IOT Solution Architecture - 2023

Who We Are:

OpSec administers and maintains technology used throughout the State that ensures security, availability, and operability.

Our Mission:

To provide secure, reliable, and integrated technology solutions to our partner agencies so they can better serve our mutual customer, the Hoosier taxpayer.

Department: 493022

Manager: John Thatcher

What We Do:

Operational Security (OpSec)

The OpSec team manages more than 2,600 certificates and URLs on the State's proxies. The team works with the Security and Operational teams at IOT to troubleshoot issues, resolve configuration issues on servers to meet compliance requirements, and ensure secure operations. They are also responsible for DNS configuration, geo-blocking, load balancing, and IP intelligence on the proxies.

Our Tools:

ASM	Ticket Management and SLA Measurement.
F5/BigIP	Load balanced proxies combine high-speed load balancing and content switching, data compression, content caching, SSL acceleration, network optimization, application visibility, and application security on a single, comprehensive platform.
Cloudflare	Public-facing edge protection that includes WAF services, DDoS protection, Bot protection, and more. Cloudflare provides external DNS record services for the State. Additionally, IOT employs Cloudflare Access to make internal applications securely available externally.
DigiCert	Secure Certificate Provider
Secret Server	Password management.
EPM	Enterprise Privilege Manager
Device42	Device interrogation, CMDB, and data sharing.
DNS	Domain Name System services (both internal and external)

Our Metrics:

Mon-Fri 6am-6pm excluding state holidays

Resolve customer issues within 40 IOT business hours: 90%+ G; 87%+ Y; <87% R

Our Customers:

Executive Branch, Attorney General, Judicial Branch, and Secretary of State.

Our Budget:

$6 million (funded by Server Administration)

Our Growth:

In the past year, the Operational Security team has added 2 new employees, replacing the individuals who were responsible for a pair of technologies that have moved back to the Server Administration teams (SCCM & SCOM), 2 new contractors responsible for implementing and growing the Device42 environment, and 2 SEAL associates. Device42, Cloudflare, EPM, and Secret Server are all new technologies that the OpSec team has added responsibility for during the past year.

Recent Major Accomplishments:

Implemented Cloudflare services to help protect the State from advanced threats.

Assumed ownership of the Delinea (Secret Server and EPM) suite of products.

Implemented Device42 and have configured scanning jobs to gather intelligence from tens of thousands of devices throughout the State.