
Steven Grimes

Information Security Officer

**CWS-NS Project Release 1 Planning Session : Architecture
Capabilities and Vision**

December 2016

Information Security Program

Architecture, Capabilities and Vision

Technical Capabilities

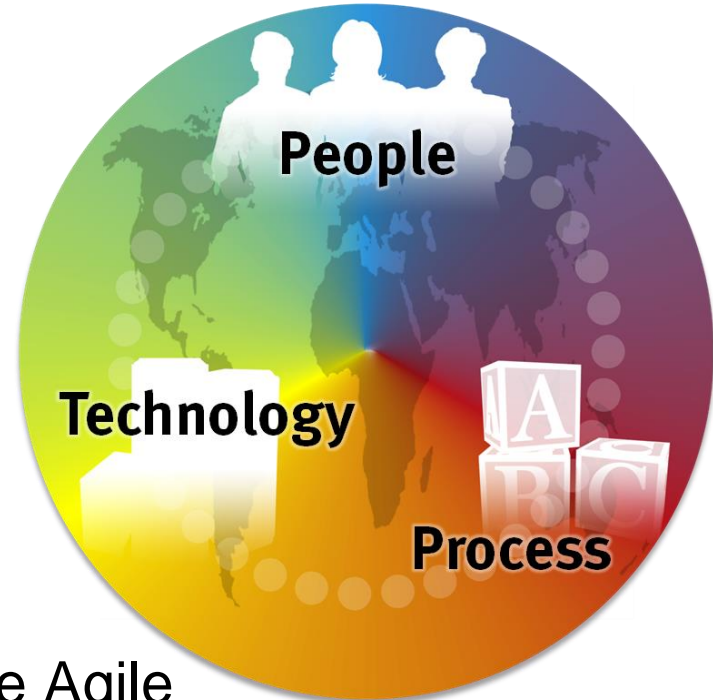
- Technology Based Security Capabilities

Our People

- Training and Awareness

Process

- Incident Management and the Agile Security Framework



Information Security Program

Information Security Wiki

Github: <https://github.com/ca-cwds/Information-Security/wiki>

The image shows a screenshot of the Child Welfare Digital Services (CWDS) GitHub profile and a preview of the Information Security Wiki page. The GitHub profile header includes the CWDS logo, the organization name, location (Sacramento, California), website (https://cwds.ca.gov), and email (cws-ns@osi.ca.gov). Below the header, there are statistics for Repositories, People (43), Teams (8), and Projects (0). The 'Pinned repositories' section features the 'Information-Security' repository, described as 'CWDS Information Security Program public documents and Wiki.' To the right, a preview of the 'ca-cwds / Information-Security' repository is shown, specifically the 'Wiki' tab. The wiki page has a 'Home' section with a note that Steven Grimes edited it 27 days ago. The main heading is 'CWDS Information Security Wiki'. Under the 'Overview' section, it states: 'The CWDS Information Security Wiki is the source of truth for all project level security policy, procedures and standards that the development teams shall follow for development activities. CWDS team members shall follow the policy, procedures and standards in the Information Security'. A sidebar on the right lists pages: Home, Agile Security Framework, Code Walk through, and Definition of PII (Personally Identifiable Information).

Child Welfare Digital Services
Sacramento, California | <https://cwds.ca.gov> | cws-ns@osi.ca.gov

Repositories | People 43 | Teams 8 | Projects 0

Pinned repositories

- Information-Security**
CWDS Information Security Program public documents and Wiki.

ca-cwds / Information-Security | Watch 3 | Star 0 | Fork 0

Code | Issues 0 | Pull requests 0 | Projects 0 | **Wiki** | Pulse | Graphs | Settings

Home
Steven Grimes edited this page 27 days ago · 6 revisions

CWDS Information Security Wiki

Overview

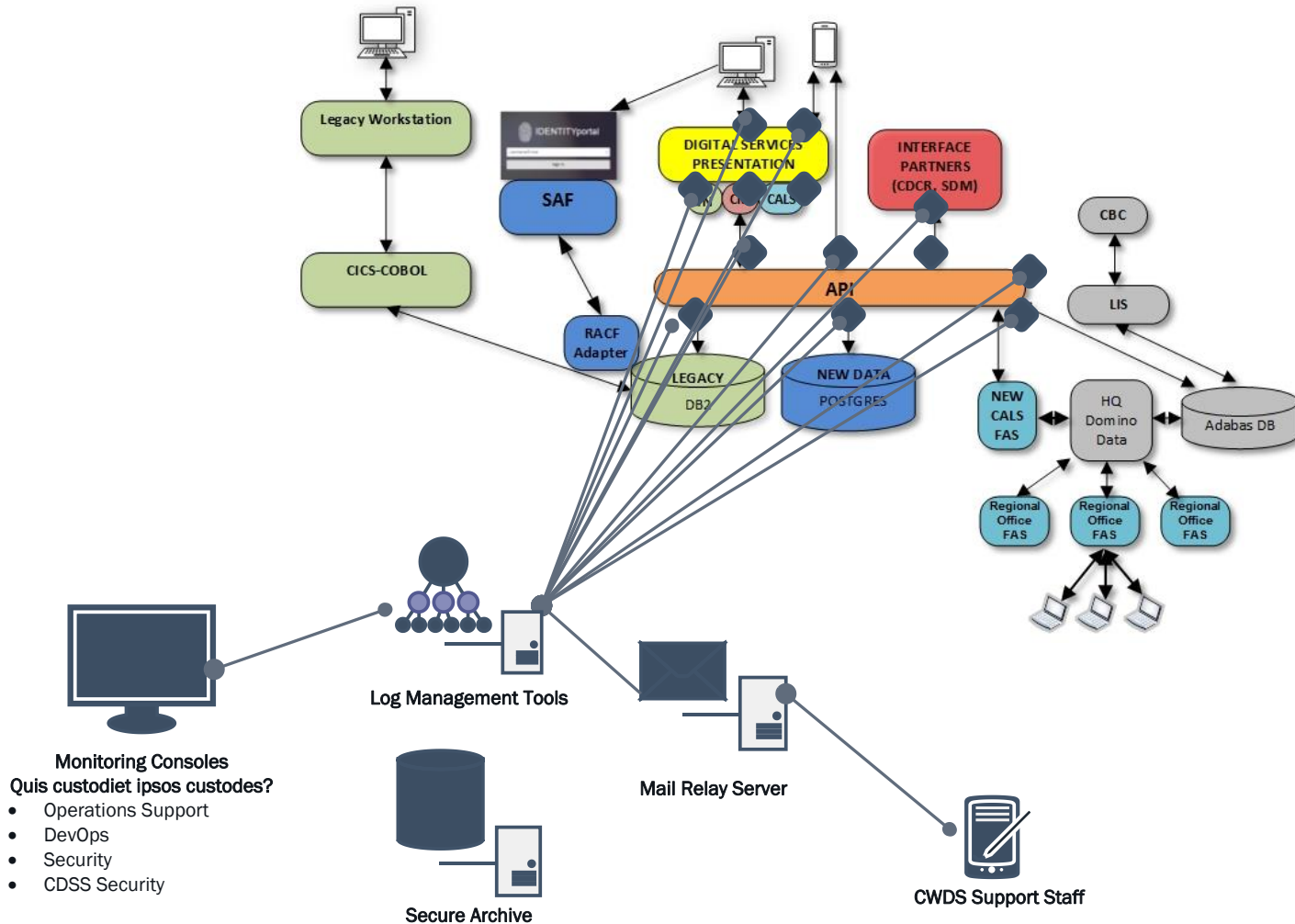
The CWDS Information Security Wiki is the source of truth for all project level security policy, procedures and standards that the development teams shall follow for development activities.

CWDS team members shall follow the policy, procedures and standards in the Information Security

Pages 19

- Home
- Agile Security Framework
- Code Walk through
- Definition of PII (Personally Identifiable Information)

Technology - Audit and Non Repudiation controls

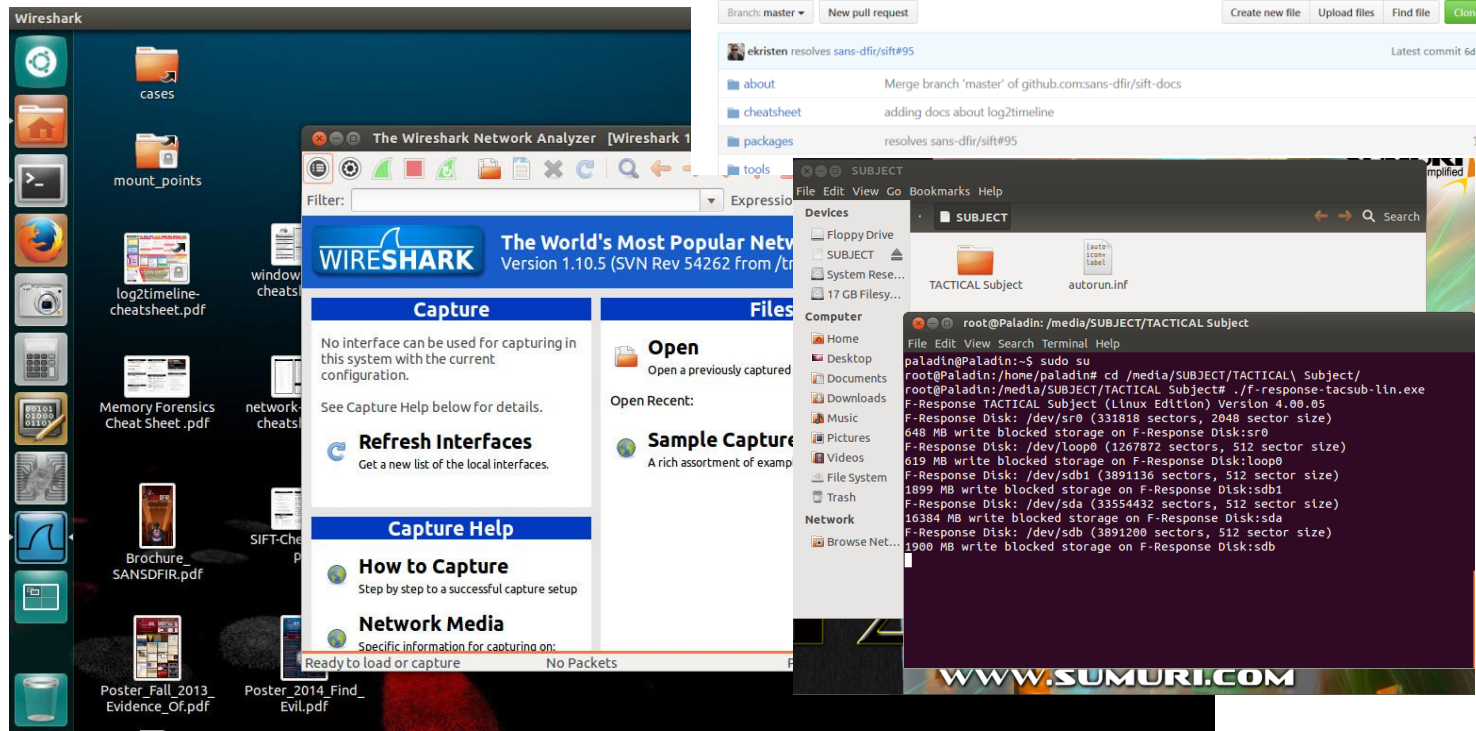


Information Security Program

Technology - Forensics capabilities

Forensic Laptop

Digital Forensics & Incidence Response



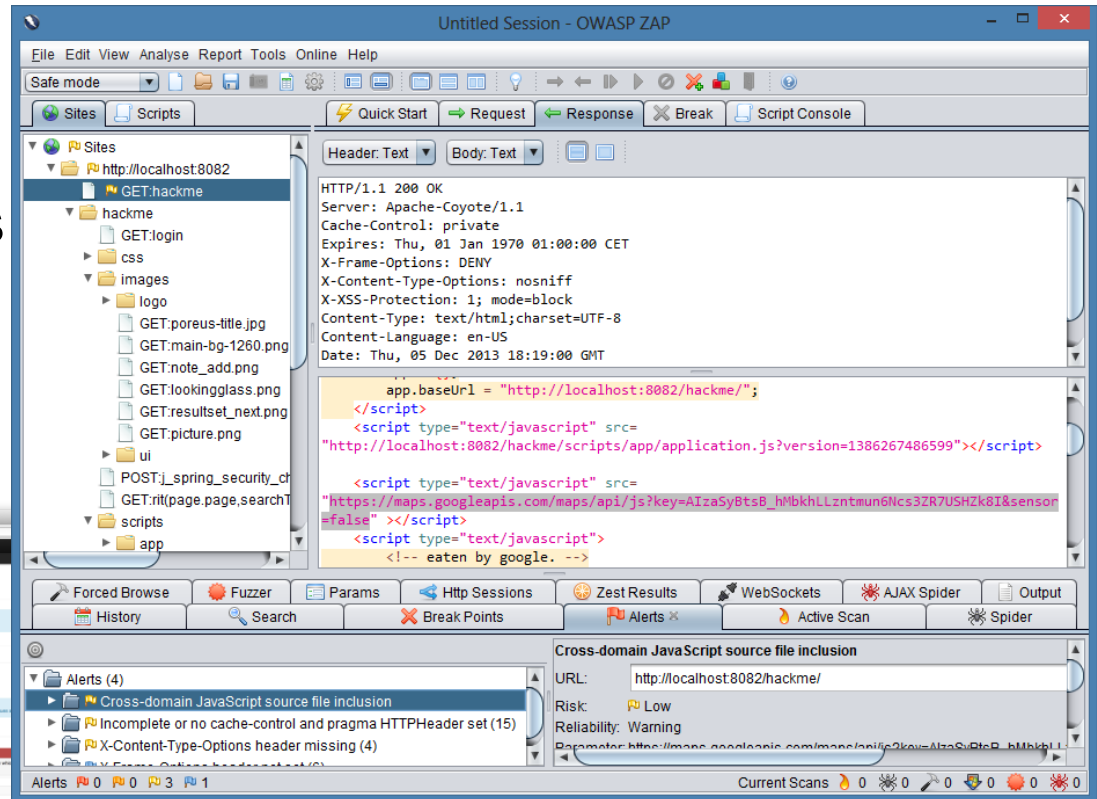
Information Security Program

Technology - Vulnerability and Penetration Testing

- Vulnerability and Penetration Tools
- Discovery Scanners
- Packet Sniffers

```
Starting Nmap 4.20 < http://insecure.org > at 2007-04-20 03:34 CEST
Interesting ports on 192.168.1.120:
Not shown: 1686 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
35/tcp    open  nmap
39/tcp    open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1026/tcp  open  LSA-over-nterm
1031/tcp  open  iad2
1800/tcp  open  vnc-http
1900/tcp  open  vnc
MAC Address: 00:01:03:0A:E0:56 (3com)

Nmap finished: 1 IP address (1 host up) scanned in 0.891 seconds
```



Information Security Program

Process – Incident Management

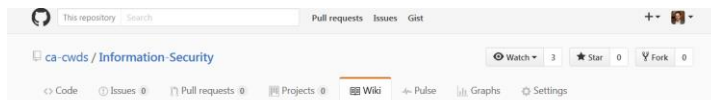
Incident Management Process

- Roles
- Response Times
- Triage
- Reporting Requirements
- Communications
- Root Cause



Information Security Program

Process – Agile Security Framework



Agile Security Framework

Steven Grimes edited this page 22 days ago · 32 revisions

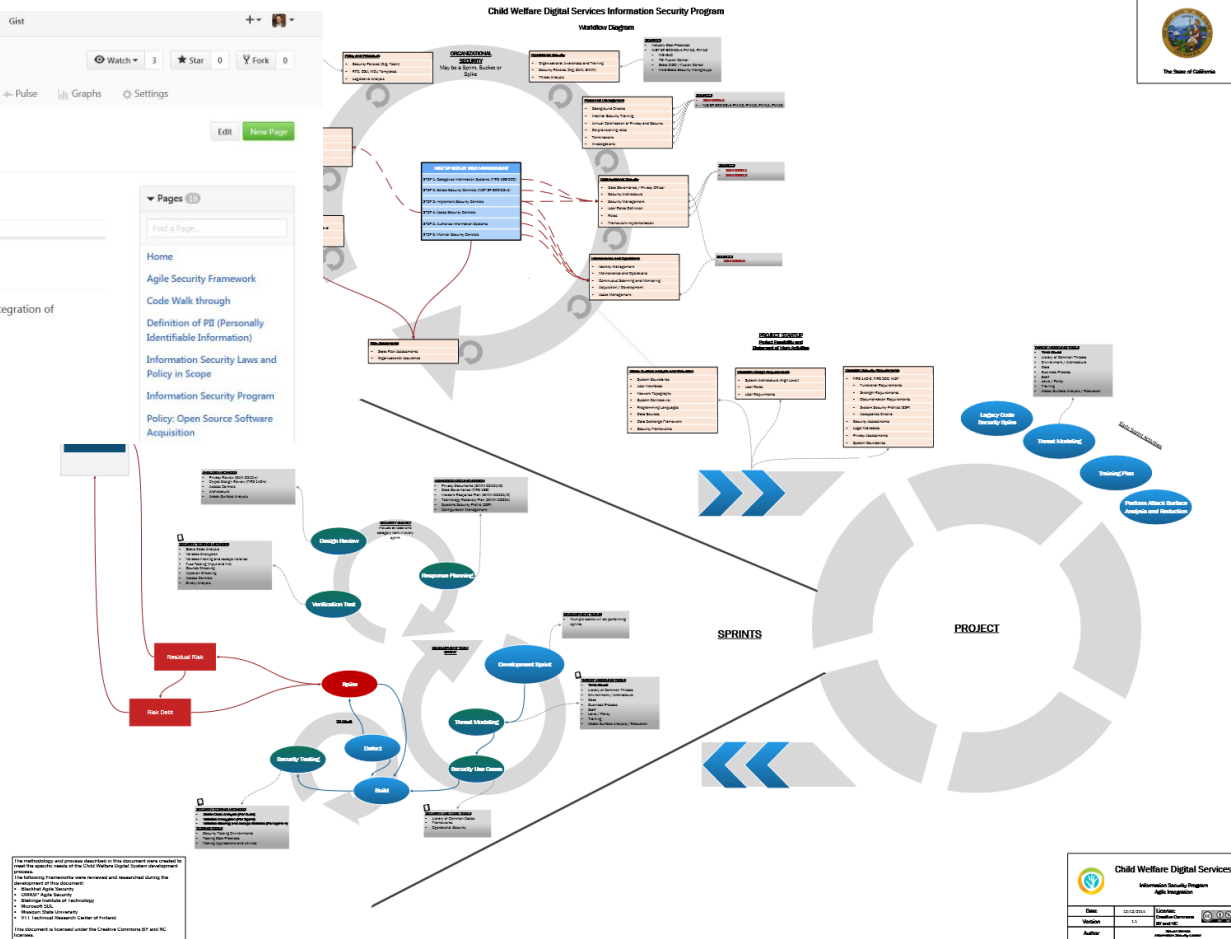
CWDS Agile Security Framework

1.0 Overview

Child Welfare Digital Services (CWDS) uses an agile security framework for integration of information security to software development activities.

The CWDS agile security framework has six components:

- Project Start-up
- Project Team
- Sprint
- Security Bucket



Information Security Program

Our People - Training

Training	Delivery Date	Curriculum	Required Y/N	Notes
Personally Identifiable Information - Overview	4Q 2016		N	Driven by security incident. (redaction's in curriculum under GC 6254.19)
Annual Security and Privacy Certification	4Q 2016 2016	Security & Privacy Awareness Training rev 8-25.pptx	Y	This curriculum is OSI owned material and will not be posted to the CWDS Github site.
Phishing Training	4Q 2016		N	Driven by operational security - state phishing audit results. (redaction's in curriculum under GC 6254.19)
Agile Security framework overview	1Q 2017		N	
Applying PII to software development	1Q 2017		N	