

InSpec Profiles* and HDF** include NIST SP 800-53 Security Control associations

DRAFT

March 2020

* built within the saf.mitre.org community and [CMS ISPG GitHub](https://github.com/CMS-ISPG)

** Heimdall Data Format



Background – InSpec Profile Development Tool Chain

[https://github.com/
mitre/vulcan](https://github.com/mitre/vulcan)



Security Testing Content Development

[https://inspec-
tools.mitre.org/](https://inspec-tools.mitre.org/)

MITRE
Inspec_tools

Automated
Conversion

Human Code
Completion/Refinement

[https://github.com/
mitre/*baseline](https://github.com/mitre/*baseline)



Security Validation as Code Execution

System(s) Under Evaluation
Master Nodes (3)

Ingest Nodes (X)

Data Nodes - Hot (X)

Data Nodes - Warm (X)

InSpec Engine



CCE, CVE, Least Functionality Tests

Data Mapping and Visualization Tools

"HDF", the
Heimdall Data Format
Includes NIST SP 800-53
associations for each test!

Validation
Results



[https://heimdall-
tools.mitre.org/](https://heimdall-tools.mitre.org/)



Static & Dynamic Code Analysis
CWE Tests



[https://Heimdall-
lite.mitre.org](https://Heimdall-lite.mitre.org)



[https://github.com/
mitre/heimdall](https://github.com/mitre/heimdall)

MITRE

Background: The Heimdall Data Format (HDF)

Originally based on the InSpec JSON results reporter format, ISPG has extended and standardized it as the means of recording and transporting (i.e., via Splunk) security data from any source: InSpec profiles, SonarQube, Fortify, OWASP ZAP, etc.

HDF JSON File Schema:

<https://github.com/mitre/inspecjs/blob/master/schemas/exec-json.json>

HDF Splunk Schema:

<https://github.com/mitre/hdf-json-to-splunk#control-event-structure>

We are currently extending [Heimdall tools](#) to convert output from Burp Suite Pro, Nessus, Nikto, Sneak, NetSparker, etc. to HDF.

```
{
  "id": "V-71935",
  "title": "Passwords must be a minimum of 15 characters in length.",
  "desc": "The shorter the password, the lower the number of possible combinations\nthat need to be tested before the password is compromised.\n\n",
  "descriptions": [
    {
      "label": "default",
      "data": "The shorter the password, the"
    },
    {
      "label": "check",
      "data": "Verify the operating system en"
    },
    {
      "label": "fix",
      "data": "Configure operating system to"
    }
  ],
  "impact": 0.5,
  "refs": [],
  "tags": {
    "gttitle": "SRG-OS-000078-GPOS-00046",
    "gid": "V-71935",
    "rid": "SV-86559r1_rule",
    "stig_id": "RHEL-07-010280",
    "cci": [
      "CCI-000205"
    ],
    "documentable": false,
    "nist": [
      "IA-5 (1) (a)",
      "Rev_4"
    ],
    "subsystems": [
      "pam",
      "pwquality",
      "password"
    ],
    "fix_id": "F-78287r1_fix"
  },
  "code": "control \\\"V-71935\\\" do\n  title \\\"Pass",
  "source_location": {
    "line": 10,
    "ref": "inspec-profile-disa_stig-el7-master"
  },
  "results": [
    {
      "status": "failed",
      "code_desc": "Parse Config File /etc/se",
      "run_time": 0.000149026,
      "start_time": "2019-11-04T16:17:07-05:0",
      "message": "\\nexpected it to be >= 15\\n"
    }
  ]
},
{
  "id": "cis-aws-foundations-1.9",
  "title": "Ensure IAM password policy requires minimum length of 14 or greater",
  "desc": "Password policies are, in part, used to enforce password complexity\nrequirements",
  "descriptions": [
    {
      "label": "default",
      "data": "Password policies are, in part, used to enforce password complexity\\nrequi"
    }
  ],
  "impact": 0.3,
  "refs": [],
  "tags": {
    "rationale": "Setting a password complexity policy increases account\\nresiliency agains",
    "cis_impact": "",
    "cis_rid": "1.9",
    "cis_level": 1,
    "csc_control": [
      [
        "5.7",
        "16.12"
      ],
      "6.0"
    ],
    "nist": [
      "IA-5(1)",
      "IA-2",
      "Rev_4"
    ],
    "cce_id": "CCE-78907-3",
    "check": "Perform the following to ensure the password policy is\\nconfigured as prescr",
    "fix": "Perform the following to set the password policy as prescribed:\\n\\nVia AWS Co"
  },
  "code": "control \\\"cis-aws-foundations-1.9\\\" do\n  title \\\"Ensure IAM password policy requ",
  "source_location": {
    "line": 3,
    "ref": "./controls/cis-aws-foundations-1.9.rb"
  },
  "results": [
    {
      "status": "passed",
      "code_desc": "IAM Password-Policy minimum_password_length should cmp >= 14",
      "run_time": 0.000143,
      "start_time": "2018-11-18T20:21:40-05:00"
    }
  ]
},
}
```



DISA STIG

Use Case 1 of 3: DISA STIG to InSpec Profile (with NIST SP 800-53)

DISA STIG Source

The screenshot shows a web browser window displaying the [DISA STIG Source](https://public.cyber.mil/stigs/) website. The page has a dark blue header with the **DoD CYBER EXCHANGE PUBLIC** logo. The main content area features a large banner with the text "Security Technical Implementation Guides (STIGs)". On the left sidebar, there is a "DISA STIG" icon (a document with a pen) and a list of links: "SRG/STIGs Home" (highlighted with a red box), "Control Correlation Identifier (CCI)", "Document Library", "DoD Annex for NIAP Protection Profiles", and "DoD Cloud Computing Security". The main content area includes a shield icon, the word "STIGs", and a paragraph explaining the purpose of STIGs. A yellow button labeled "View and Download STIGs" is also highlighted with a red box.

SRG/STIGs Home

Control Correlation Identifier (CCI)

Document Library

DoD Annex for NIAP Protection Profiles

DoD Cloud Computing Security

View and Download STIGs

<https://public.cyber.mil/stigs/>

MITRE

Example DISA STIG

The screenshot shows a web browser window for the DoD CYBER EXCHANGE PUBLIC site. The URL in the address bar is https://public.cyber.mil/stigs/downloads/?_dl_facet_stigs=operating-systems%2Cunix-linux. The page displays a list of STIGs for various operating systems, sorted by title. A red box highlights the "Red Hat Enterprise Linux 7 STIG - Ver 2, Rel 6" entry.

TITLE	SIZE	UPDATED
Canonical Ubuntu 16.04 STIG - Ver 1, Rel 3	669.67 KB	16 Jan 2020
IBM AIX 7.x STIG - Ver 1, Rel 1	684.81 KB	15 Aug 2019
IBM AIX 7.x STIG - Version 1 - Release Memo	865.71 KB	14 May 2019
Oracle Linux 5 STIG - Ver 1, Rel 13	500.65 KB	26 Jun 2019
Oracle Linux 6 STIG - Ver 1, Rel 17	851.18 KB	31 Oct 2019
Oracle Linux 7 STIG - Ver 1, Rel 1	1.41 MB	28 Feb 2020
Red Hat Enterprise Linux 6 STIG - Ver 1, Rel 24	721.58 KB	31 Oct 2019
Red Hat Enterprise Linux 7 STIG - Ver 2, Rel 6	911.05 KB	16 Jan 2020
Solaris 10 SPARC STIG - Ver 1, Rel 26	695.16 KB	16 Jan 2020
Solaris 10 X86 STIG - Ver 1, Rel 26	815.68 KB	16 Jan 2020

https://public.cyber.mil/stigs/downloads/?_dl_facet_stigs=operating-systems%2Cunix-linux

One of 200+ requirements in the DISA RHEL7 STIG:

*C:\Users\earonne\Desktop\CMS\STIG\U_Red_Hat_Enterprise_Linux_7_V1R4_STIG\U_Red_Hat_Enterprise_Linux_7_V1R4_Manual_STIG\U_Red_Hat_Enterprise_Linux_7_STIG_V1R4_Manual-xccdf.xml Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

U_Red_Hat_Enterprise_Linux_7_STIG_V1R4_Manual-xccdf.xml

This V-71935 is the unique ID for this requirement/test!

```
<Group id="V-71935">
    <title>SRG-OS-000078-GPOS-00046</title>
    <description>&lt;/GroupDescription&gt;&lt;/GroupDescription&gt;</description>
    <Rule id="SV-86559r1_rule" severity="medium" weight="10.0">
        <version>RHEL-07-010280</version>
        <title>Passwords must be a minimum of 15 characters in length.</title>
        <description>&lt;/VulnDiscussion&gt;&lt;/FalsePositives&gt;&lt;/FalsePositives&gt;&lt;/FalseNegatives&gt;&lt;/FalseNegatives&gt;&lt;/Documentable&gt;&lt;/Documentable&gt;&lt;/Mitigations&gt;&lt;/Mitigations&gt;&lt;/SeverityOverrideGuidance&gt;&lt;/SeverityOverrideGuidance&gt;&lt;/PotentialImpacts&gt;&lt;/PotentialImpacts&gt;&lt;/ThirdPartyTools&gt;&lt;/ThirdPartyTools&gt;&lt;/MitigationControl&gt;&lt;/MitigationControl&gt;&lt;/Responsibility&gt;&lt;/Responsibility&gt;&lt;/IAControls&gt;&lt;/IAControls&gt;</description>
        <reference>
            <dc:title>DPMS Target Red Hat 7</dc:title>
            <dc:publisher>DISA</dc:publisher>
            <dc:type>DPMS Target</dc:type>
            <dc:subject>Red Hat 7</dc:subject>
            <dc:identifier>2777</dc:identifier>
        </reference>
        <ident system="http://iase.disa.mil/cci">CCI-000205</ident>
    <fixtext fixref="F-78287rl_fix">Configure operating system to enforce a minimum 15-character password length.
    Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):
    minlen = 15</fixtext>
    <fix id="F-78287rl_fix" />
    <check system="C-72167rl_chk">
        <check-content-ref name="M" href="DPMS_XCCDF_Benchmark_RHEL_7_STIG.xml" />
        <check-content>Verify the operating system enforces a minimum 15-character password length. The "minlen" option sets the minimum number of characters in a new password.
    <check>
        <check-content>Check for the value of the "minlen" option in "/etc/security/pwquality.conf" with the following command:
        # grep minlen /etc/security/pwquality.conf
        minlen = 15
    <check>
        If the command does not return a "minlen" value of 15 or greater, this is a finding.</check-content>
    </check>
    </Rule>
</Group>
```

DISA STIG authors associate each requirement/test

(STIG in XML form found in the ZIP download file: [U Red Hat Enterprise Linux 7 STIG V1R4 Manual-xccdf.xml](#))

CCIs are DISA's Control Correlation Identifiers

The screenshot shows a web browser window displaying the 'Control Correlation Identifier (CCI)' page. The URL in the address bar is <https://public.cyber.mil/stigs/cci/>. The page header includes the 'DoD CYBER EXCHANGE PUBLIC' logo and navigation links for Topics, Training, PKI/PKE, SRGs/STIGs, Resources, and Help. A search bar and a 'Login with CAC' button are also present.

The main content area features a large banner with the title 'Control Correlation Identifier (CCI)'. Below the banner, the breadcrumb navigation shows Home > Security Technical Implementation Guides (STIGs) > Control Correlation Identifier (CCI). The left sidebar contains links for SRG/STIGs Home, Control Correlation Identifier (CCI), Document Library, DoD Annex for NIAP Protection Profiles, DoD Cloud Computing Security, Frequently Asked Questions – FAQs, Group Policy Objects, Quarterly Release Schedule and Summary. The 'Control Correlation Identifier (CCI)' link is highlighted with a red box. The 'CCI DOWNLOADS' section displays a table with three rows:

TITLE	SIZE	UPDATED
CCI List	133.52 KB	02 Feb 2017
CCI Process	37.09 KB	28 Feb 2011
CCI Specification	112.14 KB	01 May 2014

The 'CCI List' file is also highlighted with a red box.

<https://public.cyber.mil/stigs/cci/>

Each CCI maps to one or more NIST SP 800-53 Controls

C:\Users\earonne\Desktop\CMS\STIG\U_CCI_List\U_CCI_List.xml Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

U_Red_Hat_Enterprise_Linux_7_STIG_V1R4_Manual-xccdf.xml U_CCI_List.xml

```

5998 <references>
5999   <reference creator="NIST" title="NIST SP 800-53" version="3" location="http://csrc.nist.gov/publications/PubsSPs.html" index=
6000     "IA-5 (7) " />
6001   <reference creator="NIST" title="NIST SP 800-53A" version="1" location="http://csrc.nist.gov/publications/PubsSPs.html" index=
6002     "IA-5 (7).1" />
6003   <reference creator="NIST" title="NIST SP 800-53 Revision 4" version="4" location="http://csrc.nist.gov/publications/PubsSPs.html"
6004     index="IA-5 (7)" />
6005   </references>
6006 </cci_item>
6007 <cci_item id="CCI-000205">
6008   <status>draft</status>
6009   <publishdate>2009-05-22</publishdate>
6010   <contributor>DISA FSO</contributor>
6011   <definition>The information system enforces minimum password length.</definition>
6012   <type>technical</type>
6013   <parameter>Number of Characters</parameter>
6014   <references>
6015     <reference creator="NIST" title="NIST SP 800-53" version="3" location="http://csrc.nist.gov/publications/PubsSPs.html" index=
6016       "IA-5 (1) (a)" />
6017     <reference creator="NIST" title="NIST SP 800-53A" version="1" location="http://csrc.nist.gov/publications/PubsSPs.html" index=
6018       "IA-5 (1).1 (i)" />
6019     <reference creator="NIST" title="NIST SP 800-53 Revision 4" version="4" location="http://csrc.nist.gov/publications/PubsSPs.html"
6020       index="IA-5 (1) (a)" />
6021   </references>
6022 </cci_item>
6023 <cci_item id="CCI-001544">
6024   <status>draft</status>
6025   <publishdate>2009-11-30</publishdate>
6026   <contributor>DISA FSO</contributor>
   <definition>The organization manages information system authenticators by ensuring that authenticators have sufficient strength of
   mechanism for their intended use.</definition>
   <type>policy</type>
   <references>
     <reference creator="NIST" title="NIST SP 800-53" version="3" location="http://csrc.nist.gov/publications/PubsSPs.html" index=
       "IA-5 c" />
     <reference creator="NIST" title="NIST SP 800-53A" version="1" location="http://csrc.nist.gov/publications/PubsSPs.html" index=
       "IA-5.1 (ii)" />
     <reference creator="NIST" title="NIST SP 800-53 Revision 4" version="4" location="http://csrc.nist.gov/publications/PubsSPs.html"
       ...
   </references>

```

CCI-000205 is associated with...

...IA-5 (1) NIST SP 800-53 Security Control (Enhancement)

eXtensible Markup Language file length : 2,376,818 lines : 38,403 Ln : 6,004 Col : 34 Sel : 0 | 0 Windows (CR LF) UTF-8-BOM IN

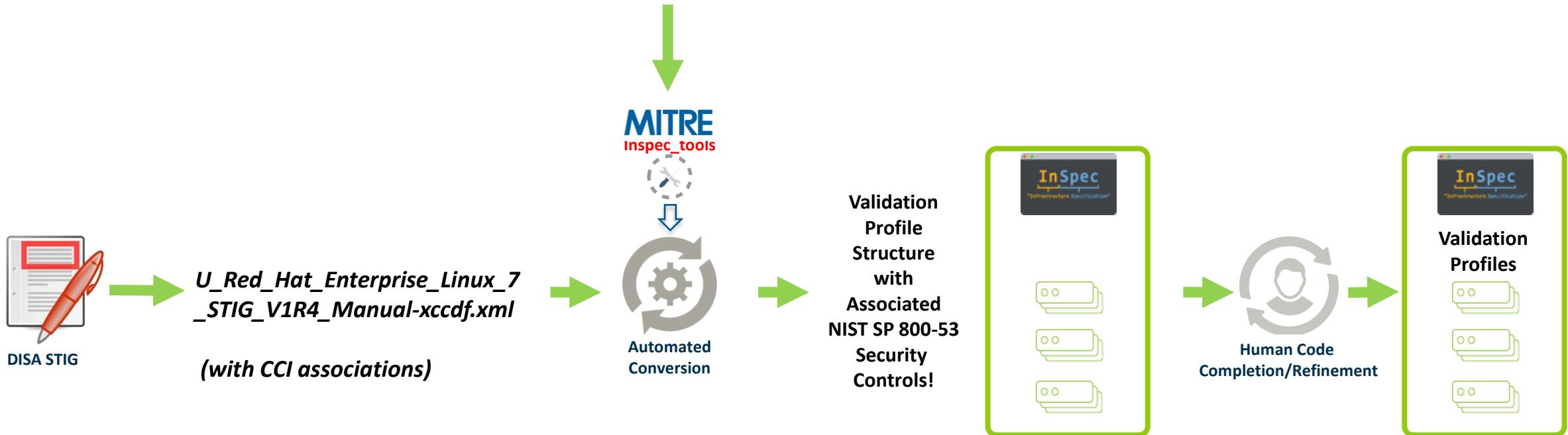
(CCI list in XML form found in the ZIP download file: U_CCI_List.xml)

MITRE's InSpec_tools Generates the STIG InSpec Profile Structure

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/u_cci_list.zip

DISA's U_CCI_List.xml
(map of CCIs to NIST)

https://github.com/mitre/inspec_tools/blob/master/lib/data/U_CCI_List.xml



<https://inspec-tools.mitre.org/>

One of 200+ requirements from the RHEL7 STIG in InSpec Profile Code:

The unique STIG V-number,
title,

CCI,
and associated
NIST SP 800-53 Security Control
are included in the InSpec profile structure!

```
control "V-71935" do
  title "Passwords must be a minimum of 15 characters in length."
  desc "
    The shorter the password, the lower the number of possible combinations
    that need to be tested before the password is compromised.

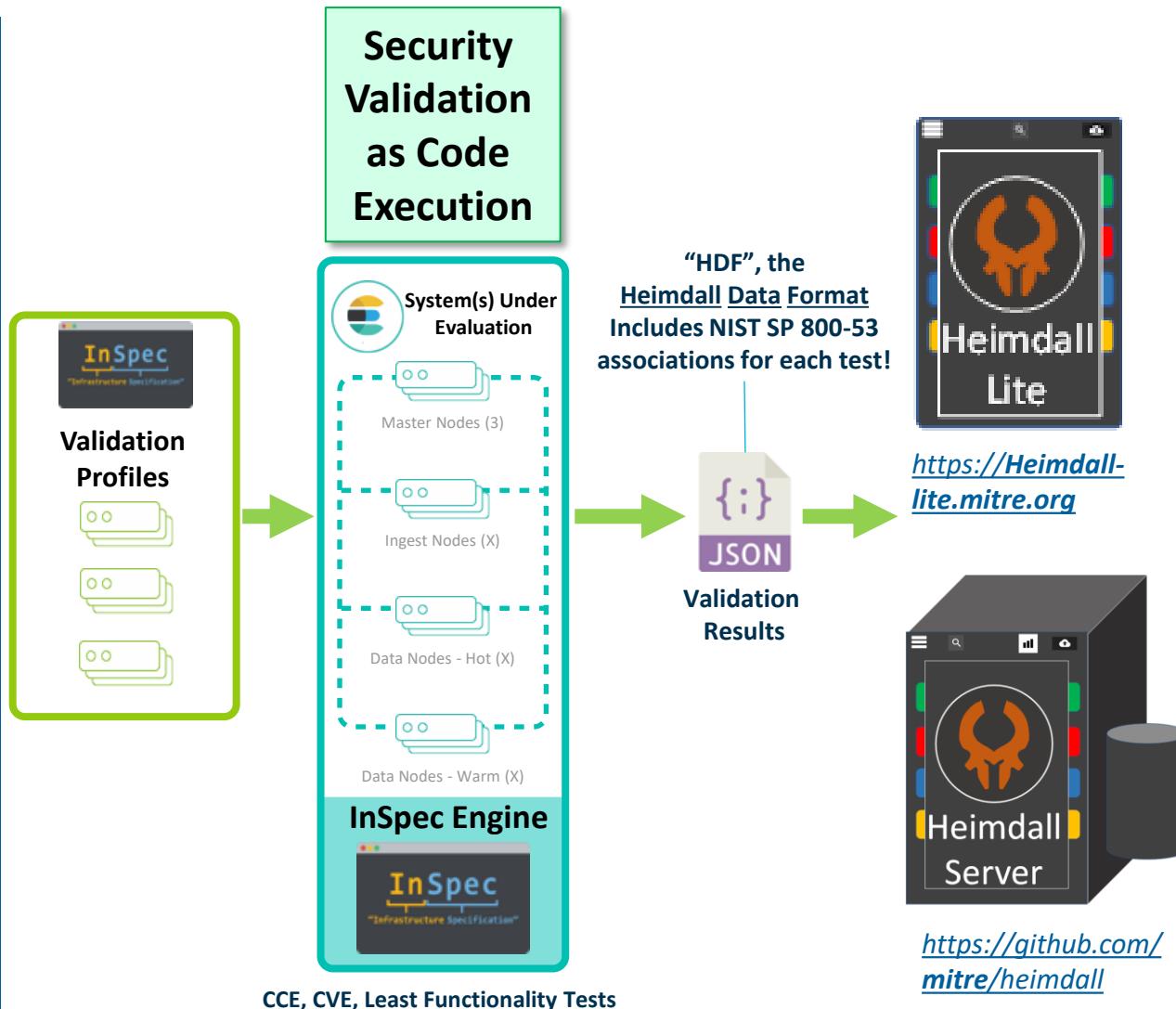
    Password complexity, or strength, is a measure of the effectiveness of a
    password in resisting attempts at guessing and brute-force attacks. Password
    length is one factor of several that helps to determine strength and how long
    it takes to crack a password. Use of more characters in a password helps to
    exponentially increase the time and/or resources required to compromise the
    password.

    "
  impact 0.5
  tag "gttitle": "SRG-OS-000078-GPOS-00046"
  tag "gid": "V-71935"
  tag "rid": "SV-86559r1_rule"
  tag "stig_id": "RHEL-07-010280"
  tag "cci": ["CCI-000205"]
  tag "documentable": false
  tag "nist": ["IA-5 (1) (a)", "Rev_4"]
  tag "subsystems": ['pam', 'pwquality', 'password']
  desc "check", "Verify the operating system enforces a minimum 15-character
    password length. The \"minlen\" option sets the minimum number of characters in
    a new password.

    Check for the value of the \"minlen\" option in
```

As well as all other original
information from the STIG
such as impact (i.e., CAT),
check, and fix instructions

When STIG InSpec Profiles are run, test results and the InSpec code are included in the JSON validation results file, and viewable in MITRE's Heimdall



The screenshot shows the **heimdall-lite 2** browser window displaying the heimdall-lite.mitre.org/#/results/1 page. The search bar contains the ID **71935**. The results table shows a single entry:

Severity	Control	Title	Desc	Severity
Failed	V-71935	Passwords must be a minimum of 15 characters in length.	The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.	MEDIUM

The right side of the interface shows detailed information for the control V-71935, including:

- Code:** IA-5 (1) (a), Rev_4
- Control:** V-71935
- Title:** Passwords must be a minimum of 15 characters in length.
- Desc:** The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.
- Severity:** MEDIUM

The bottom of the page includes the copyright notice: **The MITRE Corporation © 2019**.

When STIG InSpec Profiles are run, test results and the InSpec code are included in the JSON validation results file, and viewable in MITRE's Heimdall

The screenshot shows the Heimdall web interface with the URL heimdall-lite.mitre.org/#/results/2. The search bar contains "71935". The main area displays a failed test result for control V-71935:

- Severity:** Failed
- Message:** Passwords must be a minimum of 15 characters in length.
- Control ID:** V-71935
- Tags:** IA-5 (1) (a), Rev_4
- Metric:** MEDIUM
- Test Status:** FAILED
- Description:** One or more of the automated tests failed or was inconclusive for the control:
The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised. Password complexity, or strength, is a measure of the effectiveness of a password.
- Test Details:**

Test	Result
Parse /etc/security/pwquality.conf minlen.to_i should cmp >= 15	expected it to be >= 15 got: 0 (compared using `cmp` matcher)

The screenshot shows the Heimdall web interface with the URL heimdall-lite.mitre.org/#/results/1. The search bar contains "71935". The main area displays the InSpec code for control V-71935, which is highlighted with a red box:

```

control "V-71935" do
  title "Passwords must be a minimum of 15 characters in length."
  desc "
    The shorter the password, the lower the number of possible combinations
    that need to be tested before the password is compromised.

    Password complexity, or strength, is a measure of the effectiveness of a
    password in resisting attempts at guessing and brute-force attacks. Password
    length is one factor of several that helps to determine strength and how long
    it takes to crack a password. Use of more characters in a password helps to
    exponentially increase the time and/or resources required to compromise the
    password.
  "
  impact 0.5
  tag "gtitle": "SRG-OS-000078-GPOS-00046"
  tag "gid": "V-71935"
  tag "rid": "SV-86559r1_rule"
  tag "stig_id": "RHEL-07-010280"
  tag "cci": ["CCI-000205"]
  tag "documentable": false
  tag "nist": ["IA-5 (1) (a)", "Rev_4"]
  tag "subsystems": ['pam', 'pwquality', 'password']
  desc "check", "Verify the operating system enforces a minimum 15-character
    password length. The \"minlen\" option sets the minimum number of characters in
    a new password.

    Check for the value of the \"minlen\" option in
    \"(/etc/security/pwquality.conf)\" with the following command."

```

STIG InSpec Profile Validation Results JSON Heimdall Data Format (HDF) Sample:

```
{
  "id": "V-71935",
  "title": "Passwords must be a minimum of 15 characters in length.",
  "desc": "The shorter the password, the lower the number of possible combinations\nthat need to be tested before the password is compromised.\n\n",
  "descriptions": [
    {
      "label": "default",
      "data": "The shorter the password, the lower the number of possible combinations\nthat need to be tested before the password is compromised."
    },
    {
      "label": "check",
      "data": "Verify the operating system enforces a minimum 15-character\npassword length. The \"minlen\" option sets the minimum number of characters required for a password to be considered valid. This check will fail if the minlen value is less than 15. You can verify this by running the command 'grep minlen /etc/security/pwquality.conf'. If the value is less than 15, you will need to increase it to 15 or higher. You can do this by adding or modifying the 'minlen' option in the /etc/security/pwquality.conf file. For example, you can add 'minlen=15' to the file. Once you have made the change, run the 'inspec test V-71935' command again to see if the check passes."
    },
    {
      "label": "fix",
      "data": "Configure operating system to enforce a minimum 15-character\npassword length.\n\nAdd the following line to \"/etc/security/pwquality.conf\":\nminlen=15"
    }
  ],
  "impact": 0.5,
  "refs": [],
  "tags": {
    "gttitle": "SRG-OS-000078-GPOS-00046",
    "gid": "V-71935",
    "rid": "SV-86559r1_rule",
    "stig_id": "RHEL-07-010280",
    "cci": [
      "CCI-000205"
    ],
    "documentable": false,
    "nist": [
      "IA-5 (1) (a)",
      "Rev_4"
    ],
    "subsystems": [
      "pam",
      "pwquality",
      "password"
    ],
    "fix_id": "F-78287r1_fix"
  },
  "code": "control \'V-71935\' do\n  title \'Passwords must be a minimum of 15 characters in length.\'\n  desc  \'The shorter the password, the lower the number of possible combinations\nthat need to be tested before the password is compromised.\'\n  source_location:\n    line: 10,\n    ref: \"inspec-profile-disa_stig-el7-master/controls/V-71935.rb\"\n",
  "results": [
    {
      "status": "failed",
      "code_desc": "Parse Config File /etc/security/pwquality.conf minlen.to_i should cmp >= 15",
      "run_time": 0.000149026,
      "start_time": "2019-11-04T16:17:07-05:00",
      "message": "\nexpected it to be >= 15\n      got: 0\n\n(compared using `cmp` matcher)\n"
    }
  ]
}
```

Use Case 2 of 3: CIS Benchmark to InSpec Profile (with NIST SP 800-53)



CIS Benchmarks

CIS Benchmark Source

The screenshot shows the CIS Benchmarks website at cisecurity.org/cis-benchmarks/. The page displays various CIS Benchmark categories and specific benchmarks for Amazon Web Services and Apache software.

Operating Systems: Linux

Cloud Providers: Amazon Web Services (AWS)

Benchmarks for AWS:

- CIS Benchmarks for Amazon Web Services Foundations:**
 - 1.2.0 (Green dot, latest version)
 - [Download](#)
 - 1.1.0 (Black dot, older version)
 - [Download](#)
 - 1.0.0 (Black dot, older version)
 - [Download](#)

CIS-CAT Pro: CIS SecureSuite Members Only

Build Kit: CIS SecureSuite Members Only

CIS-CAT Lite: Free Download

CIS Hardened Image: By Server Hour

Legend:

 - Green dot: Indicates the most recent version of a CIS Benchmark.
 - Black dot: Indicates older content still available for download.

Feedback: A yellow button in the bottom right corner.

<https://www.cisecurity.org/cis-benchmarks/>

MITRE

Example: An AWS CIS Foundations Benchmark Test:

1.9 Ensure IAM password policy requires minimum length of 14 or greater (Scored)

Profile Applicability:

- Level 1

“1.9” is the ID for this requirement/test

Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure password are at least a given length. It is recommended that the password policy require a minimum password length 14.

Rationale:

Setting a password complexity policy increases account resiliency against brute force login attempts.

Audit:

Perform the following to ensure the password policy is configured as prescribed:

Via AWS Console

1. Login to AWS Console (with appropriate permissions to View Identity Access Management Account Settings)
2. Go to IAM Service on the AWS Console
3. Click on Account Settings on the Left Pane
4. Ensure "Minimum password length" is set to 14 or greater.

Via CLI

```
aws iam get-account-password-policy
```

Ensure the output of the above command includes "MinimumPasswordLength": 14 (or higher)

Remediation:

Perform the following to set the password policy as prescribed:

Via AWS Console

1. Login to AWS Console (with appropriate permissions to View Identity Access Management Account Settings)
2. Go to IAM Service on the AWS Console
3. Click on Account Settings on the Left Pane

27 | Page

CIS authors associate each requirement/test to a CIS Control

4. Set "Minimum password length" to 14 or greater.
5. Click "Apply password policy"

Via CLI

```
aws iam update-account-password-policy --minimum-password-length 14
```

Note: All commands starting with "aws iam update-account-password-policy" can be combined into a single command.

References:

1. CCE-78907-3
2. CIS CSC v6.0 #5.7, #16.12

CIS Controls:

16 [Account Monitoring and Control](#)

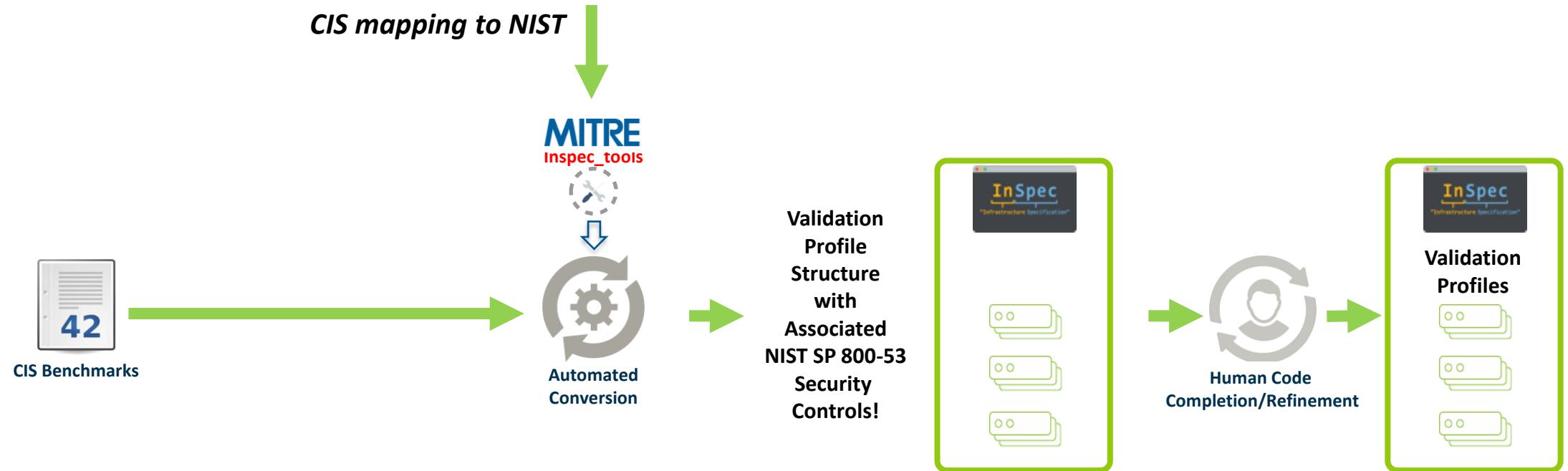
Account Monitoring and Control

In InSpec_tools, we Mapped CIS Controls to NIST Controls

NIST SP 800-53 Control #	NIST SP 800-53 Control Title	Family	Control	The Center for Internet Security Critical Security Controls Version 6.1
CA-7	CONTINUOUS MONITORING	System	4.8	Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.
AC-6	LEAST PRIVILEGE	Critical Security Control #5: Controlled Use of Administrative Privileges		
AC-6 (9)	LEAST PRIVILEGE AUDITING USE OF PRIVILEGED FUNCTIONS	System	5.1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.
AC-6 (7)	LEAST PRIVILEGE REVIEW OF USER PRIVILEGES	System	5.2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.
IA-5 (5)	AUTHENTICATOR MANAGEMENT CHANGE AUTHENTICATORS PRIOR TO DELIVERY	System	5.3	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.
AC-2 (4)	ACCOUNT MANAGEMENT AUTOMATED AUDIT ACTIONS	System	5.4	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.
AU-2	AUDIT EVENTS	System	5.5	Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.
IA-2 (1)	IDENTIFICATION AND AUTHENTICATION NETWORK ACCESS TO PRIVILEGED ACCOUNTS	System	5.6	Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.
IA-5 (1)	AUTHENTICATOR MANAGEMENT PASSWORD-BASED AUTHENTICATION	System	5.7	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).
IA-5 (8)	AUTHENTICATOR MANAGEMENT MULTIPLE INFORMATION SYSTEM ACCOUNTS	System	5.8	Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as the Windows Runas command or the sudo command.

MITRE's InSpec_tools Generates the CIS InSpec Profile Structure

https://github.com/mitre/inspec_tools/blob/master/lib/data/NIST_Map_092_12017B_CSC-CIS_Critical_Security_Controls_VER_6.1_E Excel 9.1.2016.xlsx



One of the AWS CIS Foundations Benchmark tests in InSpec Profile Code:

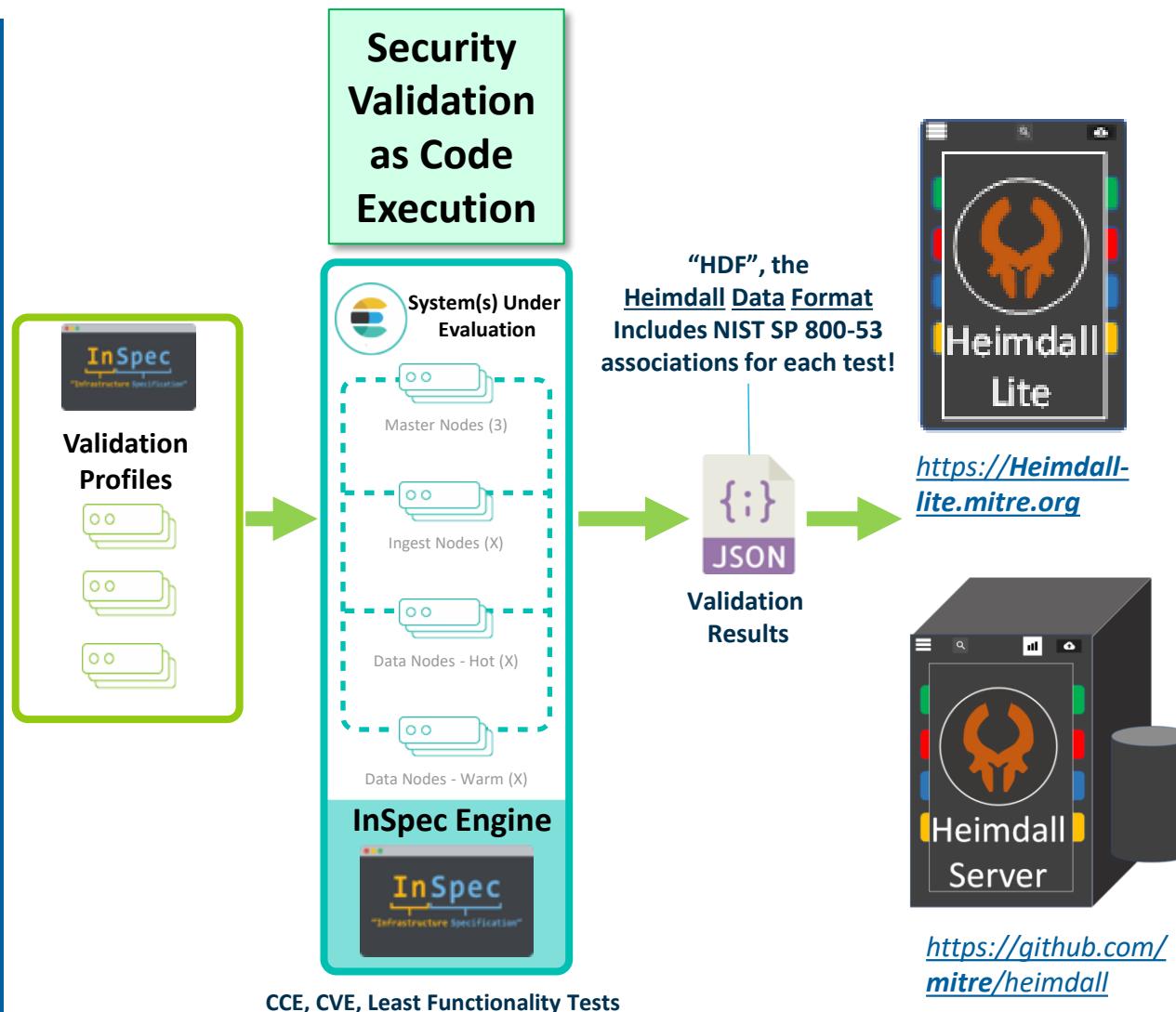
The unique CIS benchmark test number,
title,

CIS Control,
and associated
NIST SP 800-53 Security Control
are included in the InSpec profile structure!

```
control 'cis-aws-foundations-1.9' do
  title "Ensure IAM password policy requires minimum length of #{pwd_length} or greater"
  desc "Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure password are at least a given length. It is recommended that the password policy require a minimum password length #{pwd_length}."
  impact 0.3
  tag "rationale": "Setting a password complexity policy increases account resiliency against brute force login attempts."
  tag "cis_impact": ''
  tag "cis_rid": '1.9'
  tag "cis_level": 1
  tag "csc_control": [['5.7', '16.12'], '6.0']
  tag "nist": ['IA-5(1)', 'IA-2', 'Rev_4']
  tag "cce_id": 'CCE-78907-3'
  tag "check": "Perform the following to ensure the password policy is configured as prescribed:
    'Via AWS Console
      * Login to AWS Console (with appropriate Management Account Settings)
      * Go to IAM Service on the AWS Console
      * Click on Account Settings on the Left Pane
      * Ensure 'Minimum password length' is set to #{pwd_length} or greater.

As well as all other original information from the CIS benchmark such as the check (CIS audit) and fix (CIS remediation) instructions
```

When CIS InSpec Profiles are run, test results and the InSpec code are included in the JSON validation results file, and viewable in MITRE's Heimdall



heidm-all-lite 2

heidm-all-lite.mitre.org/#/results/1

Status: Passed

Title: Ensure IAM password policy requires minimum length of 14 or greater

Severity: LOW

TEST DETAILS CODE

Control: cis-aws-foundations-1.9

Title: Ensure IAM password policy requires minimum length of 14 or greater

Desc: Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure password are at least a given length. It is recommended that the password policy require a minimum password length 14.

The MITRE Corporation © 2019

A red box highlights the **Details** section of the validation result, which includes the control ID (cis-aws-foundations-1.9), title, and description.

When CIS InSpec Profiles are run, test results and the InSpec code are included in the JSON validation results file, and viewable in MITRE's Heimdall

The screenshot shows a web browser window for 'heimdall-lite 2' at the URL 'heimdall-lite.mitre.org/#/results/1'. The interface has a dark theme with various filters and search bars at the top. Below the header, there are sections for 'Status', 'Title', 'ID', 'Severity', and 'Tags'. A prominent green box indicates a 'Passed' status for the control 'Ensure IAM password policy requires minimum length of 14 or greater'. This control is associated with the ID 'cis-aws-foundations-1.9', severity 'LOW', and tags 'IA-5(1)', 'IA-2', and 'Rev_4'. The 'TEST' tab is selected, showing the message 'All Automated tests passed for the control:' followed by a summary about IAM password policies. A large green bar at the bottom displays the word 'PASSED'. A red box highlights the 'Test' section, which contains the command 'IAM Password-Policy minimum_password_length should cmp >= 14'.

Passed

Ensure IAM password policy requires minimum length of 14 or greater

cis-aws-foundations-1.9

IA-5(1) IA-2

Rev_4

TEST DETAILS CODE

All Automated tests passed for the control:

Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure password are at least a given length. It is recommended that the password po... +

PASSED

Test

IAM Password-Policy minimum_password_length should cmp >= 14

```
=====
# Profile name: cis-aws-foundations-baseline
=====

control "cis-aws-foundations-1.9" do
  title "Ensure IAM password policy requires minimum length of #{PWD_LENGTH} or greater"
  desc "Password policies are, in part, used to enforce password complexity requirements. IAM password policies can be used to ensure password are at least a given length. It is recommended that the password policy require a minimum password length #{PWD_LENGTH}."
  impact 0.3
  tag "rationale": "Setting a password complexity policy increases account resiliency against brute force login attempts."
  tag "cis_impact": ''
  tag "cis_rid": "1.9"
  tag "cis_level": 1
  tag "csc_control": [[{"version": "5.7"}, {"version": "16.12"}, {"version": "6.0"}]]
  tag "nist": ["IA-5(1)", "IA-2", "Rev_4"]
  tag "cce_id": "CCE-78907-3"
  tag "check": "Perform the following to ensure the password policy is configured as prescribed:

'Via AWS Console

* Login to AWS Console (with appropriate permissions to View Identity Access Management Account Settings)
```

CIS InSpec Profile Validation Results JSON Heimdall Data Format (HDF) Sample:

```
{
  "id": "cis-aws-foundations-1.9",
  "title": "Ensure IAM password policy requires minimum length of 14 or greater",
  "desc": "Password policies are, in part, used to enforce password complexity\\nrequirements. IAM password policies can be",
  "descriptions": [
    {
      "label": "default",
      "data": "Password policies are, in part, used to enforce password complexity\\nrequirements. IAM password policies"
    }
  ],
  "impact": 0.3,
  "refs": [],
  "tags": {
    "rationale": "Setting a password complexity policy increases account\\nresiliency against brute force login attempts."
    "cis_impact": "",
    "cis_rid": "1.9",
    "cis_level": 1,
    "csc_control": [
      [
        "5.7",
        "16.12"
      ],
      "6.0"
    ]
  },
  "nist": [
    "IA-5(1)",
    "IA-2",
    "Rev_4"
  ],
  "cce_id": "CCE-78907-3",
  "check": "Perform the following to ensure the password policy is\\nconfigured as prescribed:\\n\\n'Via AWS Console\\n\\n*",
  "fix": "Perform the following to set the password policy as prescribed:\\n\\n'Via AWS Console\\n\\n* Login to AWS Console",
  "code": "control \\"cis-aws-foundations-1.9\\" do\\n  title \\\"Ensure IAM password policy requires minimum length of #{PWD_LENGTH}\\\"",
  "source_location": {
    "line": 3,
    "ref": "./controls/cis-aws-foundations-1.9.rb"
  },
  "results": [
    {
      "status": "passed",
      "code_desc": "IAM Password-Policy minimum_password_length should cmp >= 14",
      "run_time": 0.000143,
      "start_time": "2018-11-18T20:21:40-05:00"
    }
  ]
},
```



Use Case 3 of 3: Vendor Guidance to InSpec Profile (with NIST SP 800-53)

Some InSpec Profiles are based on Vendor Guidance, when neither STIGs nor CIS Benchmarks are available. For example:

CMS
ARS 3.1:

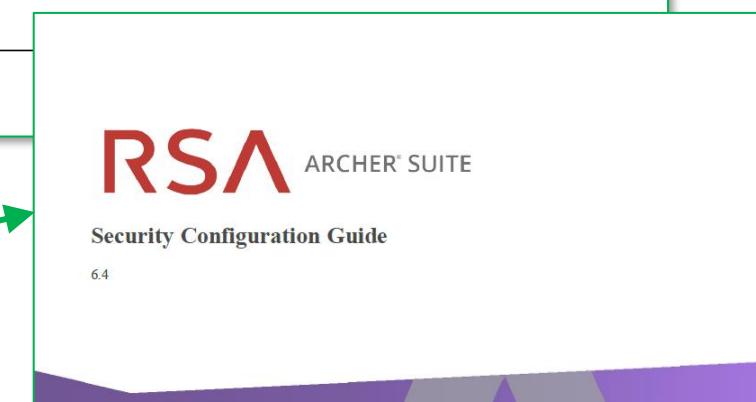
CM-6	Configuration Settings (High, Moderate, Low)	P1
Control:	<p>The organization:</p> <ul style="list-style-type: none"> a. Establishes and documents configuration settings for information technology products employed within the information system using the latest security baseline configurations established by the HHS, U.S. Government Configuration Baselines (USGCB), and the National Checklist Program (NCP) defined by NIST SP 800-70 Rev. 2 (refer to Implementation Standard 1 for specifics) that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for individual components within the information system based on explicit operational requirements (defined in the applicable system security plan); and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. <p>Implementation Standards:</p> <p>High, Moderate, & Low:</p> <p>Std.1 - Use of HHS and CMS approved Operating System (OS)</p> <ul style="list-style-type: none"> (a) HHS-specific minimum security configurations must be used for the following OS and Applications: <ul style="list-style-type: none"> 1. HHS approved USGCB Windows Standards (e.g., Microsoft supported versions only); and 2. Blackberry Server - Websense. (b) For all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing security configuration guidelines is: <ol style="list-style-type: none"> 1. USGCB; 2. NIST NCP; Tier IV, then Tier III, Tier II, and Tier I, in descending order; 3. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG); 4. National Security Agency (NSA) STIGs; 5. If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group (such as The Center for Internet Security [CIS]) checklists. 	

CMS Acceptable Risk Safeguards (ARS)
Document Number: CMS_CIO-STD-SEC01-3.1

1st choice: STIG, but none available for RSA Archer

2nd choice: CIS, but none available for RSA Archer

3rd choice: Vendor checklist/guidance – which RSA has!



Example items to be tested with InSpec Profile

The screenshot shows a section from the RSA ARCHER® SUITE Security Configuration Guide. The title of the page is "6.4 Password Strength". The main content is a table titled "The following table shows the default security parameters settings for password strength." The table has two columns: "Parameter" and "Setting". The parameters listed are Minimum password length, Alpha characters required, Numeric characters required, Special characters required, Uppercase characters required, Lowercase characters required, Password change interval, Previous passwords disallowed, Grace logons, Maximum failed logon attempts, Session time-out, and Account lockout period. The settings are 9 characters, 2 characters, 1 character, 1 character, 1 character, 1 character, 90 days, 20 passwords, 0 logon, 3 attempts, 10 minutes (sysadmin account), 10 minutes (user account), 30 minutes (service account), and 999 days respectively.

Parameter	Setting
Minimum password length	9 characters
Alpha characters required	2 characters
Numeric characters required	1 character
Special characters required	1 character
Uppercase characters required	1 character
Lowercase characters required	1 character
Password change interval	90 days
Previous passwords disallowed	20 passwords
Grace logons	0 logon
Maximum failed logon attempts	3 attempts
Session time-out	10 minutes (sysadmin account) 10 minutes (user account) 30 minutes (service account)
Account lockout period	999 days

12 individual tests

Identifying Transport(s) & targets within component to query for tests



RESTful API Reference Guide

6.4

Get all security parameters

The Get all security parameters resource retrieves all security parameters for the current RSA Archer instance.

Request

```
POST http://RsaArcher/api/core/system/securityparameter
```

Request Header

```
Accept: application/json, text/html, application/xhtml+xml, application/xml;q=0.9,*/*;q=0.8
```

```
Authorization: Archer session-id="SessionToken"
```

```
Content-Type: application/json
```

```
X-Http-Method-Override: GET
```

```
{
...
...
{
  "Name": "Test Security Param",
  "Description": "test sec",
  "MinPasswordLength": 9,
  "AlphaCharsRequired": 2,
  "NumericCharsRequired": 1,
  "UppercaseCharsRequired": 1,
  "LowercaseCharsRequired": 1,
  "SpecialCharsRequired": 1,
  "PasswordChangeInterval": 90,
  "GraceLogins": 0,
  "MaximumFailedLoginAttempts": 3,
  "PreviousPasswordsDisallowed": 20,
  "LockoutPeriod": 999,
  "SessionTimeout": 10,
  ...
}
}
```

(API Response example)

The following table shows the default security par...

Parameter	Setting
Minimum password length	9 characters
Alpha characters required	2 characters
Numeric characters required	1 character
Special characters required	1 character
Uppercase characters required	1 character
Lowercase characters required	1 character
Password change interval	90 days
Previous passwords disallowed	20 passwords
Grace logons	0 logon
Maximum failed logon attempts	3 attempts
Session time-out	10 minutes (sys)
	10 minutes (use)
	30 minutes (ser)
Account lockout period	999 days

Defining Default title, description, check text, fix text, NIST SP 800-53 control (use for baseline* InSpec Profile)

Rule/Test #	Title	Description	Check Text	Fix Text	NIST SP 800-53 Control
rsa-archer-1.1	Minimum Password Length	Passwords must be a minimum of 9 characters in length.	In security parameters, check if MinPasswordLength = 9	In security parameters, set MinPasswordLength = 9	IA-5(1)
rsa-archer-1.2	Alpha characters required	When passwords are changed or new passwords are established, the new password must contain at least two alpha characters.	In security parameters, check if AlphaCharsRequired = 2	In security parameters, set AlphaCharsRequired = 2	IA-5(1)
rsa-archer-1.3	Numeric characters required	When passwords are changed or new passwords are established, the new password must contain at least one numeric character.	In security parameters, check if NumericCharsRequired = 1	In security parameters, set NumericCharsRequired = 1	IA-5(1)
rsa-archer-1.4	Special characters required	When passwords are changed or new passwords are established, the new password must contain at least one special character.	In security parameters, check if SpecialCharsRequired = 1	In security parameters, set SpecialCharsRequired = 1	IA-5(1)
rsa-archer-1.5	Uppercase characters required	When passwords are changed or new passwords are established, the new password must contain at least one uppercase character.	In security parameters, check if UppercaseCharsRequired = 1	In security parameters, set UppercaseCharsRequired = 1	IA-5(1)
rsa-archer-1.6	Lowercase characters require	When passwords are changed or new passwords are assigned, the new password must contain at least one lowercase character.	In security parameters, check if LowercaseCharsRequired = 1	In security parameters, set LowercaseCharsRequired = 1	IA-5(1)
rsa-archer-1.7	Password change interval	Existing passwords must be restricted to a 90-day maximum lifetime.	In security parameters, check if PasswordChangeInterval = 90	In security parameters, set PasswordChangeInterval = 90	IA-5(1)
rsa-archer-1.8	Previous passwords disallowed	Passwords must be prohibited from reuse for a minimum of 20 generations.	In security parameters, check if PreviousPasswordsDisallowed = 20	In security parameters, set PreviousPasswordsDisallowed = 20	IA-5(1)
rsa-archer-1.9	Grace logons	After password expiration, zero grace logons are permitted using the expired password.	In security parameters, check if GraceLogins = 0	In security parameters, set GraceLogins = 0	IA-5(1)
rsa-archer-1.10	Maximum failed logon attempts	Accounts subject to 3 unsuccessful logon attempts must be locked.	In security parameters, check if MaximumFailedLoginAttempts = 3	In security parameters, set MaximumFailedLoginAttempts = 3	AC-7
rsa-archer-1.11	Session time-out	The operating system must initiate a session time-out after a 10 minute period of inactivity	In security parameters, check if SessionTimeout = 10	In security parameters, set SessionTimeout = 10	AC-11
rsa-archer-1.12	Account lockout period	Accounts locked due to unsuccessful logon attempts will stay locked until unlocked by an administrator.	In security parameters, check if LockoutPeriod = 999	In security parameters, set LockoutPeriod = 999	AC-7

Associated NIST SP 800-53 Security Controls are identified based on experienced security assessors familiar with the context of the tests.

Example of an InSpec Profile test based on Vendor Guidance

Unique test number,
title,

and associated
NIST SP 800-53 Security Control
are included in the InSpec profile
structure!

```
control 'rsa-archer-1.1' do
  title 'Minimum Password Length'
  desc 'Passwords must be a minimum of 9 characters in length.'
  impact 'medium'
  desc 'check', 'In security parameters, check if MinPasswordLength = 9.'
  desc 'fix', 'In security parameters, set MinPasswordLength = 9.'
  tag 'nist': ['IA-5(1)', 'Rev_4']

  archer_api_helper = archer(url: attribute('url'),
   instancetype: attribute('instancetype'),
    user_domain: attribute('user_domain'),
    username: attribute('username'),
    password: attribute('password'),
    ssl_verify: attribute('ssl_verify'))

  describe archer_api_helper do
    its('default_administrative_user.MinPasswordLength') { should cmp >= attribute('minimum_password_length') }
    its('general_user_parameter.MinPasswordLength') { should cmp >= attribute('minimum_password_length') }
    its('archer_services_parameter.MinPasswordLength') { should cmp >= attribute('minimum_password_length') }
  end
end
```

CMS ARS 3.1 title, description, check text, fix text, NIST SP 800-53 control (use for CMS overlay* InSpec Profile)

Rule/Test #	Title	Description	Check Text	Fix Text	NIST SP 800-53 Control
rsa-archer-1.1	Minimum Password Length	Passwords must be a minimum of 15 characters in length.	In security parameters, check if MinPasswordLength = 15	In security parameters, set MinPasswordLength = 15	IA-5(1)
rsa-archer-1.2	Alpha characters required	When passwords are changed or new passwords are established, the new password must contain at least one alpha characters.	In security parameters, check if AlphaCharsRequired = 1	In security parameters, set AlphaCharsRequired = 1	IA-5(1)
rsa-archer-1.3	Numeric characters required	When passwords are changed or new passwords are established, the new password must contain at least one numeric character.	In security parameters, check if NumericCharsRequired = 1	In security parameters, set NumericCharsRequired = 1	IA-5(1)
rsa-archer-1.4	Special characters required	When passwords are changed or new passwords are established, the new password must contain at least one special character.	In security parameters, check if SpecialCharsRequired = 1	In security parameters, set SpecialCharsRequired = 1	IA-5(1)
rsa-archer-1.5	Uppercase characters required	When passwords are changed or new passwords are established, the new password must contain at least one uppercase character.	In security parameters, check if UppercaseCharsRequired = 1	In security parameters, set UppercaseCharsRequired = 1	IA-5(1)
rsa-archer-1.6	Lowercase characters require	When passwords are changed or new passwords are assigned, the new password must contain at least one lowercase character.	In security parameters, check if LowercaseCharsRequired = 1	In security parameters, set LowercaseCharsRequired = 1	IA-5(1)
rsa-archer-1.7	Password change interval	Existing passwords must be restricted to a 60 -day maximum lifetime.	In security parameters, check if PasswordChangeInterval = 60	In security parameters, set PasswordChangeInterval = 60	IA-5(1)
rsa-archer-1.8	Previous passwords disallowed	Passwords must be prohibited from reuse for a minimum of 12 generations.	In security parameters, check if PreviousPasswordsDisallowed = 12	In security parameters, set PreviousPasswordsDisallowed = 12	IA-5(1)
rsa-archer-1.9	Grace logons	After password expiration, zero grace logons are permitted using the expired password.	In security parameters, check if GraceLogins = 0	In security parameters, set GraceLogins = 0	IA-5(1)
rsa-archer-1.10	Maximum failed logon attempts	Accounts subject to 3 unsuccessful logon attempts must be locked.	In security parameters, check if MaximumFailedLoginAttempts = 3	In security parameters, set MaximumFailedLoginAttempts = 3	AC-7
rsa-archer-1.11	Session time-out	The operating system must initiate a session time-out after a 15 minute period of inactivity	In security parameters, check if SessionTimeout = 15	In security parameters, set SessionTimeout = 15	AC-11
rsa-archer-1.12	Account lockout period	Accounts locked due to unsuccessful logon attempts will stay locked until unlocked by an administrator.	In security parameters, check if LockoutPeriod = 999	In security parameters, set LockoutPeriod = 999	AC-7

Non-InSpec Use Case: Using Heimdall_tools to Convert Other Security Data to Heimdall Data Format (HDF) (with NIST SP 800-53 associations)

“HDF”, the
Heimdall Data Format
Includes NIST SP 800-53
associations for each test!

Validation
Results



<https://heimdall-tools.mitre.org/>



sonarqube OWASP ZAP

Static & Dynamic Code Analysis

CWE Tests

Many Security Tools use other associations for their test results.

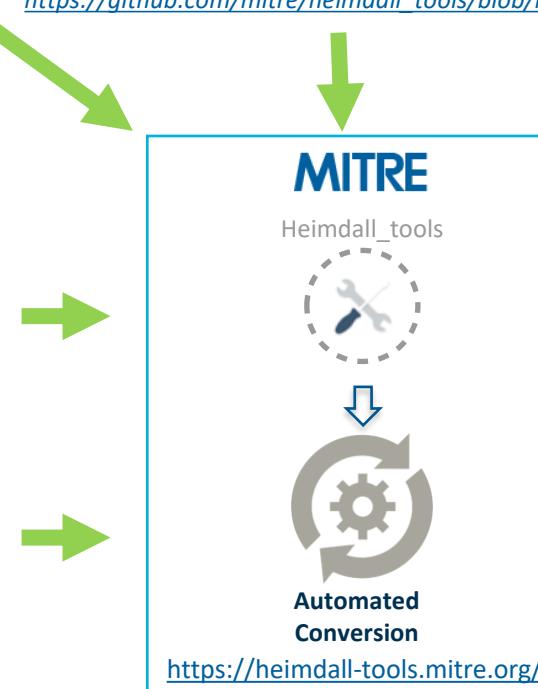
Heimdall_tools takes the native format, converts to Heimdall Data Format, and maps the native association to the NIST SP 800-53 Security Controls:

11 lines (11 sloc) 639 Bytes					
Raw Blame History					
Search this file...					
1	OWASP-ID	OWASP Name	NIST-ID	Rev	NIST Name
2	A1	Injection	SI-10	4	Information Input Validation
3	A2	Broken Authentication	SC-23	4	Session Authenticity
4	A3	Sensitive Data Exposure	SI-11	4	Error Handling
5	A4	XML External Entities (XXE)	SI-10	4	Information Input Validation
6	A5	Broken Access Control	AC-3	4	Access Enforcement
7	A6	Security Misconfiguration	CM-6	4	Configuration Settings
8	A7	Cross-Site Scripting (XSS)	SI-10	4	Information Input Validation
9	A8	Insecure Deserialization	SC-23	4	Session Authenticity
10	A9	Using Components with Known Vulnerabilities	SI-2	4	Flaw Remediation
11	A10	Insufficient Logging&Monitoring	AU-12	4	Audit Generation

https://github.com/mitre/heimdall_tools/blob/master/lib/data/owasp-nist-mapping.csv

195 lines (195 sloc) 14 KB					
Raw Blame History					
Search this file...					
1	CWE-ID	CWE Name	NIST-ID	Rev	NIST Name
2	5	J2EE Misconfiguration: Data Transmission Without Encryption	SC-8	4	Transmission Confidentiality and Integrity
3	6	J2EE Misconfiguration: Insufficient Session-ID Length	SC-23	4	Session Authenticity
4	7	J2EE Misconfiguration: Missing Custom Error Page	SI-11	4	Error Handling
5	8	J2EE Misconfiguration: Entity Bean Declared Remote	AC-3	4	Access Enforcement
6	9	J2EE Misconfiguration: Weak Access Permissions for EJB Methods	AC-3	4	Access Enforcement
7	11	ASP.NET Misconfiguration: Creating Debug Binary	SI-11	4	Error Handling
8	14	Compiler Removal of Code to Clear Buffers	SI-16	4	Memory Protection
9	15	External Control of System or Configuration Setting	SI-10	4	Information Input Validation
10	20	Improper Input Validation	SI-10	4	Information Input Validation
11	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	SI-10	4	Information Input Validation

https://github.com/mitre/heimdall_tools/blob/master/lib/data/cwe-nist-mapping.csv



"HDF", the Heimdall Data Format Includes NIST SP 800-53 associations for each test!

Validation Results

JSON



<https://Heimdall-lite.mitre.org>



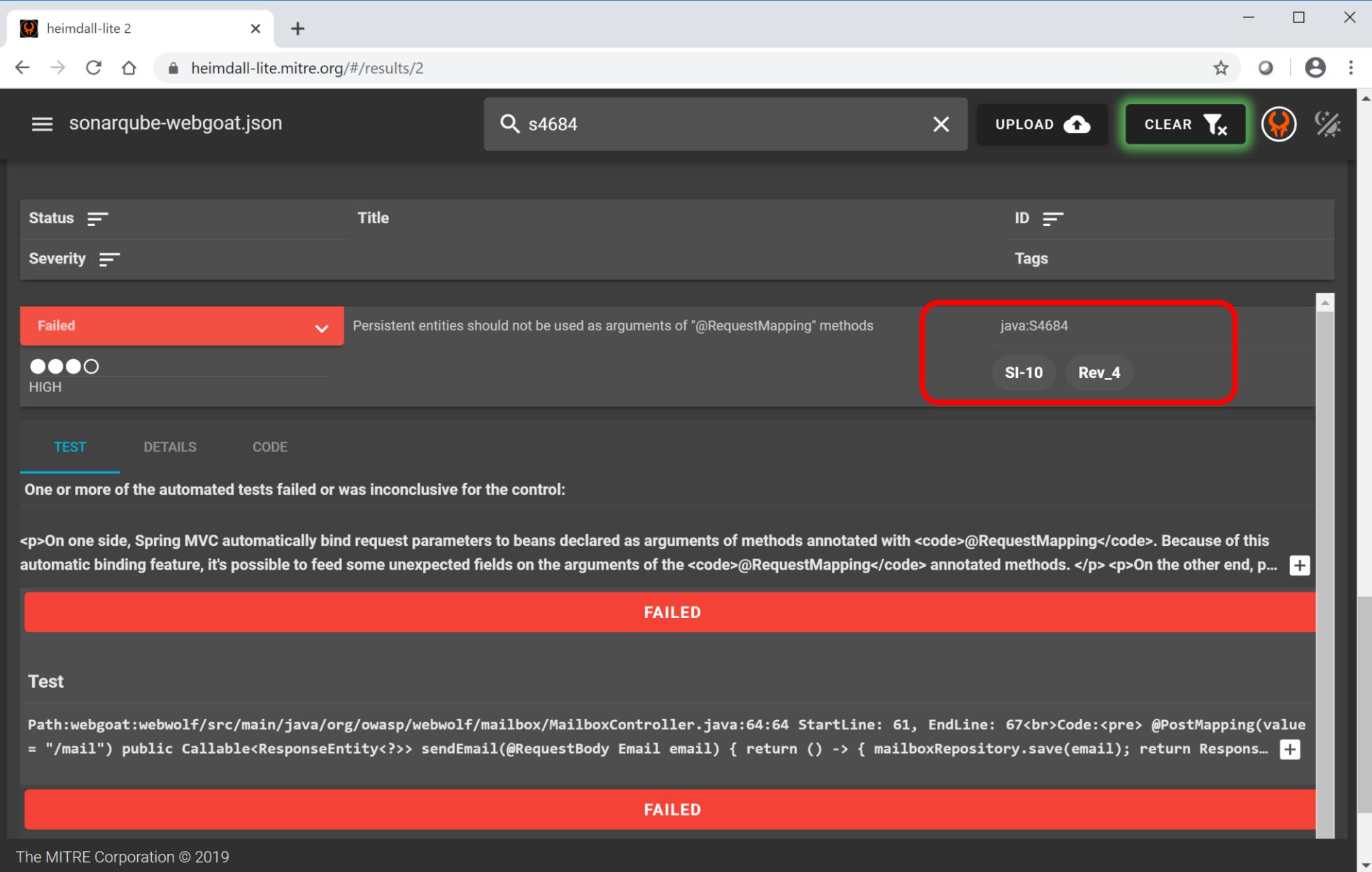
<https://github.com/mitre/heimdall>

MITRE

Sample SonarQube output in Heimdall Data Format (HDF), including NIST tag:

```
{  
    "title": "Persistent entities should not be used as arguments of \"@RequestMapping\" methods",  
    "desc": "<p>On one side, Spring MVC automatically bind request parameters to beans declared as arguments of methods  
    "impact": 0.7,  
    "tags": {  
        "nist": [  
            "SI-10",  
            "Rev 4"  
        ]  
    },  
    "results": [  
        {  
            "status": "failed",  
            "code_desc": "Path:webgoat:webwolf/src/main/java/org/owasp/webwolf/mailbox/MailboxController.java:64:64 Sta",  
            "run_time": 0.0,  
            "start_time": "Mon,09 Mar 2020 08:53:27"  
        },  
        {  
            "status": "failed",  
            "code_desc": "Path:webgoat:webgoat-lessons/missing-function-ac/src/main/java/org/owasp/webgoat/missing_ac/M",  
            "run_time": 0.0,  
            "start_time": "Mon,09 Mar 2020 08:53:27"  
        }  
    ],  
    "code": null,  
    "id": "java:S4684",  
    "descriptions": [],  
    "refs": [],  
    "source_location": {}  
},
```

Sample SonarQube output in Heimdall Data Format (HDF), viewed in Heimdall:



The screenshot shows the Heimdall web interface displaying SonarQube results for the file 'sonarqube-webgoat.json'. The search bar at the top contains the identifier 's4684'. The main view lists issues categorized by Status (Failed) and Severity (HIGH). One specific issue is highlighted with a red box and a green arrow pointing to it. This highlighted issue is identified as 'java:S4684' and is associated with 'SI-10' and 'Rev_4'. The interface also includes sections for TEST, DETAILS, and CODE, and provides a detailed description of the failing test case.

heidm-all-lite 2

heimdall-lite.mitre.org/#/results/2

sonarqube-webgoat.json

s4684

UPLOAD

CLEAR

Status

Severity

Title

ID

Tags

Failed

Persistent entities should not be used as arguments of "@RequestMapping" methods

HIGH

TEST DETAILS CODE

One or more of the automated tests failed or was inconclusive for the control:

<p>On one side, Spring MVC automatically bind request parameters to beans declared as arguments of methods annotated with <code>@RequestMapping</code>. Because of this automatic binding feature, it's possible to feed some unexpected fields on the arguments of the <code>@RequestMapping</code> annotated methods. </p> <p>On the other end, p... +

FAILED

Test

Path:webgoat:webwolf/src/main/java/org/owasp/webwolf/mailbox/MailboxController.java:64:64 StartLine: 61, EndLine: 67
Code:<pre> @PostMapping(value = "/mail") public Callable<ResponseEntity<?>> sendEmail(@RequestBody Email email) { return () -> { mailboxRepository.save(email); return Respons... +

FAILED

The MITRE Corporation © 2019

MITRE

Sample OWASP ZAP output in Heimdall Data Format (HDF), including NIST tag:



```

{
  "id": "10024",
  "title": "Information Disclosure - Sensitive Informations in URL",
  "desc": "The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure",
  "impact": 0.3,
  "tags": [
    {
      "nist": [
        "SC-8",
        "Rev_4"
      ],
      "cwe": "900",
      "wascid": "13",
      "sourceid": "3",
      "confidence": "2",
      "riskdesc": "Informational (Medium)",
      "check": "<p>Do not pass sensitive information in URIs.</p>\n<p>The URL contains potentially sensitive information.</p>\n<p>The URL contains potentially sensitive information.</p>",
      "descriptions": [],
      "refs": [],
      "source_location": {},
      "code": "",
      "results": [
        {
          "status": "failed",
          "code_desc": "Evidence: ZAP\\nMethod: GET\\nParam: username_reg\\nUri: http://mymac.com:8191/WebGoat/challenge/6?confirm_password_reg=ZAP&email_reg=foo-bar%40example.com",
          "run_time": 0.0,
          "start_time": "Thu, 6 Dec 2018 10:53:11"
        },
        {
          "status": "failed",
          "code_desc": "Evidence: ZAP\\nMethod: GET\\nParam: confirm_password_reg\\nUri: http://mymac.com:8191/WebGoat/challenge/6?confirm_password_reg=ZAP&email_reg=foo-bar%40example.com",
          "run_time": 0.0,
          "start_time": "Thu, 6 Dec 2018 10:53:11"
        },
        {
          "status": "failed",
          "code_desc": "Evidence: foo-bar@example.com\\nMethod: GET\\nParam: email_reg\\nUri: http://mymac.com:8191/WebGoat/challenge/6?confirm_password_reg=ZAP&email_reg=foo-bar%40example.com",
          "run_time": 0.0,
          "start_time": "Thu, 6 Dec 2018 10:53:11"
        },
        {
          "status": "failed",
          "code_desc": "Evidence: Guest\\nMethod: GET\\nParam: user\\nUri: http://mymac.com:8191/WebGoat/JWT/votings/login?user=Guest\\n",
          "run_time": 0.0,
          "start_time": "Thu, 6 Dec 2018 10:53:11"
        },
        {
          "status": "failed",
          "code_desc": "Evidence: ZAP\\nMethod: GET\\nParam: password_reg\\nUri: http://mymac.com:8191/WebGoat/challenge/6?confirm_password_reg=ZAP&email_reg=foo-bar%40example.com",
          "run_time": 0.0,
          "start_time": "Thu, 6 Dec 2018 10:53:11"
        }
      ]
    }
}

```

Sample OWASP ZAP output in Heimdall Data Format (HDF), viewed in Heimdall:

The screenshot shows a browser window titled "heimdall-lite 2" displaying the results of an OWASP ZAP audit. The URL is "heimdall-lite.mitre.org/#/results/1". The main title is "OWASP ZAP Webgoat Heimdall_tools Sample". A search bar contains the ID "10024". The interface includes filters for Status (Failed), Severity (LOW), Title, ID, and Tags.

A red box highlights the "Tags" section, which lists "10024", "SC-8", and "Rev_4". A green arrow points from the right side towards this red box.

The "TEST" tab is selected. A message states: "One or more of the automated tests failed or was inconclusive for the control:". Below this, a note says: "The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment." A large red bar indicates a "FAILED" status.

The "Test" section shows evidence of a failed test with the following details:

```
Evidence: ZAP Method: GET Param: username_reg Uri: http://mymac.com:8191/WebGoat/challenge/6?confirm_password_reg=ZAP&email_reg=foobar%40example.com&password_reg=ZAP&register-submit=Register+Now&username_reg=ZAP
```

Another red bar indicates a "FAILED" status.

The bottom of the page includes the copyright notice "The MITRE Corporation © 2019" and the MITRE logo.

Samples Available in Heimdall-Lite

Samples available in Heimdall Lite at <https://heimdall-lite.mitre.org/>:

The screenshot shows a web-based interface for Heimdall Lite. The left sidebar has three main categories: LOCAL FILES, S3 BUCKET, and SPLUNK. The LOCAL FILES section contains a single entry: "Samples to show the power of the Heimdall application and supported HDF formats". The S3 BUCKET section contains several entries, some of which are highlighted with red boxes: "Sonarqube Java Heimdall_tools Sample", "OWASP ZAP Webgoat Heimdall_tools Sample", "AWS CIS Foundations Baseline InSpec Sample", and "RedHat 7 STIG Baseline InSpec Sample". The SPLUNK section contains entries for "OWASP ZAP Zero_WebAppSecurity Heimdall_tools Sample", "Fortify Heimdall_tools Sample", "AWS S3 Permissions Check InSpec Sample", "NGINX Inspec Sample", "Red Hat CVE Vulnerability Scan InSpec Sample", and "Ubuntu STIG Baseline InSpec Sample". Each entry in the S3 BUCKET section has a small circular icon with a plus sign next to it.

LOCAL FILES
Samples to show the power of the Heimdall application and supported HDF formats

S3 BUCKET
Sonarqube Java Heimdall_tools Sample
OWASP ZAP Webgoat Heimdall_tools Sample
AWS CIS Foundations Baseline InSpec Sample
RedHat 7 STIG Baseline InSpec Sample

SPLUNK
OWASP ZAP Zero_WebAppSecurity Heimdall_tools Sample
Fortify Heimdall_tools Sample
AWS S3 Permissions Check InSpec Sample
NGINX Inspec Sample
Red Hat CVE Vulnerability Scan InSpec Sample
Ubuntu STIG Baseline InSpec Sample

The MITRE Corporation © 2019

MITRE