does
- Imagine you have no idea what risks are important to the company
- You've just imagined your management. **Help them out!**

Metrics

Here's what we've found important to report. Make yours cooler.

Future Planning

- Fun things to consider for next year (as budget permits, and maturity allows)
  - SIEM
  - SOAR
  - Pentest
  - WAF
  - PAM

Resources

IR Plans and Playbooks

- https://www.gov.scot/publications/cyber-resilience-incident-management/

User Education

- https://staysafeonline.org/resources
- User Awareness Maturity Model - https://www.sans.org/security-awareness-training/resources/maturity-model/

Vulnerability Management

- Perimeter - https://shodan.io
- Vulnerability Scanner https://www.greenbone.net

Frameworks

- NIST CSF https://www.nist.gov/cyberframework
- CMMC https://dodcio.defense.gov/CMMC/Model/
- ISO 27001 https://www.iso.org/standard/27001

Resources (cont.)

Endpoint Security

- Windows App Control https://github.com/microsoft/AaronLocker
- Mac App Control https://github.com/google/santa
- Sysmon Config https://github.com/SwiftOnSecurity/sysmon-config
- Privilege Management for Mac https://github.com/SAP/macOS-enterprise-privileges

Red Team Simulation

- https://github.com/redcanaryco/atomic-red-team

Security Policies

- https://www.sans.org/information-security-policy/

Security Case Management

- https://www.strangebee.com/thehive

Tl;dl (too long; didn't listen)

- Have a good attitude
- Set priorities based upon business objectives
- Threat model all the things
- Discover all the things
- Document all the things
- Backup all the things
- (Don't necessarily) open source all the things
- Buy all the things … eventually
- Help management understand what you do

Bootstrapped SecOps

Practical Strategies for Starting with Minimal Resources

Questions

Twitter: @HomeBrewedSec

Slides

HomeBrewedSec.com/Talks