

Local Government Cyber Threat Detection Case Study

A complete solution for your business!

At a glance

The Director of Information Technology and his team provide IT support for several city agencies, including the police and fire departments. The City's IT services must be available 24/7, but the internal IT staff is only available from 8 am – 5 pm, Monday through Friday, leaving significant gaps of time where cyber exploits could go undetected.

Key solution

ProVision SOCaas Monitoring & Alerting



24/7

Security Monitoring



100%

Scalable solution



www.foresite.com
+44-800-358-4915
+1-800-940-4699

CT Office:
1 Hartfield Blvd, Suite 300
East Windsor, CT 06088

World Headquarters:
7311 West 132nd Street, Suite 305
Overland Park, KS 66213

UK Office:
A8 Ively Road, Farnborough
Hampshire, GU14 0LX UK

CHALLENGES



- 24/7 coverage for threat detection and assistance with an initial response.
- Add threat intelligence and log correlation to enrich the value of the log data.
- Align with compliance requirements for monitoring and logging.
- Establish a relationship with a firm that can provide resources for aspects of cybersecurity that are not required full-time (such as forensics, cyber testing, and compliance consulting).



**Trained
Cybersecurity
Team**



**Powerful &
Flexible**



**Threat
Intelligence**

RESULTS



1

Foresite assisted the IT Director with identifying the assets that would provide the most value for threat detection to confirm the scope for this engagement. We also worked with the City to get the assets onboarded right away with deferred billing to align with their budget cycle.

2

Onboarding support assisted the IT staff with the implementation of our ProVision solution for log collection and aggregation, application of business rules, and forwarding to the Foresite Security Operations Center (SOC).

3

Our trained security analysts investigate and validate alerts to rule out false positives and continually tune the business rules. When a threat is validated, the analyst will escalate appropriately to provide the details, associated logs or intelligence, and recommended steps to address the threat.