Let’s talk compliance

KRAMEFF SOLUTIONS LIMITED

MindPoint GROUP℠

About

- Mark Bolwell
  - Principal automation engineer on open-source project Ansible-lockdown
  - Krameff Solutions Limited - UK Consulting Company
    - In partnership with MindPoint Group Cyber security specialists
  - 25+ yrs nix admin
    - Passionate about automation and standards
  - Ansible since 2014
    - Responsible for its adoption worldwide in global MSP
    - Presented San Francisco, Austin and London
    - Customer advisory board London and San Francisco


uk-bolly

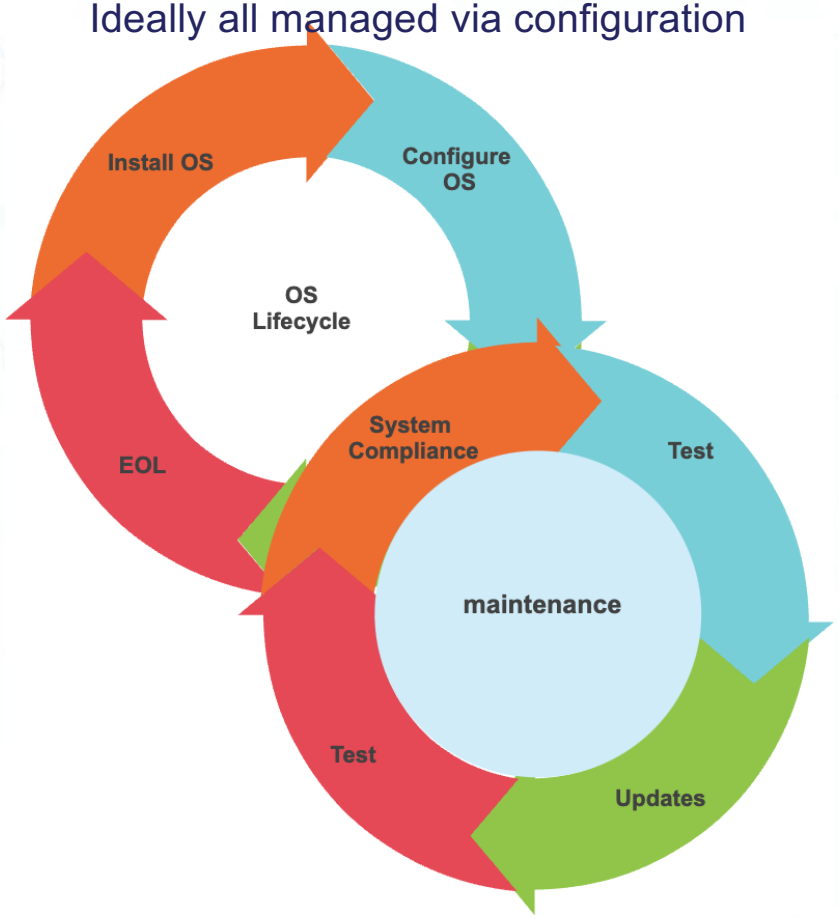

Mark-Bolwell

KRAMEFF

MindPoint GROUP

OS Lifecycle example

Ideally all managed via configuration



What is Ansible-lockdown?

- Open-Source security and compliance automation
  - Written as ansible roles
  - assists with e.g. PCI-DSS, DORA, NIS2
  - Incorporates audit capability
- Best practice and industry recognized security baselines for

CIS Center for Internet Security

DISA

Linux

Redhat, Rocky, Alma, Oracle 7,8,9
Ubuntu18, 20, 22, 24,
Debian11,12

Windows

10,11,2012,2016,2022

Other

Cisco networking
Windows firewalls
Apache
Postgres

KRAMEFF

MindPoint GROUP

Overview

- Assertions are run
- Almost everything then is optional
- Audit the system
  - Options can set the system for you
  - Can copy/installed/download dependent on requirements
  - Runs controls based on settings as per ansible
- Remediate
  - Runs ansible steps to bring system into compliance
  - Each item is selectable
- Run a post audit after changes have occurred

Inventory

```
demo:
    hosts:
      rocky9_bios:
        ansible_host: 192.168.1.208
        skip_reboot: true
        rhel9cis_allow_authselect_updates: true
        rhel9cis_authselect_custom_profile_name: mpg-cis
      alma9_efi:
        ansible_host: 192.168.1.213
        rhel9cis_allow_authselect_updates: true
        rhel9cis_authselect_custom_profile_name: mpg-cis
      rhel9_bios:
        ansible_host: 192.168.1.214
        rhel9cis_allow_authselect_updates: true
        rhel9cis_authselect_custom_profile_name: mpg-cis
```

```
vars:
    setup_audit: true
    run_audit: true
    audit_content: git
    skip_reboot: false
    sudoers_exclude_nopasswd_list:
      - ec2-user
      - rocky
      - vagrant
    rhel9cis_sudoers_exclude_nopasswd_list: "{{ sudoers_exclude_nopasswd_list }}"
    rhel9cis_rule_5_2_4: false # skip user password
    rhel9cis_rule_5_4_2_4: false # v2 skip root password
    rhel9cis_bootloader_password_hash: grub.pbkdf2.sha512…….
    allow_auditd_uid_user_exclusions: true
    rhel9cis_auditd_uid_exclude:
      - vagrant
```

KRAMEFF

MindPoint GROUP

Just get on with it!!

- Demo time

Why use another product to audit?

- Open-source single go binary – goss – www.goss.rocks
  - Go server-spec
- About 14MB in size
- Self contained binary
  - Doesn't require any further modules or dependencies
  - Great for air gapped environments
  - Runs on the host not across network(caution on shared infra)
- FAST!!!!! 700 tests < 2mins (clean OS build)
- Driven by a Yaml based configuration file
- Using ansible settings with Jinja2 to drive configuration for goss checks

KRAMEFF

MindPoint GROUP

Links

- Products
  - https://github.com/ansible-lockdown
  - https://goss.rocks/
- Support
  - Community - Discord
    - https://www.lockdownenterprise.com/discord – invite link
  - https://lockdownenterprise.com – Ask me for more
- Videos
  - https://www.youtube.com/watch?v=sbIfaNsoszM
- Vendors
  - https://mindpointgroup.com
  - https://krameff.co.uk
    - info@krameff.com

KRAMEFF

MindPoint GROUP

KRAMEFF
SOLUTIONS LIMITED

MindPoint
GROUP℠