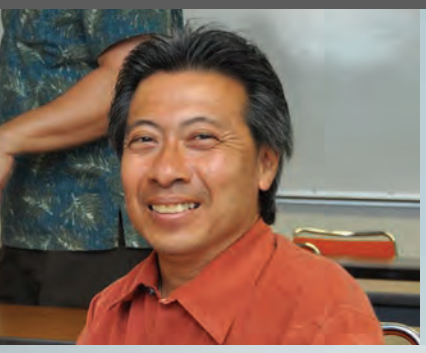


"OIMT has enhanced the State's security — they've been able to notify our department of potential security breaches and potentially suspicious activity."

—Ryan Shimamura
Acting Chief Information Officer, Department of Human Services

6.3 PROGRAM: ENTERPRISE SECURITY AND PRIVACY

Objective: Improve security and privacy controls including Identity, Credential, and Access Management; enable Single Sign-On for access across various State systems; and enable privacy protections.

Description: In 2012 OIMT conducted a preliminary security and privacy assessment that found the State had significant security and privacy vulnerabilities, exposing the State to a number of potentially devastating security breaches. Especially worrying was the fact that, in 2012, numerous state governments had already been victims of costly security breaches that had cost an average of more than $20 million to remediate. In addition to the monetary expense, each of these states had also jeopardized citizens' privacy, as evidenced in one case where 14,000 Social Security Numbers were posted to a website.

In response to the security and privacy assessment, OIMT made strengthening the State's security and privacy controls a key priority. Throughout 2012–2014, OIMT worked to establish a fully integrated Security Operations Center (SOC) and Computer Security Incident Response Center (CSIRC) that would allow the State to:

- Provide uninterrupted security services while improving security incident response times;
- Reduce security threats to the State;
- Enable quicker, well-coordinated notification to all State departments regarding security threats or issues; and
- Provide proactive monitoring of email and data services.

In 2013 OIMT completed a more detailed assessment across 17 categories, performed an audit to further assess security capabilities, and identified vulnerabilities that require more than 60 security-related projects.

Impact: OIMT's five security and privacy initiatives have reduced the State's exposure to security breaches, while notifications to departments have alerted IT personnel within those departments of potential threats.

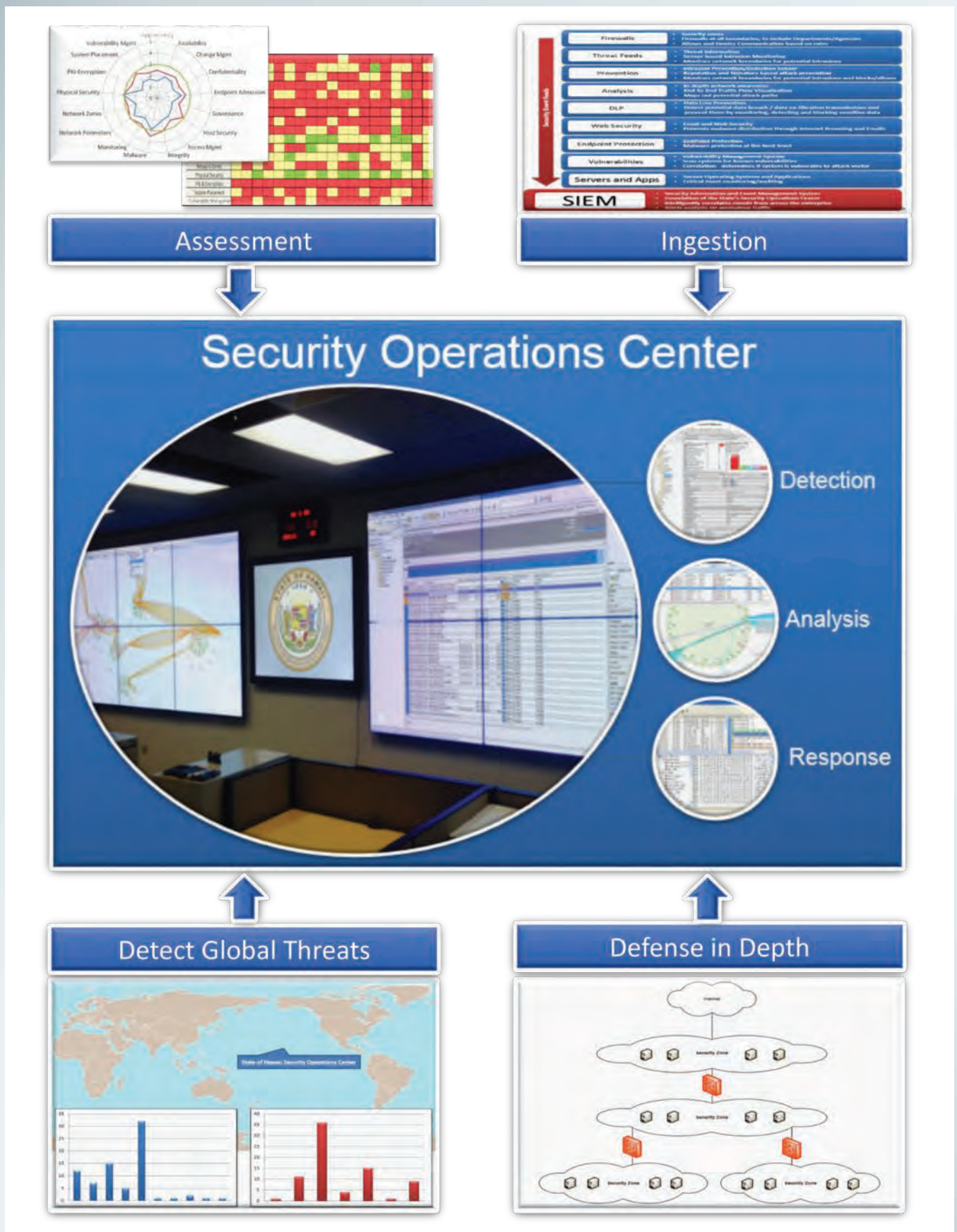
Related Projects and Initiatives:

New Chief Information Security Officer (CISO)
In 2013, OIMT was focused on the following:

- Hiring a Chief Information Security Officer (CISO) — Matthew Wong
- Establishing Security Governance policies for the overall Information Security Program
- Creating Enterprise Information Security Policy, BYOD Policy, and overall Security and Privacy Policy
- Creating a Security and Privacy Road Map based on the completed security assessment

Proactive Security Monitoring and Notification for Departments
In 2013 OIMT began proactively monitoring the State's network (through Hawaii's first-ever SOC) for potential security breaches and notifying departments of potential threats found. OIMT also publishes regular security announcements to inform departments of recent occurrences and provide security policy updates.

Security Infrastructure
OIMT has begun to implement upgrades to the State's security infrastructure to prevent breaches of personal data.


Assessment
Ingestion
Security Operations Center
Detection
Analysis
Response
Detect Global Threats
Defense in Depth