ocio

Office of the
Chief Information Officer
Iowa Department of Management

Cybersecurity Services

PRESENTER: Jess Flaherty

DATE: February 2023

OCIO Overview

Oversight responsibilities for agencies including:

- IT Procurement
- Enterprise IT and Information
- Security Standards
- Agency Technology Planning

Iowa Code 8B allows the OCIO to serve:

- Executive, Judicial, and Legislative branches
- Iowa Counties and Cities
- Iowa Educational Institutions
- Iowa nonprofits

Local Government Cybersecurity Program

Security Operations Center

Endpoint Detection & Response

Security Operations Center (SOC)

Provides cybersecurity threat monitoring and alerting to local governments 24 hours a day, 7 days a week, and 365 days a year

Security Operations Center (SOC)

- **What is a Security Operations Center (SOC)?**
  - The purpose of a SOC is to monitor, prevent, detect, investigate, and respond to cyber threats
- **Types of Cybersecurity Experts in a SOC:**
  - **Tier 1 Analysts** - monitor the SOC cybersecurity tools, analyze events as detected and initiate remediation procedures
  - **Threat Intelligence Analyst** - investigate emerging threats and advise of mitigation efforts
  - **Security Engineers** - architect the cybersecurity tools for implementation and point of escalation for high priority incidents
  - **Security Governance, Risk, and Compliance** - experts that advise and collaborate with customers on audits, training, and policy

Security Operations Center (SOC)

- **High Alert - Urgent**
  - May include automated device containment
  - Hourly phone calls from OCIO SOC team
  - Incident remediation support form SOC
  - Escalation to Chief Information Security Officer
- **Medium/Low Alert**
  - Can be false positive
  - Minor impact
  - Email alert from **SOC@iowa.gov**
  - OCIO remediation assistance if requested

Endpoint Detection & Response Tool (EDR)

Security tool that detects and prevents a wide range of known and unknown cyber attacks on computers, servers, and other devices

Endpoint Detection & Response (EDR) Tools

FireEye HX

- Triage collection

CrowdStrike - Next Generation

- Real time response
- Telemetry data to monitor live events
- Multi-tenant
- Falcon: Spotlight, Discover, OverWatch, Device Control, X

What is CrowdStrike Falcon?

- **Falcon: Prevent**
  - Monitors and prevents known malicious processes and malicious commands
- **Falcon: Spotlight**
  - Vulnerability Scanning Feature
    - Scans devices for known vulnerabilities & helps inform patching prioritization
  - Identifies security risks on device
- **Falcon: Discover**
  - Inventory and User Management
    - Assists IT technicians in keeping device inventory lists accurate

What is CrowdStrike Falcon?

- **Falcon: OverWatch**
  - Managed threat hunting. CrowdStrike professionals looking for potential breaches and incidents 24/7. They will call the ISS if any malicious activity is happening on the network
- **Falcon: Device Control**
  - Ensures safe USB usage and can monitor and alert if there is suspicious USB usage or activity
  - Ensures safe connections to USB ports on computer
- **Falcon: X**
  - Threat intelligence on actors and indicators
  - CrowdStrike professionals gather data on hacker groups and indicators of compromise

CrowdStrike Migration: What's Next?

- **Participation Survey**
  - Look for survey link next week
    - Survey will come from Jess at **government.services@iowa.gov**
  - Information gathering survey
  - Awareness of anticipated participation
  - Will assist in the creation of the individual County IDs
- **Board of Supervisors sign Memorandum of Understanding (MOU)**
  - This is the first step in migrating from FireEye HX to CrowdStrike

CrowdStrike Migration: MOU

- **Memorandum of Understanding (MOU)**
  - Must be signed to participate in OCIO's CrowdStrike & Security Operations Center Monitoring
- **Board of Supervisors should sign MOU**
  - Delegation of Authority could allow for signature from another county employee
- **MOU will supersede all other security service MOUs with OCIO**

CrowdStrike Migration: MOU

MOU Highlights

- Streamlined MOU format
- Roles, Responsibilities, and Obligations of Parties clearly outlined
  - Obligations of Parties is in main contract
  - Previously Obligations of Parties was only in the terms and conditions
- Requires County to provide an "Authorized Installations" or device count

CrowdStrike Migration - Important Dates

- February 8th: ISAC/OCIO Webinar
- February 13th: Survey sent
- February 20th: Release of MOU
- March 9/10: ISAC Spring Conference
- Late March: CrowdStrike onboarding begins
- August 31: CrowdStrike Migration deadline

**All dates are subject to change*

OCIO Contacts

Looking for proactive cyber support?

Jess Flaherty, Local Government Program Manager

515.380.3765 | government.services@iowa.gov

Need cyber incident help?

State of Iowa's Security Operations Center

1.855.442.4357 | 515.725.1296 | soc@iowa.gov

CONNECT WITH US

Follow us

@IowaOCIO

Visit us

@StateofIowaOCIO

ocio
Office of the
Chief Information Officer

OCIO.iowa.gov