ANSIBLE

SECURITY AUTOMATION WITH ANSIBLE

Faz Sadeghi
Specialist Solution Architect

redhat.

WHY SECURITY AUTOMATION

ANSIBLE

INFO SEC AREAS

Application Security

Network Security

Forensics

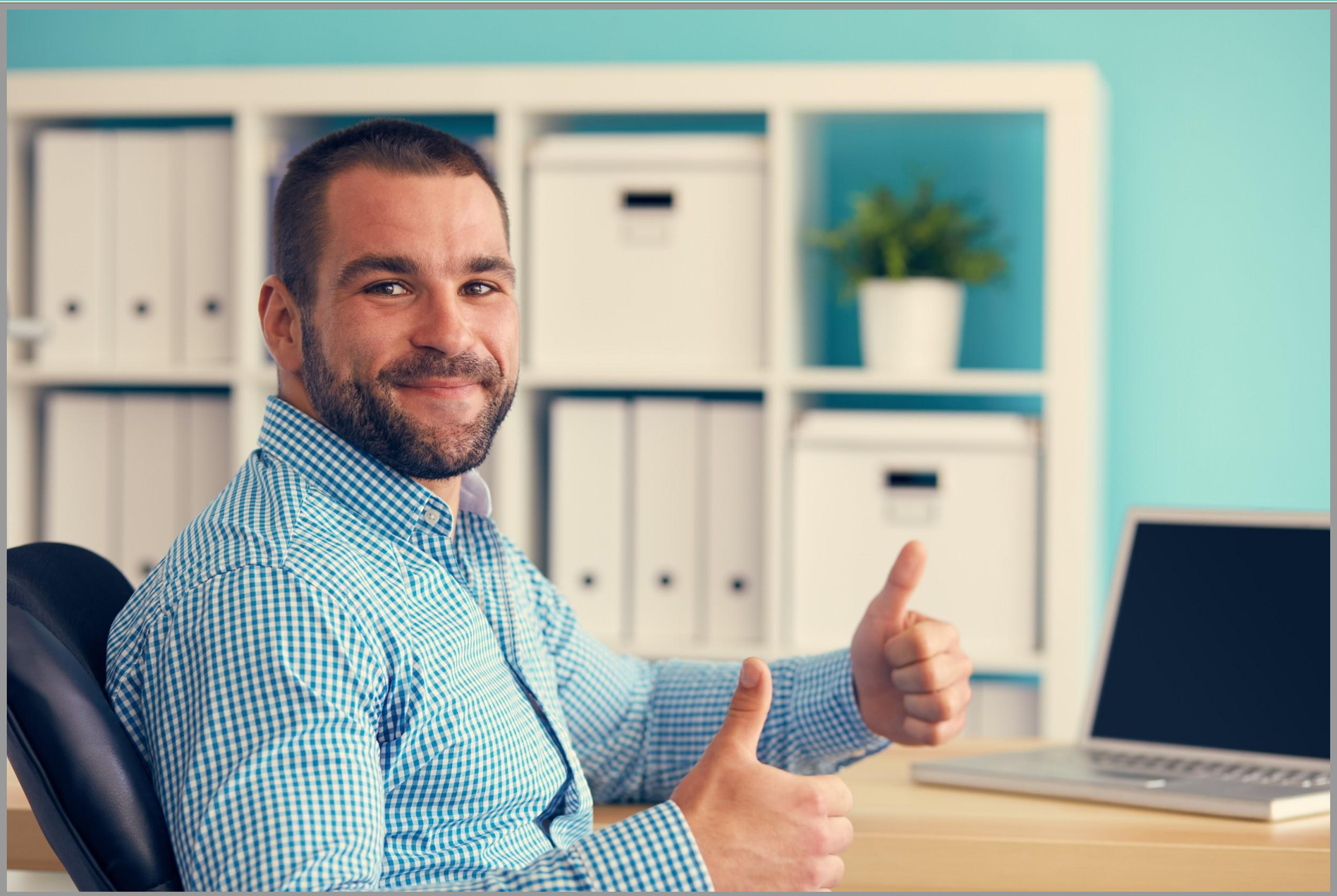
Incident Response

Penetration Testing

Fraud Detection and Prevention

Governance, Risk, Compliance

STORY OF MARKO



SEC OPS SILOS

ANSIBLE

WALL OF SEPARATION

SECurity

Wants to ensure Information Assurance

OPerationS

Wants to ensure System Availability

https://www.niceideas.ch/roller2/badtrash/entry/devops-explained

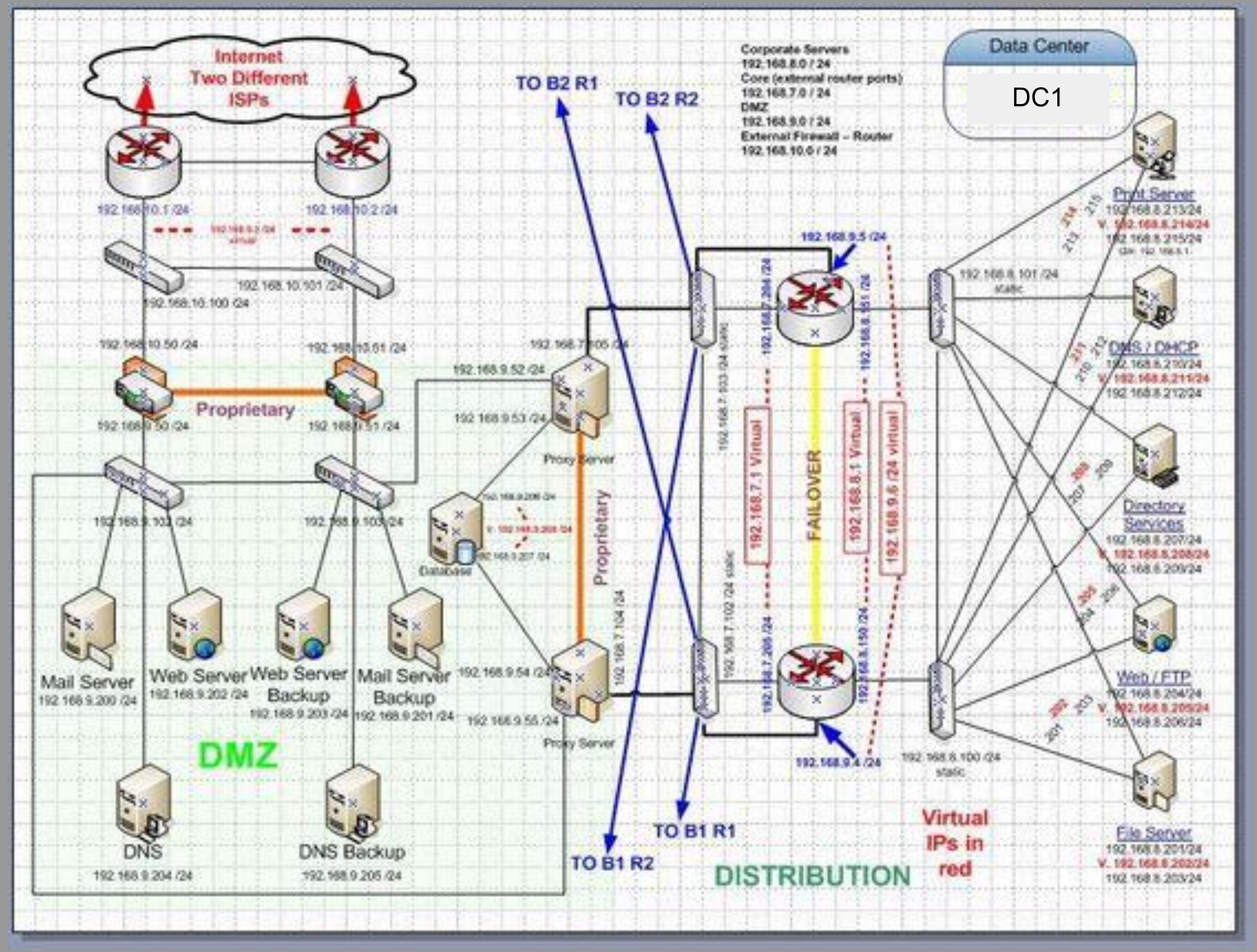
redhat.

RUNBOOK ITEMS

Rule Title: The SSH daemon must not allow authentication using an empty password Linux servers .
Rule Title: Anonymous enumeration of shares must be restricted on Windows servers.
Rule Title: The network element must only allow management connections for administrative access from hosts residing in to the management network.
Rule Title: Change root password on all servers, according to policy every 60 days.
Rule Title: Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release.
Rule Title: Protect against CVE-2016-5696.
Rule Title: Fix and test shellshock.

PLANNING THE IMPLEMENTATION

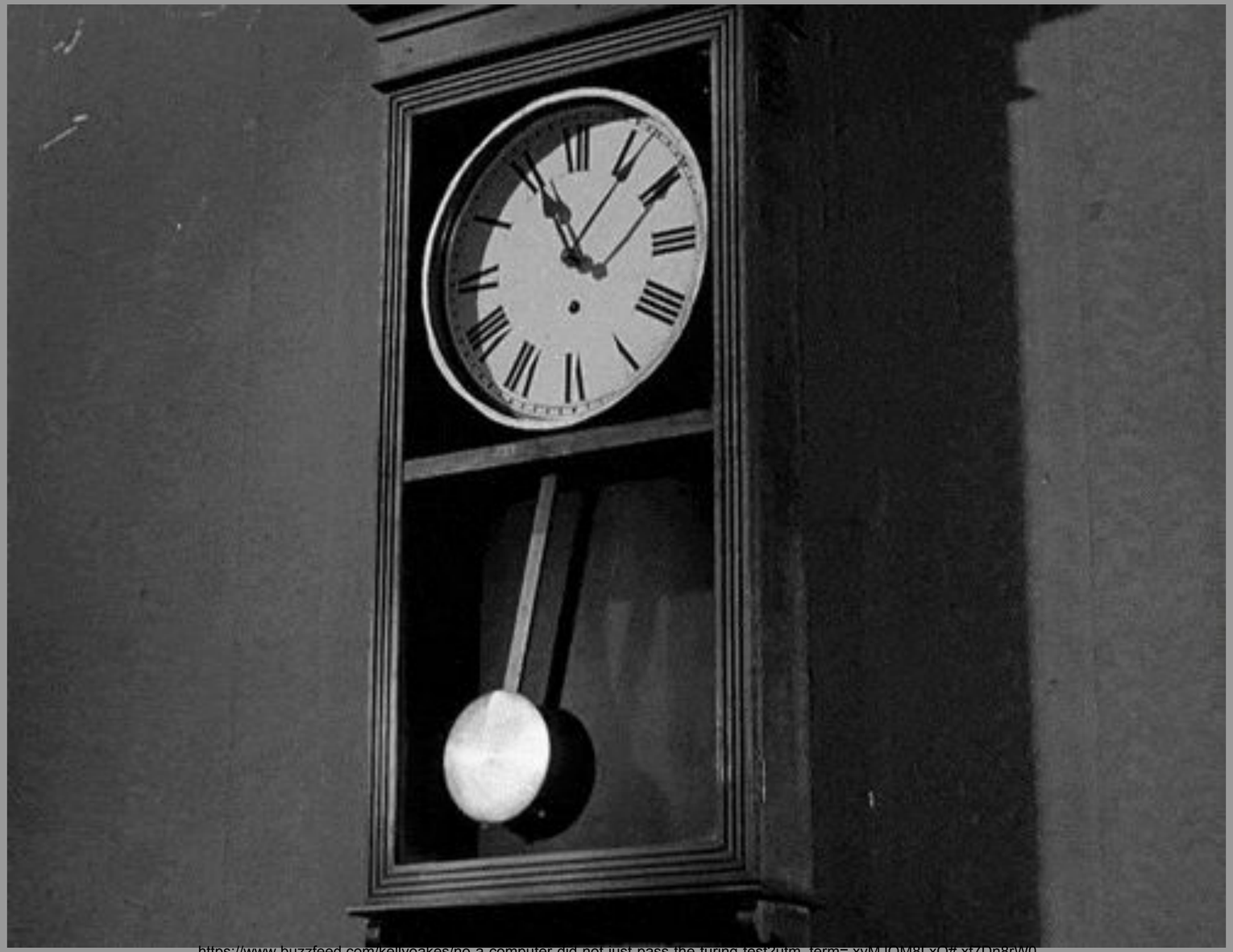
ANSIBLE



THE MELTDOWN

TROUBLESHOOTING

ANSIBLE



https://www.buzzfeed.com/kellyoakes/no-a-computer-did-not-just-pass-the-turing-test?utm_term=.xvMJQM8LxQ#.xf7Dn8rW0n

SYSTEM MELTDOWN

ANSIBLE

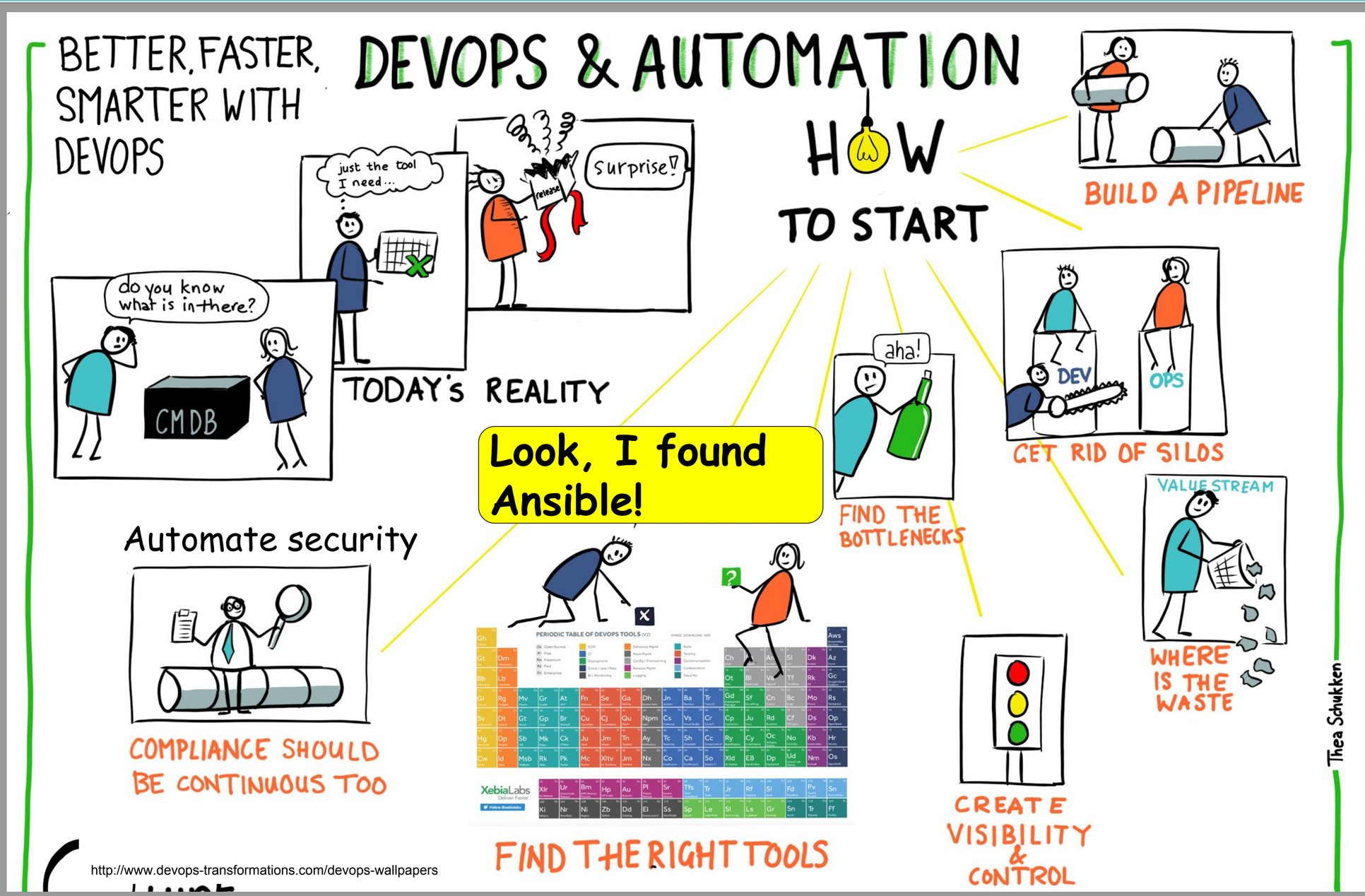
Something has to change

WE NEED A SOLUTION

ANSIBLE

DEVOPS AND AUTOMATION

ANSIBLE



WHY ANSIBLE FOR SECURITY AUTOMATION?

- Agentless
- SSH/WinRM
- Desired State
- Idempotent
- Easy to learn
- Extensible and modular
- Push-based architecture
- Easy targeting based on facts

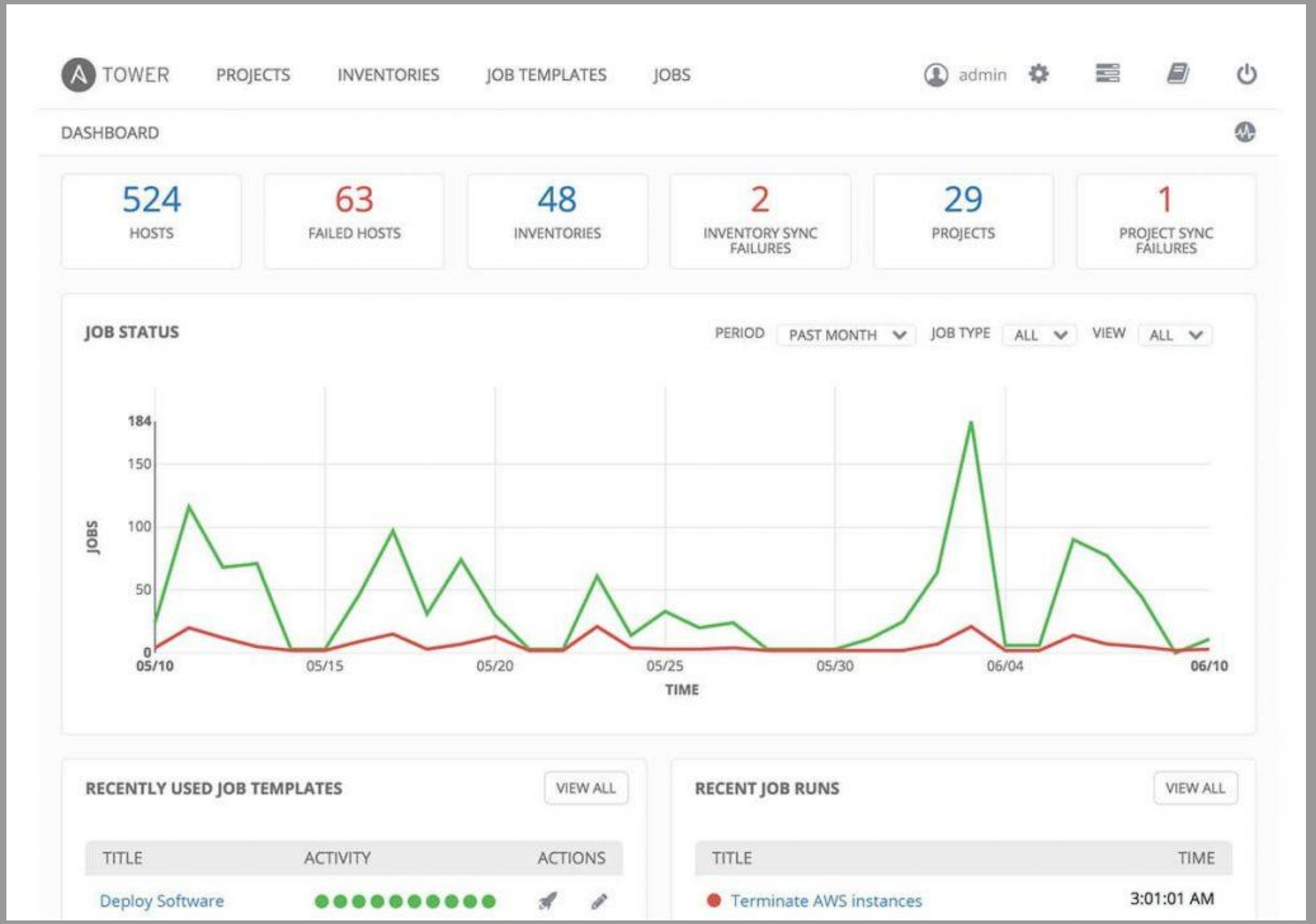
NOT ZERO SUM

+ !=

0

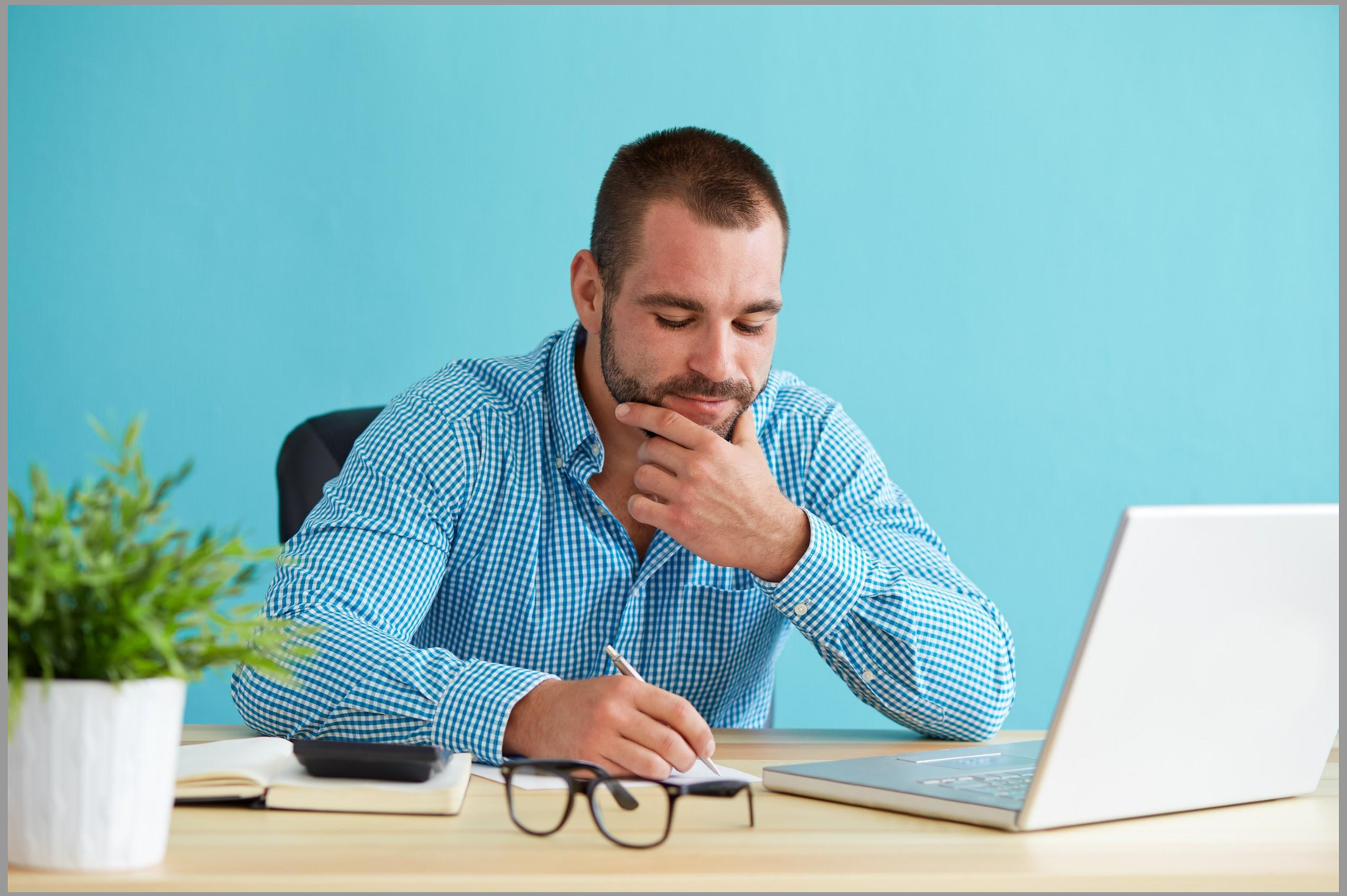
MORE SECURITY

ANSIBLE



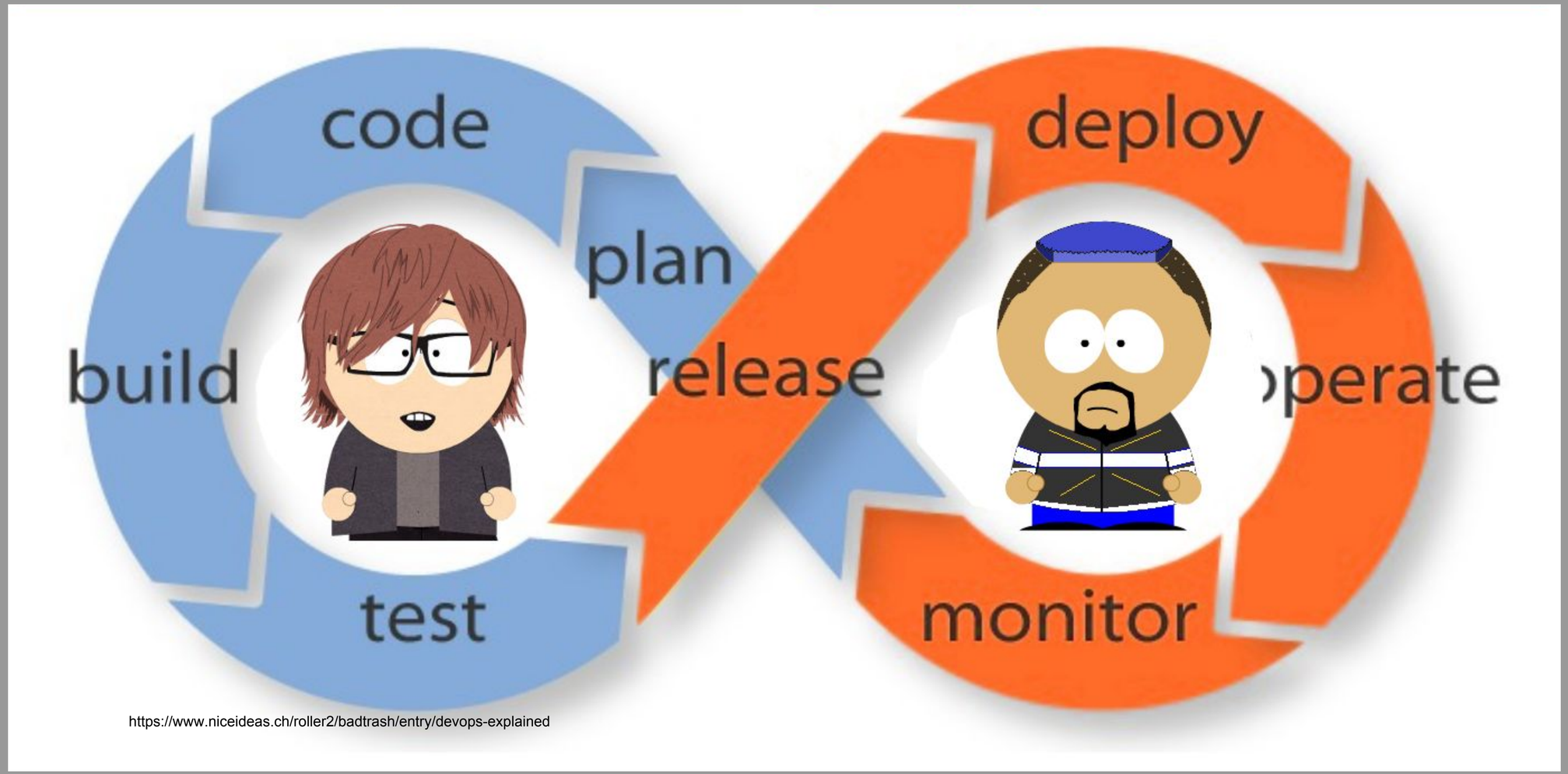
LET'S GET AUTOMATING

ANSIBLE



LET'S GET AUTOMATING

ANSIBLE



https://www.niceideas.ch/roller2/badtrash/entry/devops-explained

SECURITY POLICY - LINUX

ANSIBLE

Rule Title: The SSH daemon must not allow authentication using an empty password.

Fix Text: To explicitly disallow remote logon from accounts with empty passwords, add or correct the following line in "/etc/ssh/sshd_con

line

/etc/ssh/sshd_config

PermitEmptyPasswords no

PermitEmptyPasswords no

```
- name: "HIGH | RHEL-07-010270 | PATCH | The SSH daemon must not allow authentication using an empty password."
  lineinfile:
    state: present
    dest: /etc/ssh/sshd_config
    regexp: ^#?PermitEmptyPasswords
    line: PermitEmptyPasswords no
    validate: sshd -tf %s
  notify: restart sshd
```


redhat.

SECURITY POLICY - NETWORK

ANSIBLE

Rule Title: The network element must only allow management connections for administrative access from hosts residing in to the management network.

Fix Text: Configure an ACL or filter to restrict management access to [illegible] from only the management network.

ACL or filter

management network

```
- hosts: ios
  connection: local

  tasks:
    - name: Create management ACL
      ios_config:
        parents: ip access-list mgmnt
        before: no ip access-list mgmnt
        lines:
          - 10 permit ip host 192.168.1.99 log
          - 20 permit ip host 192.168.1.121 log

    - name: Harden VTY lines
      ios_config:
        parents: line vty 0 15
        lines:
          - exec-timeout 15
          - transport input ssh
          - access mgmnt in
```


redhat.

SECURITY POLICY - WINDOWS

Rule Title: Anonymous enumeration of shares must be restricted.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network access: Do not allow anonymous enumeration of SAM accounts and shares" to "Enabled".

```
- hosts: windows

  tasks:
    - name: Restrict enumeration of shares
      win_regedit:
          key:
'HKLM:\System\CurrentControlSet\Control\Lsa'
          value: RestrictAnonymous
          data: 1
          datatype: dword
```

6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release.

```
- name: RHEL | Install updates
  yum:
    name: "*"
    state: latest
    exclude: "mysql* httpd* nginx*"
  when: “ansible_os_family == ‘RedHat’”

- name: DEBIAN | Install updates
  apt:
    update_cache: yes
    cache_valid_time: 7200
    name: "*"
    state: latest
  when: “ansible_os_family == ‘Debian’”
```

INTERNAL STANDARDS

Change root password every 60 days

```
- name: Change root password
  hosts: all
  become: yes
  vars:
    root_password: "{{ vault_root_password }}"
    root_password_salt: "{{ vault_root_password_salt }}"
  tasks:
    - name: Change root password
      user:
        name: root
        password: "{{ root_password |
password_hash(salt=root_password_salt) }}"
```

Protect against CVE-2016-5696

```
- name: Protect against CVE-2016-5696
  hosts: all
  become: yes
  become_user: root

  tasks:
    - name: CVE-2016-5696 | Limit TCP challenge ACK limit
      sysctl:
        name: net.ipv4.tcp_challenge_ack_limit
        value: 999999999
        sysctl_set: yes
```

Fix and test shellshock

```
- name: Fix and test shellshock
  hosts: all
  tasks:
    - name: Update bash
      yum:
        name: bash
        state: latest
        update_cache: yes

    - name: Test vulnerability 1
      shell: 'env x=''() { :;}; echo vulnerable'' bash -c "echo
this is a test"'
      executable: /bin/bash
      register: vulntest1
      failed_when: vulntest1.stdout | search('vulnerable')
      ignore_errors: yes
      changed_when: no
```

Fix and test shellshock - continued

```
- name: Test vulnerability 2
      shell: 'env X=''() { (a)=>'' bash -c ''echo date'';'
      executable: /bin/bash
      register: vulntest2
      failed_when:
        not vulntest2.stderr | search('error importing function
definition')
      ignore_errors: yes
      changed_when: no

    - name: Cleanup after vulnerability test 2
      file:
        path: ~/echo
        state: absent
```

THE END

ANSIBLE

GET INVOLVED

Ansible Lockdown

Ansible Hardening

Mailing List

Ansible Galaxy

https://github.com/samdoran/demo-playbooks