IOT Security Operations - 2023

Who We Are: A group of cybersecurity professionals tasked with protecting the Executive Branch agencies servers and workstations from threat actors with malicious intent.

Our Mission: To be a strong but transparent partner in protecting and responding to our businesses while allowing them to innovate, build new products, and deploy new services in the execution each agency mission.

Department: 493003

Manager: John Lobaugh, Brent Walls, David Whitt

Formed: 2008

What We Do:

ASM	Ticket and Request Management
Vulnerability Management	Agent- and engine-based scans of all assets managed by IOT, which produces a list of identified vulnerabilities on each endpoint.
Endpoint Protection	A comprehensive agent-based detection and protection of all IOT manage Windows and Linux based endpoints.
Endpoint Tracking	A agent-based tracking system that enables the freezing of assets when then are identified as lost or stolen.
Network Traffic Inspection	Layer 3 network traffic inspection of all ingress and egress traffic for IOT managed network infrastructure.
Internet Traffic Filtering	DNS based traffic inspection for all IOT managed endpoints
Incident Detection & Response	Detection and response to any identified cyber security threat within and of the State's 100+ Executive Branch agencies
Software Review	Known vulnerability and general security inspection all software installed on IOT managed endpoints
Centralized Enterprise Logging	Centralized logging all events required to facilitate successful threat hunting within the IOT managed network infrastructure

Our Products:
1175 Security – Baseline
1180 Security – Confidential

Our Customers: Executive Branch state agencies (~100) that use any of the 130+ products or services provided by IOT.

Major Accomplishments:
- Executive branch wide adoption of a complete endpoint detection and protection solution
- Full visibility of all ingress and egress traffic for all agencies and organizations utilizing the State's network infrastructure

Current Projects:
- Deployment of Data Level Detection and Protection solution against all Executive Branch agency data repositories
- Reevaluation and overhaul of State's vulnerability management program
- Development of a service offering focused on providing agencies with a comprehensive security and compliance evaluation and proposed remediation plan
- Continued development and enhancement of the IOT Security Operations Center