Failing to Comply: The Urgent Need for Security Policies

Lisa Umberger
Who Am I?

- Ex-NSA (yes, the scary one)
- Control freak turned Security engineer turned CEO (not a coincidence)
- Founder of a company
- Animal lover (especially snakes!)
Why you are here..

- You deal with IT compliance
- You want to find a way to deal with security policy in the least painful way possible
- You think IT and Security could have a better relationship
- You wish compliance was already automated
- You have enough security awareness, and not enough “now what?”
Policy, Benchmarks, and Compliance

- **Policy**: “what” and “why”; objectives and constraints for security at multiple levels such as business, organizational, operational
- **Benchmarks**: “how”; a specific implementation; something we test against
- **Compliance**: adherence to a governing document; measurable; ties policy and benchmarks together
Policy

- Clearly defined
- Valuable to disparate teams and organizations
  - Collaborative is preferable
- Flexible
  - We can’t intentionally create tech debt, after all
- Adherable
Benchmarks

● Technical implementation guides
  ○ STIGs, for our fellow government folks
● Typically used by scanners to check technical compliance
  ○ I really wish the XML SCAP files weren’t awful…
  ○ Ditto you, NESSUS .rules files…
● Give measurable examples to test against
  ○ Which means we also know how to get compliant
● Portable and reusable
Compliance as a Common Language

- Engineers should love compliance…
  - …yes, seriously
- Compliance is consistency
- Compliance is provable
- Compliance can be automated
- But the best… compliance can keep your security team off of your back
  - They already speak the language
  - You can scan for it to make them happy
  - You can do it once and stop worrying about it
Bridging the gap

Security Team

Define policy
Scan instances
Visualize compliance
Validate configurations

IT Engineering Team

Enforce the policy defined by security
Build infrastructure via APIs
Use existing tooling i.e Puppet, Gitlab, ServiceNow

Sicura Console

Sicura modules, content, and APIs
What this looks like in practice

Diagram: A flowchart showing the interaction between Board, CEO, Stakeholders, CISO, Security team, Platform Engineering, and their respective responsibilities such as reporting, initiatives & requirements, assess controls, verify controls, implement controls, cost saving, efficiency, budget, and input for select controls and profile tailoring.
The Cost of Engineering Without Policy Adherence
Hacked Account

Data Breach Report

CyberAttack News

Market Analysis

security failure

leaked data

Malware Attack!

Hacker, strange man in hoodie accessed the system.

Illegal activity

Fraud moves to internet

Malware

Hackers

"What's been taken is bits of data, assembled together into a whole."

Stop the presses! I've been hacked!

By Garland Technology

Officials in the small town of Panchy took part in fraud and widespread corruption, including accepting bribes from contractors.

Apple can't fix Apple, music

Tunes charge scanning

Six people have been arrested over a scam involving the creation of fake websites.

Online scam 'breached security.'
You Get The Idea
Let’s Talk Numbers
Number of Breaches Per Year (In Millions)
Just in Healthcare Alone

It is not just the number of data breaches that are increasing as the breaches are becoming more severe. 2021 was a bad year for data breaches with 45.9 million records breached, and 2022 was worse with 51.9 million records breached, but 2023 smashed all previous records with an astonishing 133 million records exposed, stolen, or otherwise impermissibly disclosed. The huge total for 2023 includes 26 data breaches of more than 1 million records and four breaches of more than 8 million records. The largest data breach of the year affected 11,270,000 individuals – the second-largest healthcare data breach of all time.
Who is committing these attacks?

- Individuals
- Groups
- Corporate espionage
- State-sponsored attackers
- AI-powered botnets
- It really could be anyone for any reason
A Real World Example of Policy in a Hybrid Environment
Just a Little Backstory

- Major financial services company
- Infrastructure team creates and manages all infrastructure both on perm and in the cloud
- Security wants to be CIS compliant
- Separate policies for separate orgs
- Constant pressure to meet deadlines for business goals
- Keep security in the loop (and off their backs)
- Automated policy updates
The Proposed Solution

● Define and tailor technical controls
● Enforce configurations on infrastructure
  ○ Apply to on-prem OS
  ○ Create a cloud image (AWS)
● Scan hardened OS to ensure compliance
  ○ Schedule scans regularly (based on policy reqs)
  ○ Remediate and enforce as needed
● Automate all of this so magic happens when policy updates exist
Relevant Technology

- **Sicura**, previously **SIMP**
- **Compliance Engine**
- **Puppet**
- **Bolt**
- **Packer**
- **AWS**
- **GitLab**
- Possibly others?
Under The Hood
Compliance Engine - Overview

- Open source compliance markup language and enforcement tool
- Create full policies as rule mappings
  - Stay tuned, this will make more sense visually
- Map benchmark rules to configuration elements
  - It’s gotta pass the scanner, right?
- Risk score associated with a given rule
- Combine policies
Compliance Engine - Setup

---

# hiera.yaml

version: 5

hierarchy:
  - name: Compliance Engine
    lookup_key: compliance_markup::enforcement

# common.yaml

compliance_markup::enforcement:
  - 'cis_profile_org1'
Compliance Engine - Profiles

profiles:

cis_profile_org1: # Org-specific CIS policy

checks: # List of rules to include in this profile

  oval:com.puppet.forge.sicura.cis.ssh.server.conf.permitrootlogin : true
  oval:com.puppet.forge.sicura.cis.ssh.server.conf.permitemptypasswords : true
  oval:com.puppet.forge.sicura.cis.ssh.server.conf.clientaliveinterval : true
  oval:com.puppet.forge.sicura.cis.ssh.server.conf.x11forwarding : false
  oval:com.puppet.forge.sicura.cis.ssh.server.conf.maxauthtries : false
  oval:com.puppet.forge.sicura.cis.ssh.server.conf.maxsessions : false
Compliance Engine - Mapping to Puppet

---

checks: # The rule IDs, and how they map to Puppet code

oval:com.puppet.forge.sicura.cis.ssh.server.conf.permitrootlogin

settings:

  parameter: profile::ssh_server::permit_root_login  # Standard class param
  value: 'no'                                        # Standard class value

  type: puppet-class-parameter

remediation:

  risk:

    - level: 41
      reason: >-
        Systems that only use root users to login will no longer be able to login.
Bolt for One-time Apply

plan cis::apply (  
    TargetSpec $targets = 'localhost',
) {
    apply_prep($targets)

    $apply_results = apply($targets, '_catch_errors' => true) {
        $classes = lookup('profile::ssh_server', Array[String], 'unique', [])
        include $classes
    }
}
Packer to Build the Image

build {
  provisioner "shell" {
    inline = [
      "sudo yum -y install puppet-bolt",
      "bolt plan run cis::apply -t localhost --run-as root --stream"
    ]
  }
}

Scan For CIS Coverage

<table>
<thead>
<tr>
<th>&quot;CIS Red Hat Enterprise Linux 8 Benchmark&quot;: &quot;2.0.0&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;CIS Level 1 - Server&quot;</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Stage</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>pre</td>
</tr>
<tr>
<td>post</td>
</tr>
</tbody>
</table>
And... Voila!

Amazon Machine Images (AMIs) (1/1)  Info

Owned by me ▼  Find AMI by attribute or tag

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>AMI name</th>
<th>AMI ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>CIS Org1</td>
<td>sicura-1699975918</td>
<td>ami-0a278cea6bbee6c6f</td>
</tr>
</tbody>
</table>
Converting Benchmarks
Benchmark Format

- XML, usually SCAP
- Tons of metadata
- Difficult to parse
- Not consistent between authors
- :-(
The `PermitRootLogin` parameter specifies if the root user can log in using ssh. The default is no.

Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via or . This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident.

Edit the file to set the parameter as follows:

```bash
PermitRootLogin no
```
Converting the Benchmark

- Check if new benchmark or updating existing
- Convert to YAML
- Parse out the rule ID from the benchmark XML
- Create unique keys based on all rules
- Create configuration element backend
- Serialize to json (cut compile time by 90%)
Pipeline | Needs | Jobs | Tests
---|---|---|---
new_benchmark_check
  - Check for benchmarks
  - Convert and automap new benchmarks
    - Trigger job
Downstream
  - Convert and automap new benchmarks
    - #127106
      - Child
  - test
    - job
A Visual
### Customize ruleset

**Available Rules from cis on Redhat Enterprise Linux 8**

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure mounting of cramfs filesystems is disabled</td>
<td>5</td>
</tr>
<tr>
<td>Ensure gpgcheck is globally activated</td>
<td>3</td>
</tr>
<tr>
<td>Ensure AIDE is installed</td>
<td>3</td>
</tr>
<tr>
<td>Ensure filesystem integrity is regularly checked</td>
<td>3</td>
</tr>
<tr>
<td>Ensure bootloader password is set</td>
<td>9</td>
</tr>
<tr>
<td>Ensure permissions on bootloader config are configured</td>
<td>9</td>
</tr>
<tr>
<td>Ensure address space layout randomization (ASLR) is enabled</td>
<td>7</td>
</tr>
<tr>
<td>Ensure SELinux is installed</td>
<td>9</td>
</tr>
<tr>
<td>Ensure SELinux is not disabled in bootloader configuration</td>
<td>9</td>
</tr>
<tr>
<td>Ensure permissions on /etc/motd are configured</td>
<td>9</td>
</tr>
<tr>
<td>Ensure permissions on /etc/issue are configured</td>
<td></td>
</tr>
<tr>
<td>Ensure permissions on /etc/security/limits.conf are configured</td>
<td></td>
</tr>
<tr>
<td>Ensure SELinux policy is configured</td>
<td></td>
</tr>
<tr>
<td>Ensure no unconfined services exist</td>
<td></td>
</tr>
<tr>
<td>Ensure SETroubleshoot is not installed</td>
<td></td>
</tr>
<tr>
<td>Ensure the MCS Translation Service (mcstrans) is not installed</td>
<td></td>
</tr>
<tr>
<td>Ensure message of the day is configured properly</td>
<td></td>
</tr>
<tr>
<td>Ensure local login warning banner is configured properly</td>
<td></td>
</tr>
<tr>
<td>Ensure remote login warning banner is configured properly</td>
<td></td>
</tr>
<tr>
<td>Ensure GDM login banner is configured</td>
<td></td>
</tr>
<tr>
<td>Ensure last logged in user display is disabled</td>
<td></td>
</tr>
<tr>
<td>Ensure updates, patches, and</td>
<td></td>
</tr>
</tbody>
</table>

**Active Rules in “Custom CIS Level 1”**

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure SELinux policy is configured</td>
<td>9</td>
</tr>
<tr>
<td>Ensure no unconfined services exist</td>
<td>5</td>
</tr>
<tr>
<td>Ensure SETroubleshoot is not installed</td>
<td>9</td>
</tr>
<tr>
<td>Ensure the MCS Translation Service (mcstrans) is not installed</td>
<td>5</td>
</tr>
<tr>
<td>Ensure message of the day is configured properly</td>
<td>8</td>
</tr>
<tr>
<td>Ensure local login warning banner is configured properly</td>
<td>8</td>
</tr>
<tr>
<td>Ensure remote login warning banner is configured properly</td>
<td>8</td>
</tr>
<tr>
<td>Ensure GDM login banner is configured</td>
<td>8</td>
</tr>
<tr>
<td>Ensure last logged in user display is disabled</td>
<td>8</td>
</tr>
</tbody>
</table>

Search:
## Enforcement Profiles

**Default**  |  **Custom**
---|---

**Creator:**

(Optional) filter by creator...

**Platform:**

(Optional) filter by platform...

---

**Platform**  |  **Name**  |  **Version**  |  **Description**  |  **Creation Date**  |  **Creator**  |  **Actions**
---|---|---|---|---|---|---
Redhat Enterprise Linux 8  |  Custom CIS Level 1  |  2.0.0  |  Items in this profile intend to: be practical and prudent; provide a clear security benefit; and not inhibit the utility of the technology beyond acceptable means. This profile is intended for servers.  |  2023-11-17 19:09:40 +0000  |  kendall@sicura.us  |  ![Generate AMI](image)

---

Show 10 entries  |  Showing 1 to 1 of 1 entries  |  Previous  |  1  |  Next
Questions?

lisa@sicura.us