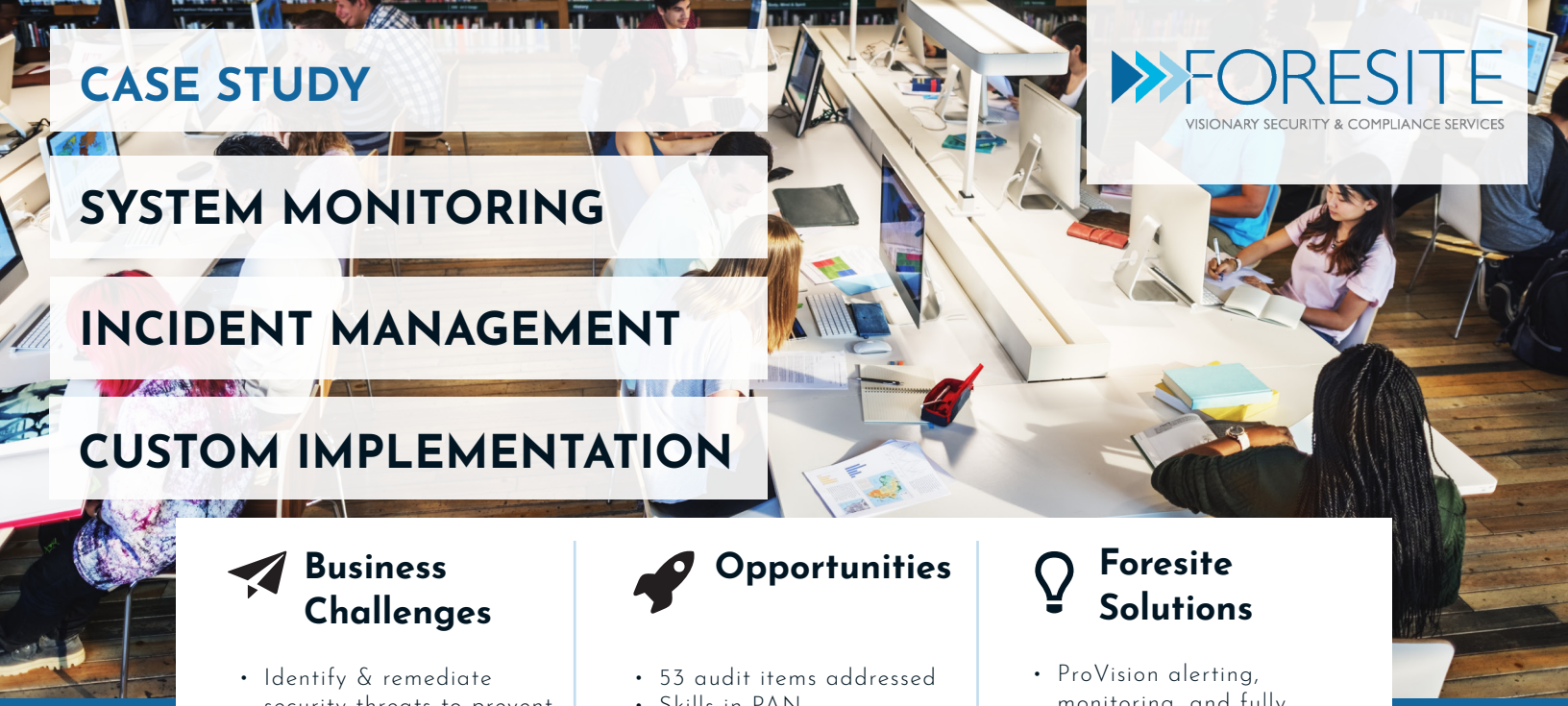

FORESITE
VISIONARY SECURITY & COMPLIANCE SERVICES

CASE STUDY

SYSTEM MONITORING

INCIDENT MANAGEMENT

CUSTOM IMPLEMENTATION

Business Challenges

- Identify & remediate security threats to prevent major cyber breach
- Become & remain NIST & SANS audit ready
- Ensure repeatable content compliance process across all locations

Opportunities

- 53 audit items addressed
- Skills in PAN
- Structure under same authority
- Process definition (i.e. change control)
- Service management

Foresite Solutions

- ProVision alerting, monitoring, and fully managed services
- Customized implementation
- Ongoing tuning

BACKGROUND

A multi-location state university needed to be able to fulfill all NIST and SANS controls to improve security operations, implement process standards, and become audit ready. This required addressing procedures within change management, logging and monitoring, configuration, hardening standards, and general security policies.

The university also needed the ability to log and monitor procedures to ensure that risky events are reviewed on a 7/24/365 basis. An audit requires monitoring analysis and correlation, and providing real-time alerts from all devices across all locations. Lack of system standardization across all locations posed an additional challenge in finding a monitoring solution.

With limited human resources wearing multiple hats, the university's internal IT staff needed additional outside

OUR **OBJECTIVES**

- Meet compliance requirements for network monitoring of disparate systems
- Outsource monitoring to ensure 7/24/365 coverage without added FTE costs
- Allow the internal IT staff to focus on the strategic initiatives of the university
- Implement a solution that can be tuned to screen out false positives and alert on

OUR **SOLUTION**

- Co-managed services means both Foresite and the university will have the ability to implement changes on the infrastructure. Both organizations will use the same change control process and implementation to ensure all documentation is aligned and kept up-to-
- Functions of the co-managed service:
  - System monitoring
  - Log file analysis
  - Alerting & escalation
  - Incident analysis & management
  - Change management & implementation

WORLD **HEADQUARTERS**
7311 West 132nd Street, Suite 305
Overland Park, KS 66213
+1 (800) 940-4699

CT **OFFICE**
1 Hartfield Blvd, Suite 300
East Windsor, CT 06088
info@foresite.com

UK **OFFICE**
A8 Ively Road, Farnborough
Hampshire, GU14 0LX UK
+44 (800) 358-4915