

# OIT User Conference Security Team

November 2014

## What will we be covering today?

- Introductions
- Office of Information Security and Privacy (OISP) and the Transformation effort
- Staffing Model and Points of Contact
- Standup of New Enterprise Services
- Short and Long Term Roadmaps

## Enterprise Security Control Offerings

Over the course of the IT Transformation planning effort, the IT Security working group determined a new direction for Information Security.



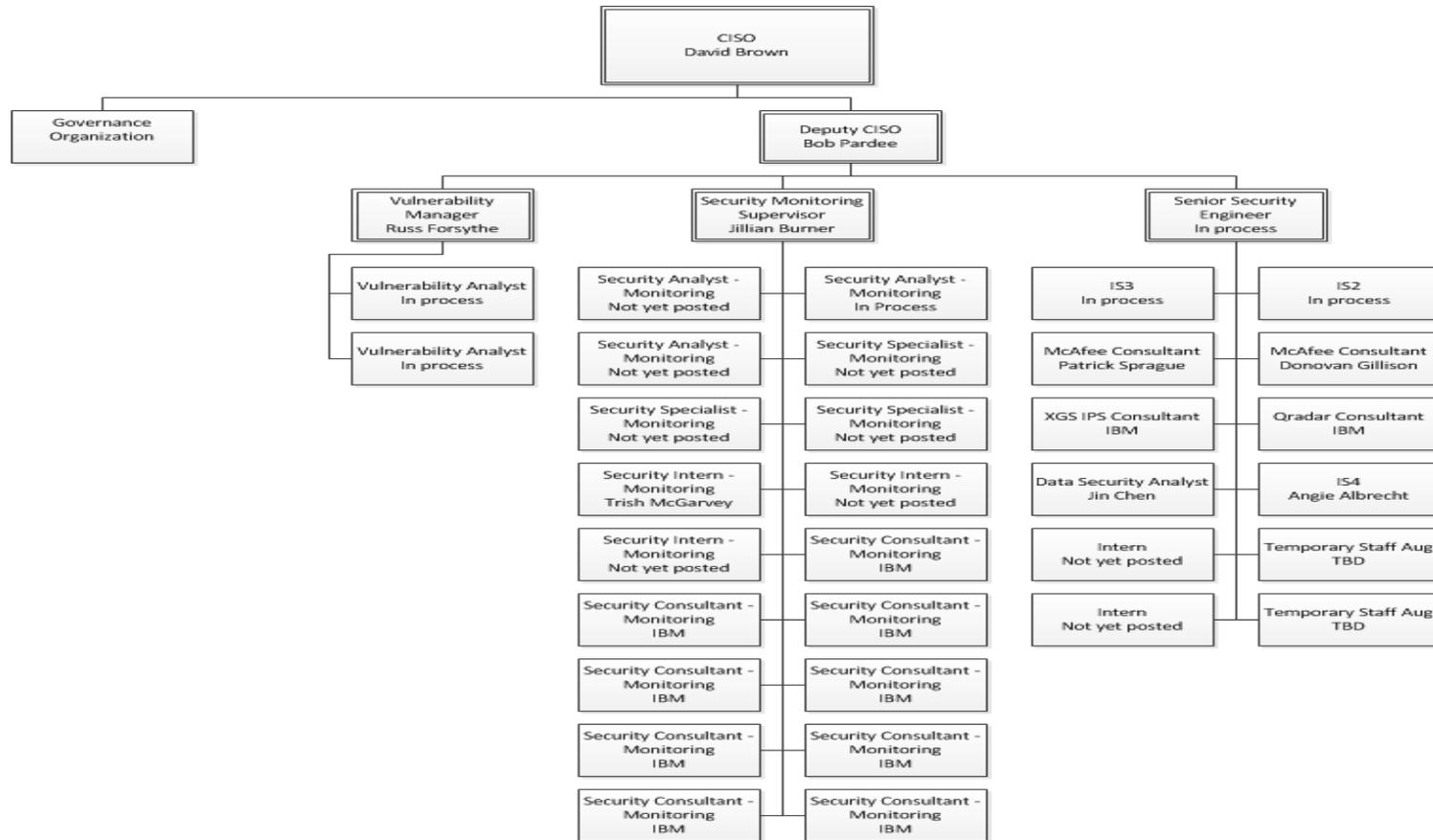
## Enterprise Security Control Offerings

The OISP now offers managed security services for the enterprise in addition to its traditional role in security governance, coordination and consultation, which includes:

- Vulnerability Management
- Intrusion Prevention
- Endpoint Protection
- Monitoring and Incident Response



# Security Operations Structure



**Note:** This structure includes consulting resources which are onboard or in progress this FY which do not appear on the Optimization slide.

# Key Points of Contact

**Customer Service Center**

**614.644.6860**

OISP

614.644.9391

Bob Pardee, Deputy CISO

614.387.1632

Jillian Burner, CND Manager

614.387.0320

Russ Forsythe, Vulnerability Mgr.

614.995.1534

Senior Security Engineer

Coming soon

# Security Team



Security Team Left to Right: Jillian Burner, Russ Forsythe, John McCarty, Bob Pardee, Paul Kamenan, Carolyn Jordan, Daren Arnold, Jason Mather, Matt Williams, James Matheke, Rick Shipley, Miki Calero and Dave Brown.

## **OISP Services Includes:**

- Vulnerability Management
- Security Engineering
- Enterprise Endpoint Protection
- Security Incident and Event Management
- Monitoring and Incident Response

# Vulnerability Management

## Vulnerability Management Includes

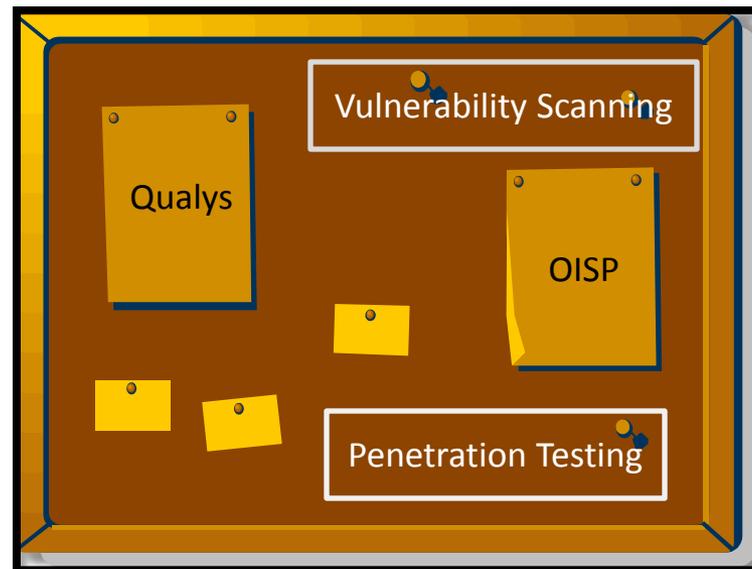
- Vulnerability scanning and reporting services statewide
- Advice and consulting for vulnerability impact and remediation
- Web application scanning
- Penetration Testing



# Vulnerability Management

## Current Status

Vulnerability Scanning services using Qualys is currently being rolled out to all agencies. Limited resources are available for penetration testing, but contact us if your agency is interested.

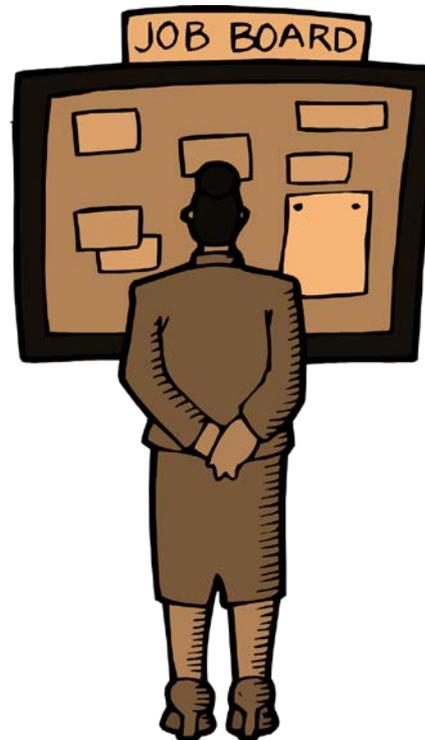


## Security Engineering Includes

- Intrusion Prevention Systems – IBM XGS (former Proventia) IPS
- Security Incident and Event Management – IBM Qradar
- Antivirus, Host Intrusion Prevention, Web Safety Checking – McAfee
- Encryption – McAfee (whole disk & file/folder)
- Scanning for indicators of compromise and other weaknesses – McAfee RealTime

## Current Status

Security Engineering is currently staffing the team and will continue through the end of FY15.



# Enterprise Endpoint Protection

## Enterprise Endpoint Protection Includes

Deployment of a full suite of McAfee endpoint protection software to every workstation and server owned by the state:

- Antivirus
- Host Intrusion Prevention
- Host Firewall
- Endpoint Encryption
- File & Folder Encryption
- Port and Device Control
- Pre-boot scanning
- Software Whitelisting
- Compliance Measurement
- Optimized Scanning for VDI
- Data Loss Prevention
- Realtime

# Enterprise Endpoint Protection

## Current Status

All cabinet agencies to be engaged by the end of CY14 and the project completion is scheduled for the end of CY15.



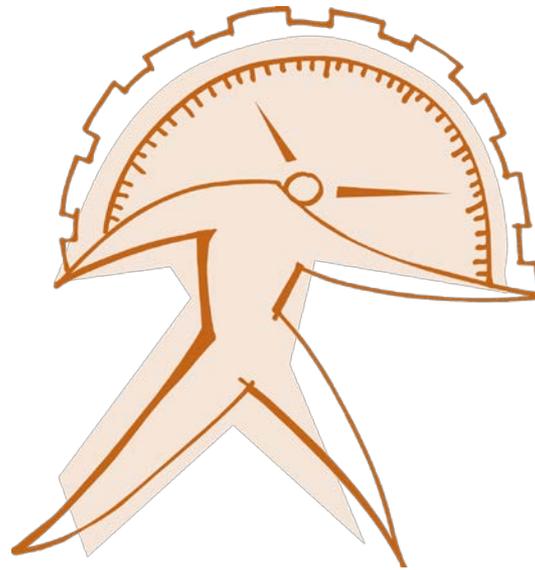
## Security Incident & Event Mgmt. Includes

- Collection and correlation of log and event information from devices throughout the state
- Proactive alerting and forensic capabilities
- Visible to customers
- Works in support of the Monitoring & Incident Response team

# Security Incident and Event Management

## Current Status

The Security Incident and Event Management service has been deployed and is in use within OIT. The sensors have been deployed in several agencies.



## Monitoring and Incident Response Includes

- 24x7 Monitoring of events from Qradar
- 24x7 Response to security tickets submitted to the Customer Service Center
- Advice on remediation
- Escalation path for security issues

# Monitoring and Incident Response

## Current Status

The consulting staff is in place and the first permanent Analyst is in the hiring process.

We will gradually move to 24x7 by the end of the fiscal year.



# Roadmap – Near Term

- Web Application Firewall is integrated into the load balancers
- Advanced endpoint protections:
  - Change Control
  - Pre-boot scanning
  - USB and CD/DVD write control
  - Application whitelisting
  - Compliance measurement
  - Client-side vulnerability checks – all parts of the McAfee suite

# Roadmap – Near Term

- Data Loss Prevention – Will begin with McAfee client-side components and continue with the investigation of network DLP products.



# Roadmap – Long Term

- Several technologies under review:
  - Review/refresh of DAM product
  - Centrally managed web filtering solution
  - Privileged credential management
  - System to support user provisioning flow

# Thank You!

## Thank you!

We know all of this change can make for a challenging time, we would like to thank you and your agencies for the hard work your teams are putting into helping us improve the security posture of the State of Ohio.



# Security Discussion



What are your security challenges?



How can we help you?



**We want to hear from **YOU!****



# Questions or Suggestions?

