IOT Security - 2020

Who We Are:

A 25-member team focused on Security Operations, Risk & Compliance and managing an Information Sharing & Analysis Center. Our team works with the operational teams of IOT and the agencies to mitigate risks to confidential state data.

Our Mission:

To establish and maintain an effective cybersecurity program that incorporates the appropriate resources, technologies, and strategy to deter adversaries, both financially and tactically, making the State an unattractive target. Further, to establish governance and processes that reduce risk to acceptable levels while not burdening agencies or business operations.

Department: 493003

Managers Bryan Sacks, CISO; Hemant Jain, SecOPs Director; Tad Stahl, IN-ISAC Exec. Dir.; Anu Bag Exec. Dir Risk and Compliance; Bill Woolsey Information Security Officer as a Service (Program Director)

Formed: The IOT Security team was formed in October 2005.

What We Do:

IOT Security sets information security policy for the Executive Branch of state government and then works with agencies to protect confidential citizen data by working toward compliance with those policies. IOT Security also operates a number of enterprise-wide protective tools and processes.

Our Products:

1175 Security - Baseline
1180 Security – Confidential
1212 Information Security Officer as a Service
1215 Compliance Center of Excellence

Our Tools:

Antivirus/Malware
FireEye NX – Network malware detections (workstations)
FireEye HX – Hosted Based
MS-ISAC (managed 3rd party sensor)

Internet Traffic Management
Cisco, F5, VMware (NSX)
Intel (McAfee) Web Gateways
MS-ISAC (managed 3rd party sensor)

Intrusion Detection/Prevention
FireEye NX - IPS
Citrix NetScaler/F5
MS-ISAC (managed 3rd party sensor)

Vulnerability Scanning
Rapid 7 Insight VM

Email Protection
FireEye EX
Sophos

Asset Management/Protection
Absolute – track stolen equipment
Mobile Iron (smart phones/tablets)
Archer

Logging
ELK; Azure

Privilege Management
Thycotic
Microsoft ATA & Azure (two-factor)

Our Metrics: IOT Security tracks a number of metrics for its protective tools. This year we will begin tracking agency compliance with the NIST framework.

Our Customers: All Executive Branch agencies.

Our Budget: $15MM

Our Growth:

All Agencies are using the Basic Security service
44 Agencies are using the Confidential Security service

Major Accomplishments - 2019:

- Established the Compliance Center of Excellence
- Implementation of FireEye HX across all State devices
- Established Information Security Officer as a Service Program
- Implementation of a World-Class Identity Access Management infrastructure
- Established and matured the Executive Branch Security Readiness program
- Hardened baseline builds of servers and workstations
- Implemented Rapid7 Insight VM to obtain vulnerability data on-demand
- Incident Response Plan update and refresh
-

Current Projects:

- Integration of enhanced logging tooling (ELK)
- Rationalizing application toolsets
- Azure Information Protection/Rights Management
- SOC 2.0
- Policy Update
- Training refresh