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, afterall
- 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

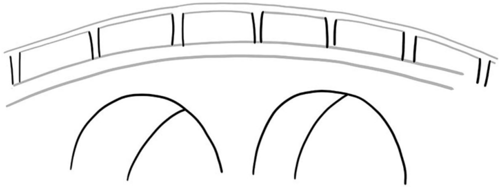
Security Team

Define policy

Scan instances

Visualize compliance

Validate configurations



IT Engineering Team

Enforce the policy defined by security

Build infrastructure via APIs

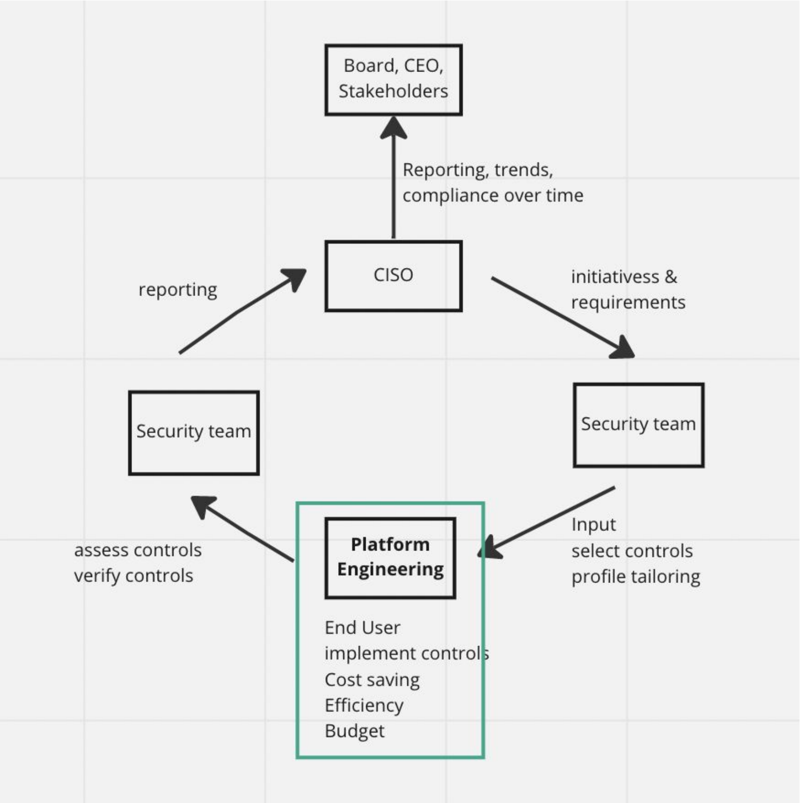
Use existing tooling i.e Puppet, Gitlab, ServiceNow

Sicura Console

SICURA

Sicura modules,content, and APIs

What this looks like in practice



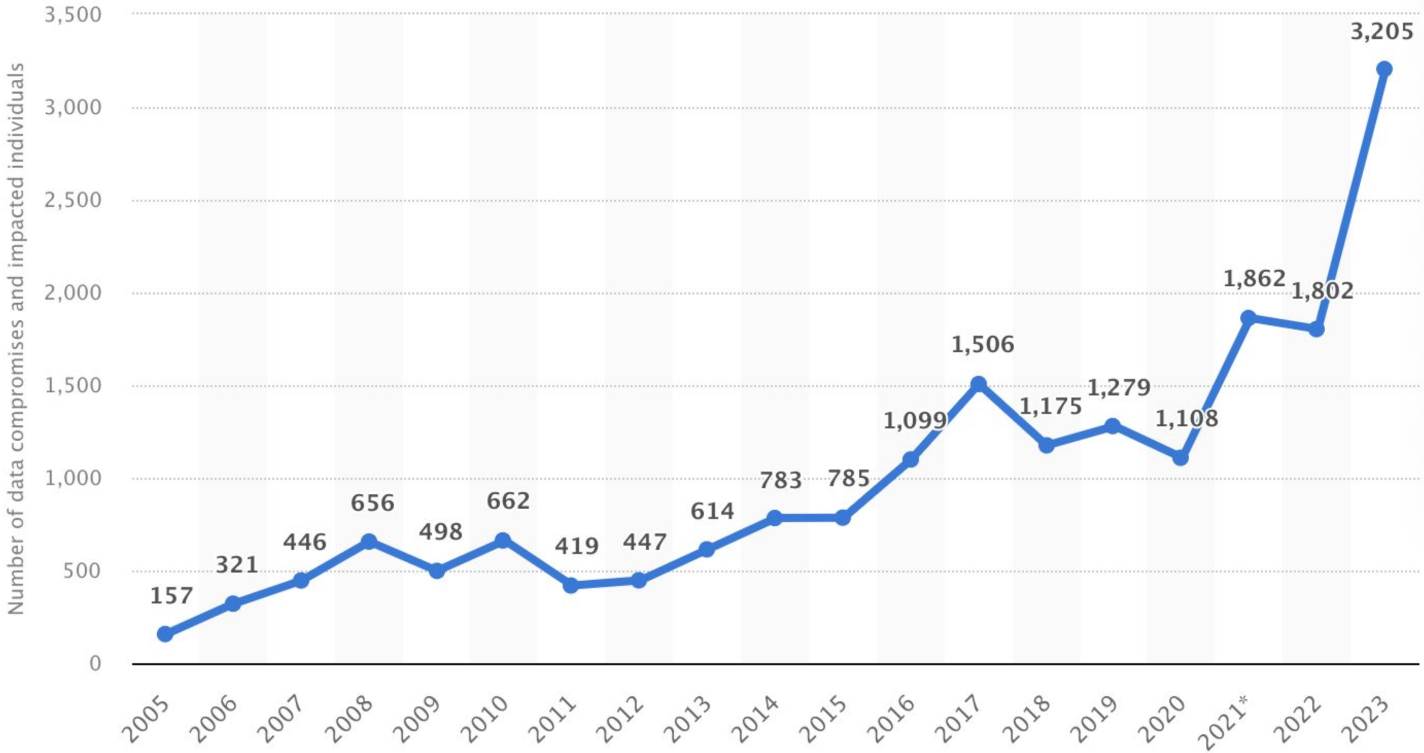
The Cost of Engineering Without Policy Adherence

Data Breach Report
2022
CyberAttack News
Market Analysis
Los Angeles Times
$1.00 DESIGNATED AREAS HIGHER 74 PAGES © 2012 WST FRIDAY, December 2018
latimes.c
Malwar
Attack!
Stop the presses! I've been hacked
By Garland Technology
Hacker, strange man in hoody accessed the
security failure
leaked data
breach
Hacked Ac
illegal activity
fraud moves to internet
gets bring new for hackers!
I announces arrests in $70 million cyber-theft
A Facebook e-mail phising
Malware
2011 will see increased security threats on mobile devices.
Apple can't iTunes charge scam
Six people have been arrested over a scam wich police
Online scam 'breached security
Hackers
"What's been taken is bits of data
cyber attack

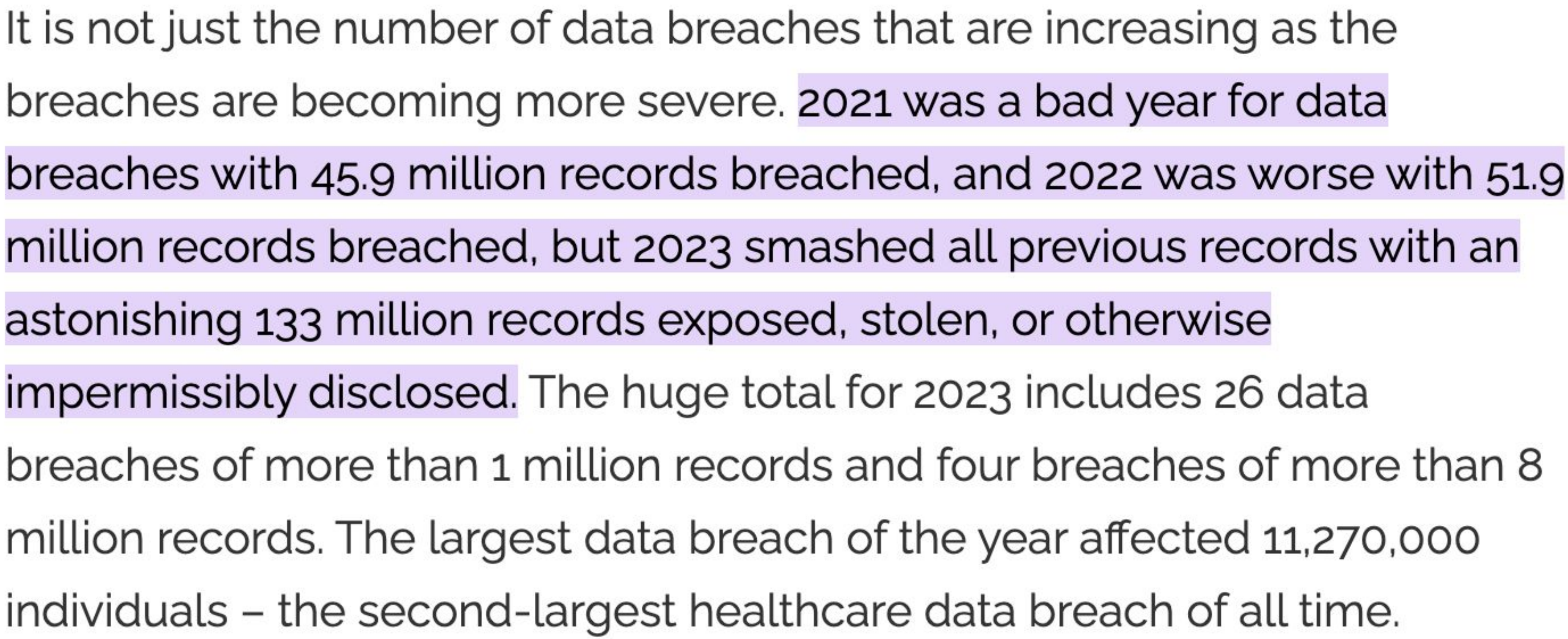
You Get The Idea

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
- Probably 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
 }
}
```

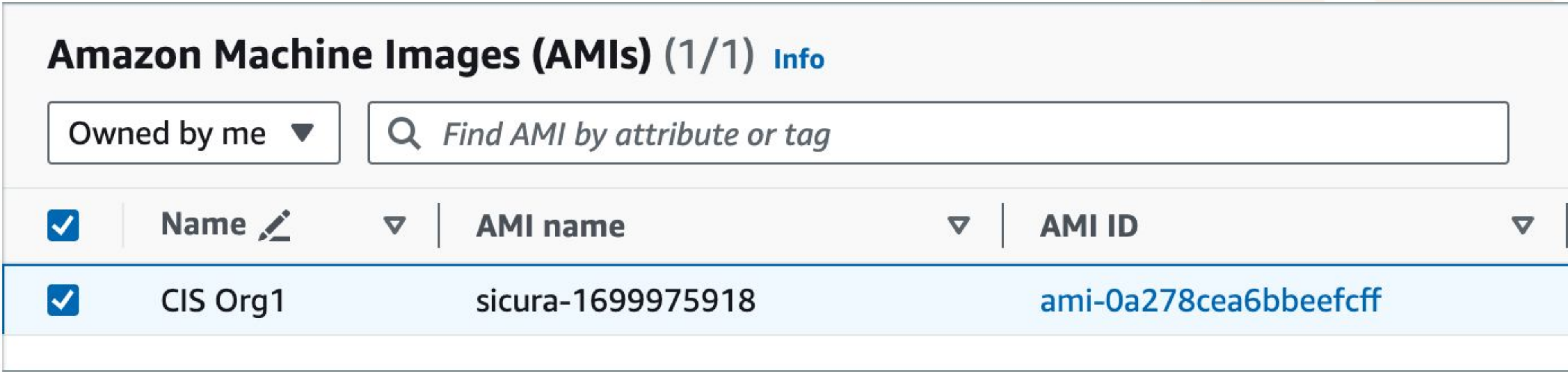
Packer to Build the Image

```
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

```
================================================================
| "CIS Red Hat Enterprise Linux 8 Benchmark": "2.0.0"          |
----------------------------------------------------------------
+--------------------------------------------------------------+
|                      "CIS Level 1 - Server"                  |
+--------------+-------+------+---------+--------------+-------+
| Stage        | Pass  | Fail | Unknown | Not Selected | Score |
+--------------+-------+------+---------+--------------+-------+
| pre          | 152.0 | 92   | 0       | 28           | 62%   |
| post         | 214.0 | 30   | 0       | 28           | 88%   |
+--------------+-------+------+---------+--------------+-------+
```

And… Voila!



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

Owned by me ▼

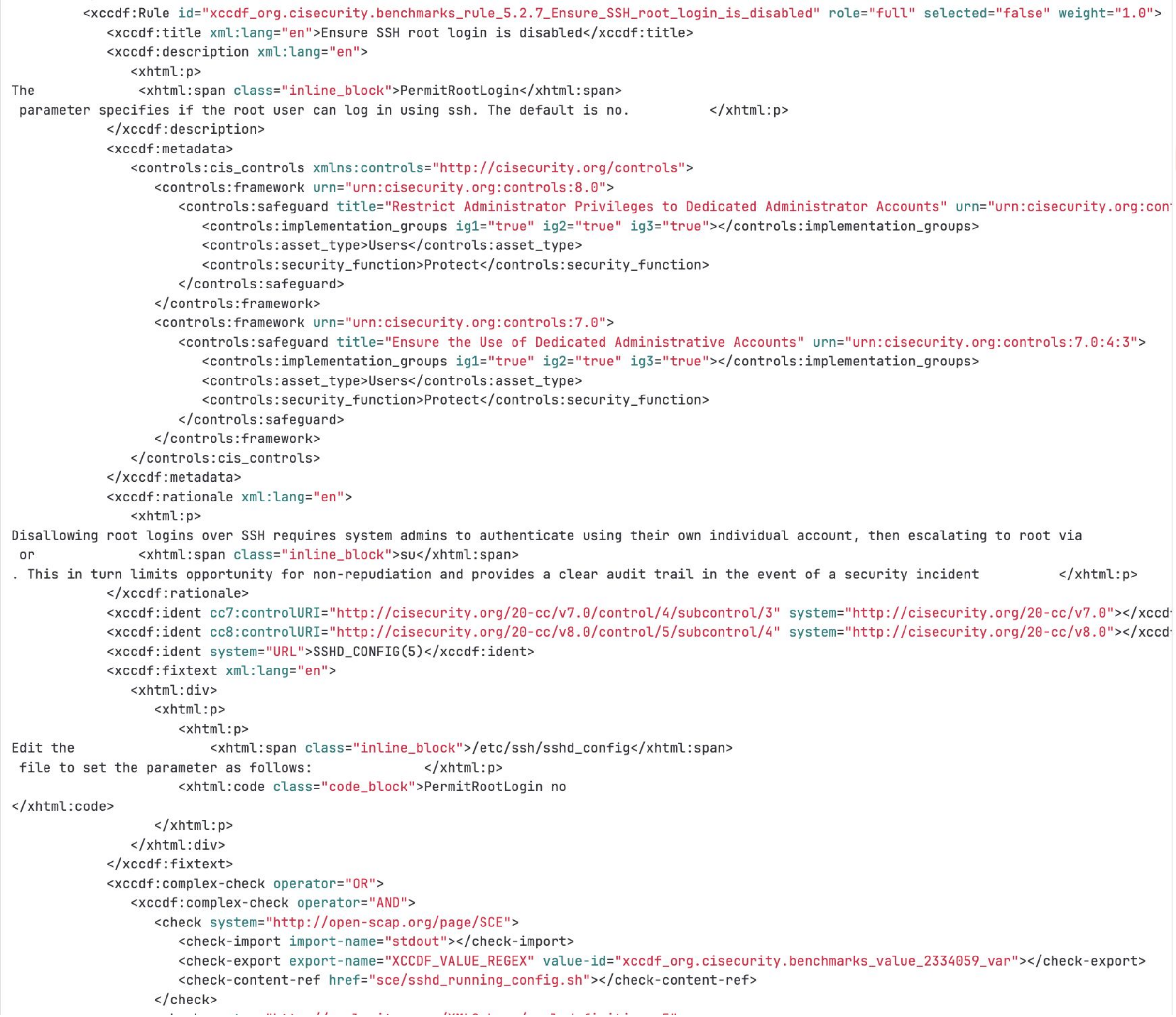
Find AMI by attribute or tag

☑	Name	AMI name	AMI ID
☑	CIS Org1	sicura-1699975918	ami-0a278cea6bbeefcff

Converting Benchmarks

Benchmark Format

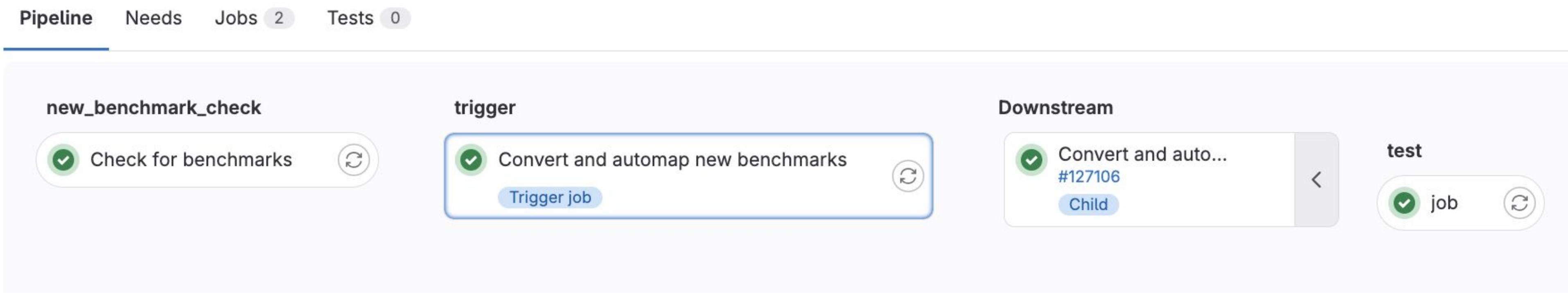
- XML, usually SCAP
- Tons of metadata
- Difficult to parse
- Not consistent between authors
- :-(



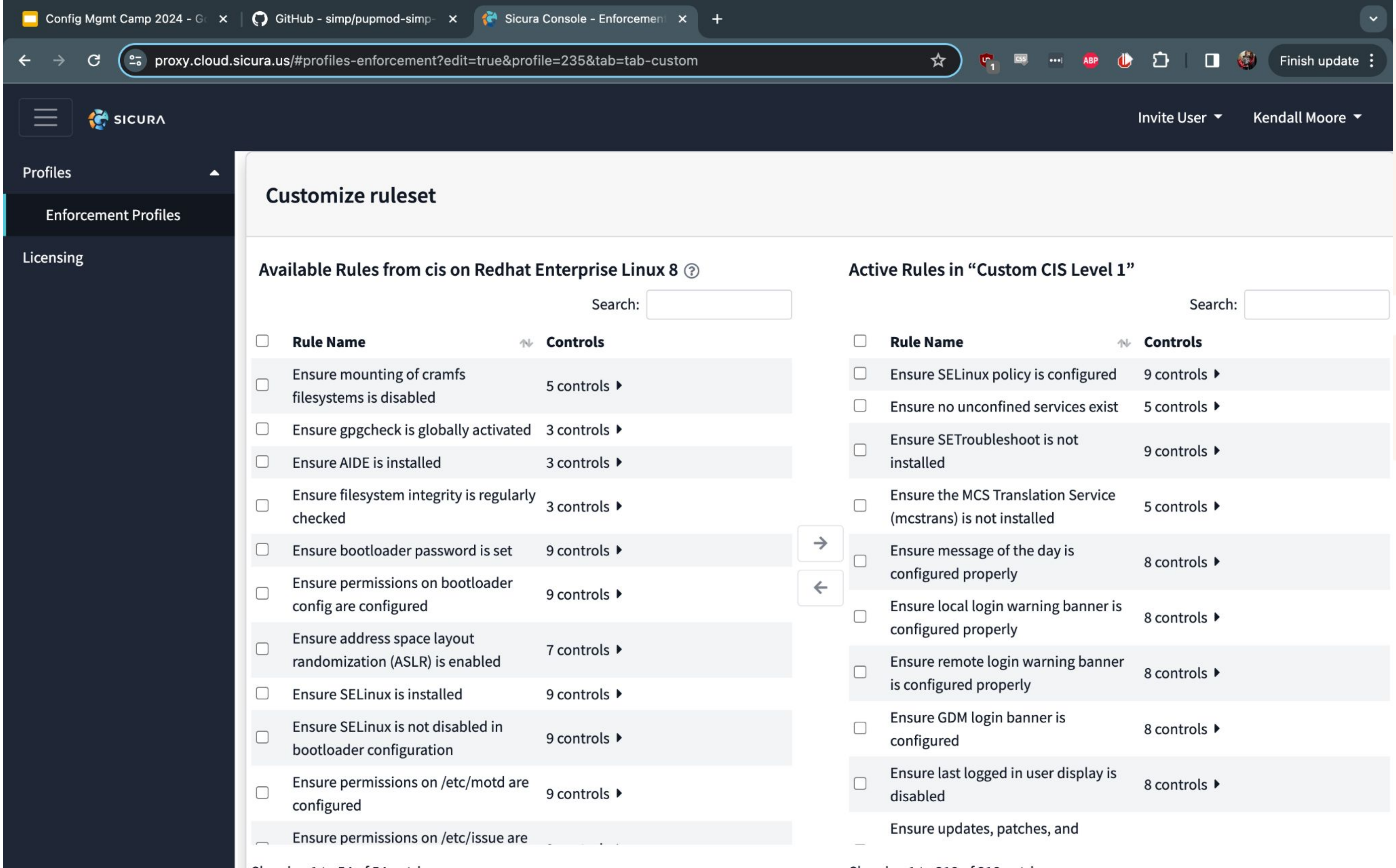
```
         <xccdf:Rule id="xccdf_org.cisecurity.benchmarks_rule_5.2.7_Ensure_SSH_root_login_is_disabled" role="full" selected="false" weight="1.0">
            <xccdf:title xml:lang="en">Ensure SSH root login is disabled</xccdf:title>
            <xccdf:description xml:lang="en">
               <xhtml:p>
The             <xhtml:span class="inline_block">PermitRootLogin</xhtml:span>
 parameter specifies if the root user can log in using ssh. The default is no.          </xhtml:p>
            </xccdf:description>
            <xccdf:metadata>
               <controls:cis_controls xmlns:controls="http://cisecurity.org/controls">
                  <controls:framework urn="urn:cisecurity.org:controls:8.0">
                     <controls:safeguard title="Restrict Administrator Privileges to Dedicated Administrator Accounts" urn="urn:cisecurity.org:con
                        <controls:implementation_groups ig1="true" ig2="true" ig3="true"></controls:implementation_groups>
                        <controls:asset_type>Users</controls:asset_type>
                        <controls:security_function>Protect</controls:security_function>
                     </controls:safeguard>
                  </controls:framework>
                  <controls:framework urn="urn:cisecurity.org:controls:7.0">
                     <controls:safeguard title="Ensure the Use of Dedicated Administrative Accounts" urn="urn:cisecurity.org:controls:7.0:4:3">
                        <controls:implementation_groups ig1="true" ig2="true" ig3="true"></controls:implementation_groups>
                        <controls:asset_type>Users</controls:asset_type>
                        <controls:security_function>Protect</controls:security_function>
                     </controls:safeguard>
                  </controls:framework>
               </controls:cis_controls>
            </xccdf:metadata>
            <xccdf:rationale xml:lang="en">
               <xhtml:p>
Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via
 or             <xhtml:span class="inline_block">su</xhtml:span>
. This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident          </xhtml:p>
            </xccdf:rationale>
            <xccdf:ident cc7:controlURI="http://cisecurity.org/20-cc/v7.0/control/4/subcontrol/3" system="http://cisecurity.org/20-cc/v7.0"></xccd
            <xccdf:ident cc8:controlURI="http://cisecurity.org/20-cc/v8.0/control/5/subcontrol/4" system="http://cisecurity.org/20-cc/v8.0"></xccd
            <xccdf:ident system="URL">SSHD_CONFIG(5)</xccdf:ident>
            <xccdf:fixtext xml:lang="en">
               <xhtml:div>
                  <xhtml:p>
                     <xhtml:p>
Edit the                 <xhtml:span class="inline_block">/etc/ssh/sshd_config</xhtml:span>
 file to set the parameter as follows:              </xhtml:p>
                     <xhtml:code class="code_block">PermitRootLogin no
</xhtml:code>
                  </xhtml:p>
               </xhtml:div>
            </xccdf:fixtext>
            <xccdf:complex-check operator="OR">
               <xccdf:complex-check operator="AND">
                  <check system="http://open-scap.org/page/SCE">
                     <check-import import-name="stdout"></check-import>
                     <check-export export-name="XCCDF_VALUE_REGEX" value-id="xccdf_org.cisecurity.benchmarks_value_2334059_var"></check-export>
                     <check-content-ref href="sce/sshd_running_config.sh"></check-content-ref>
                  </check>
                  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
```

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 2
Tests 0
new_benchmark_check
Check for benchmarks
trigger
Convert and automap new benchmarks
Trigger job
Downstream
Convert and auto...
#127106
Child
test
job

A Visual



Config Mgmt Camp 2024 - G
GitHub - simp/pupmod-simp-
Sicura Console - Enforcemen
proxy.cloud.sicura.us/#profiles-enforcement?edit=true&profile=235&tab=tab-custom
Finish update
SICURA
Invite User
Kendall Moore
Profiles
Enforcement Profiles
Licensing

Customize ruleset

Available Rules from cis on Redhat Enterprise Linux 8

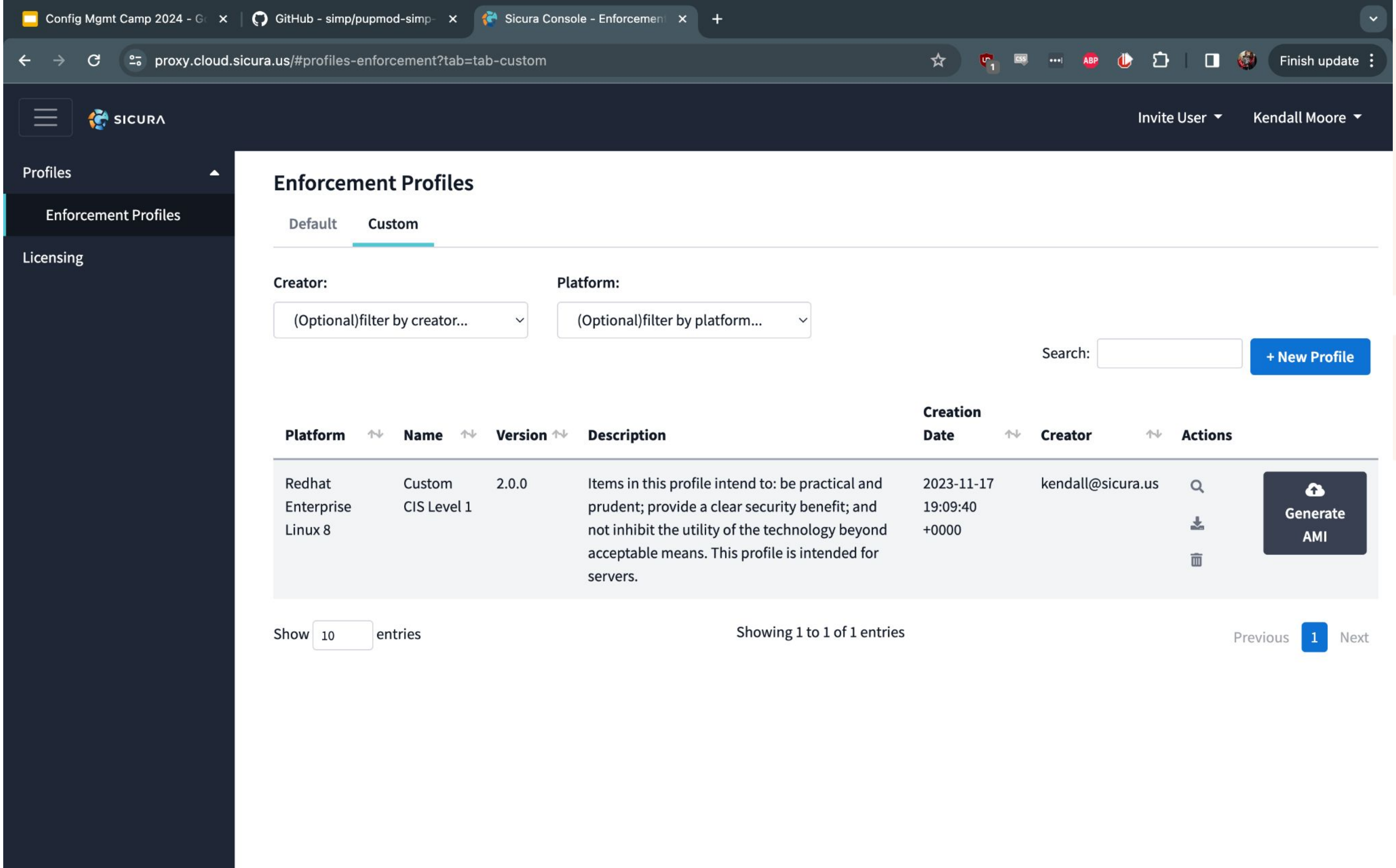
Search:

☐	Rule Name	Controls
☐	Ensure mounting of cramfs filesystems is disabled	5 controls ▸
☐	Ensure gpgcheck is globally activated	3 controls ▸
☐	Ensure AIDE is installed	3 controls ▸
☐	Ensure filesystem integrity is regularly checked	3 controls ▸
☐	Ensure bootloader password is set	9 controls ▸
☐	Ensure permissions on bootloader config are configured	9 controls ▸
☐	Ensure address space layout randomization (ASLR) is enabled	7 controls ▸
☐	Ensure SELinux is installed	9 controls ▸
☐	Ensure SELinux is not disabled in bootloader configuration	9 controls ▸
☐	Ensure permissions on /etc/motd are configured	9 controls ▸
☐	Ensure permissions on /etc/issue are	

Active Rules in “Custom CIS Level 1”

Search:

☐	Rule Name	Controls
☐	Ensure SELinux policy is configured	9 controls ▸
☐	Ensure no unconfined services exist	5 controls ▸
☐	Ensure SETroubleshoot is not installed	9 controls ▸
☐	Ensure the MCS Translation Service (mcstrans) is not installed	5 controls ▸
☐	Ensure message of the day is configured properly	8 controls ▸
☐	Ensure local login warning banner is configured properly	8 controls ▸
☐	Ensure remote login warning banner is configured properly	8 controls ▸
☐	Ensure GDM login banner is configured	8 controls ▸
☐	Ensure last logged in user display is disabled	8 controls ▸
	Ensure updates, patches, and	


Config Mgmt Camp 2024 - G
GitHub - simp/pupmod-simp-
Sicura Console - Enforcemen
proxy.cloud.sicura.us/#profiles-enforcement?tab=tab-custom
Finish update
SICURA
Invite User
Kendall Moore
Profiles
Enforcement Profiles
Licensing

Enforcement Profiles

Default | Custom

Creator: (Optional)filter by creator...

Platform: (Optional)filter by platform...

Search:

+ New Profile

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

Show 10 entries

Showing 1 to 1 of 1 entries

Previous 1 Next

Questions?

lisa@sicura.us