Cybersecurity Operations : *To Outsource or not Outsource?*

John Skaarup, CISSP, GSLC

Cybersecurity Officer

Texas Department of Transportation

March 16, 2020

Table of contents

1 What’s a SOC?

2 The three prevalent models

3 All in-house: Pro’s and Cons

4 Outsourced: it’s cheaper, right? (Hint: no)

5 Hybrid: Texas agencies have another choice

6 What TxDOT is doing and whether or not it’s working

7 Q & A

WHAT IS A CYBERSECURITY OPERATIONS CENTER? SOC? CSOC?

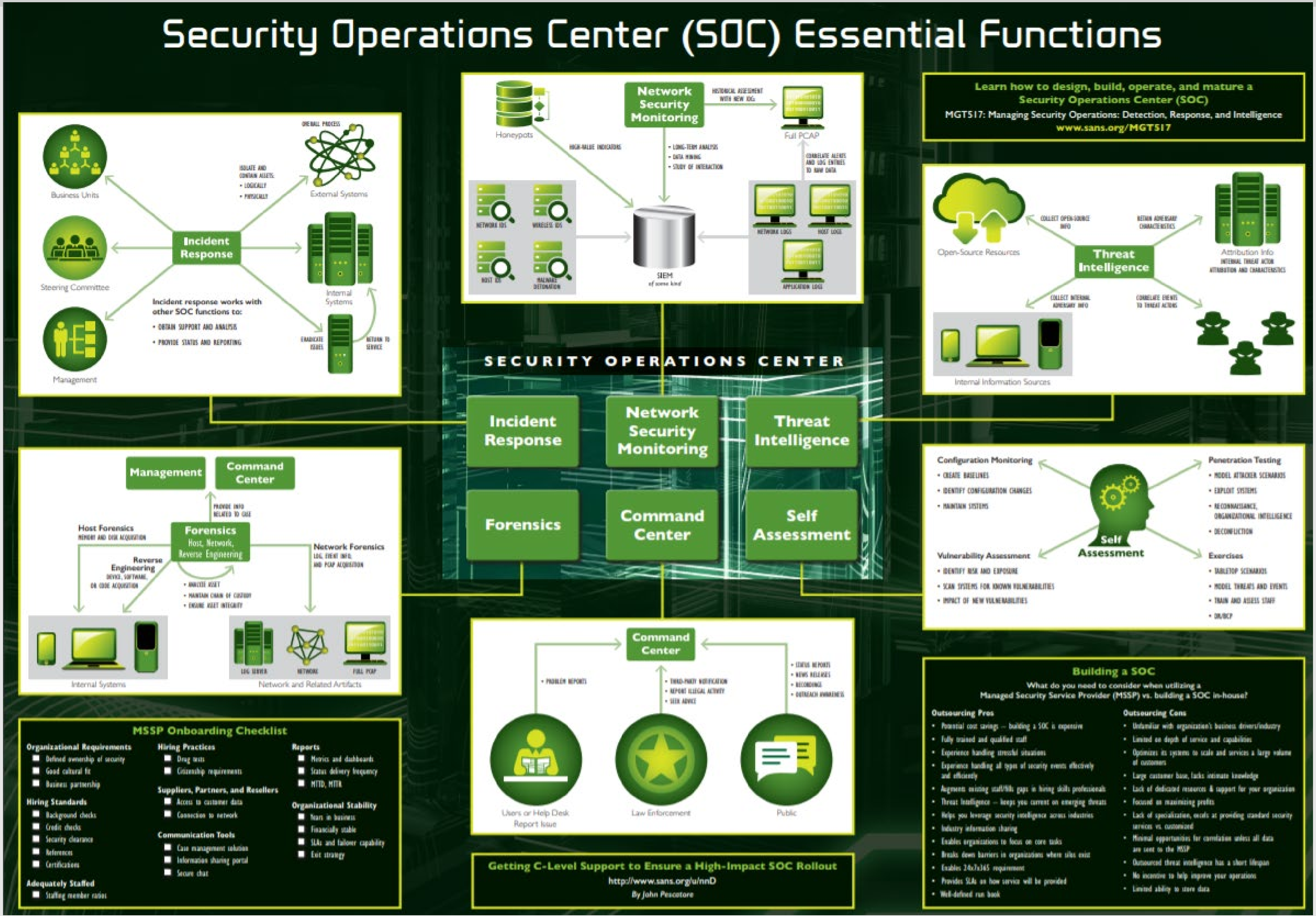
An information security operations center (ISOC) is a dedicated site where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.

- *Wikipedia "Security operations center"*

WHAT IS A CYBERSECURITY OPERATIONS CENTER? SOC? CSOC?

It's where all the zombie techs turn the geek knobs

WHAT DO SOCS DO?



Security Operations Center (SOC) Essential Functions

Incident Response

Business Units

Steering Committee

Management

OVERALL PROCESS

ISOLATE AND CONTAIN ASSETS:
- LOGICALLY
- PHYSICALLY

External Systems

Internal Systems

ERADICATE ISSUES

RETURN TO SERVICE

Incident response works with other SOC functions to:
- OBTAIN SUPPORT AND ANALYSIS
- PROVIDE STATUS AND REPORTING

Network Security Monitoring

Honeypots

HIGH-VALUE INDICATORS

HISTORICAL ASSESSMENT WITH NEW IOCs

Full PCAP

- LONG-TERM ANALYSIS
- DATA MINING
- STUDY OF INTERACTION

CORRELATE ALERTS AND LOG ENTRIES TO RAW DATA

NETWORK IDS, WIRELESS IDS, HOST IDS, MALWARE DETONATION

SIEM *of some kind*

NETWORK LOGS, HOST LOGS, APPLICATION LOGS

Learn how to design, build, operate, and mature a Security Operations Center (SOC)

MGT517: Managing Security Operations: Detection, Response, and Intelligence

www.sans.org/MGT517

Threat Intelligence

Open-Source Resources

COLLECT OPEN-SOURCE INFO

RETAIN ADVERSARY CHARACTERISTICS

Attribution Info
INTERNAL THREAT ACTOR ATTRIBUTION AND CHARACTERISTICS

COLLECT INTERNAL ADVERSARY INFO

CORRELATE EVENTS TO THREAT ACTORS

Internal Information Sources

SECURITY OPERATIONS CENTER

Incident Response | Network Security Monitoring | Threat Intelligence

Forensics | Command Center | Self Assessment

Forensics

Management

Command Center

PROVIDE INFO RELATED TO CASE

Forensics
Host, Network, Reverse Engineering

Host Forensics
MEMORY AND DISK ACQUISITION

Reverse Engineering
DEVICE, SOFTWARE, OR CODE ACQUISITION

- ANALYZE ASSET
- MAINTAIN CHAIN OF CUSTODY
- ENSURE ASSET INTEGRITY

Network Forensics
LOG, EVENT INFO, AND PCAP ACQUISITION

Internal Systems

LOG SERVER, NETWORK, FULL PCAP

Network and Related Artifacts

Self Assessment

Configuration Monitoring
- CREATE BASELINES
- IDENTIFY CONFIGURATION CHANGES
- MAINTAIN SYSTEMS

Penetration Testing
- MODEL ATTACKER SCENARIOS
- EXPLOIT SYSTEMS
- RECONNAISSANCE, ORGANIZATIONAL INTELLIGENCE
- DECONFLICTION

Vulnerability Assessment
- IDENTIFY RISK AND EXPOSURE
- SCAN SYSTEMS FOR KNOWN VULNERABILITIES
- IMPACT OF NEW VULNERABILITIES

Exercises
- TABLETOP SCENARIOS
- MODEL THREATS AND EVENTS
- TRAIN AND ASSESS STAFF
- DR/BCP

Command Center

- PROBLEM REPORTS

Users or Help Desk Report Issue

- THIRD-PARTY NOTIFICATION
- REPORT ILLEGAL ACTIVITY
- SEEK ADVICE

Law Enforcement

- STATUS REPORTS
- NEWS RELEASES
- RECORDINGS
- OUTREACH AWARENESS

Public

MSSP Onboarding Checklist

Organizational Requirements
- □ Defined ownership of security
- □ Good cultural fit
- □ Business partnership

Hiring Standards
- □ Background checks
- □ Credit checks
- □ Security clearance
- □ References
- □ Certifications

Adequately Staffed
- □ Staffing member ratios

Hiring Practices
- □ Drug tests
- □ Citizenship requirements

Suppliers, Partners, and Resellers
- □ Access to customer data
- □ Connection to network

Communication Tools
- □ Case management solution
- □ Information sharing portal
- □ Secure chat

Reports
- □ Metrics and dashboards
- □ Status delivery frequency
- □ MTTD, MTTR

Organizational Stability
- □ Years in business
- □ Financially stable
- □ SLAs and failover capability
- □ Exit strategy

Getting C-Level Support to Ensure a High-Impact SOC Rollout

http://www.sans.org/u/nnD

By John Pescatore

Building a SOC

What do you need to consider when utilizing a Managed Security Service Provider (MSSP) vs. building a SOC in-house?

Outsourcing Pros
- Potential cost savings – building a SOC is expensive
- Fully trained and qualified staff
- Experience handling stressful situations
- Experience handling all types of security events effectively and efficiently
- Augments existing staff/fills gaps in hiring skills professionals
- Threat Intelligence – keeps you current on emerging threats
- Helps you leverage security intelligence across industries
- Industry information sharing
- Enables organizations to focus on core tasks
- Breaks down barriers in organizations where silos exist
- Enables 24x7x365 requirement
- Provides SLAs on how service will be provided
- Well-defined run book

Outsourcing Cons
- Unfamiliar with organization's business drivers/industry
- Limited on depth of service and capabilities
- Optimizes its systems to scale and services a large volume of customers
- Large customer base, lacks intimate knowledge
- Lack of dedicated resources & support for your organization
- Focused on maximizing profits
- Lack of specialization, excels at providing standard security services vs. customized
- Minimal opportunities for correlation unless all data are sent to the MSSP
- Outsourced threat intelligence has a short lifespan
- No incentive to help improve your operations
- Limited ability to store data

THE CYBERSECURITY OPERATIONS MODELS

Network Security Monitoring

Incident Response

Forensics (or investigation support)

Threat Intelligence

Internal / External / Correlation Events

Self Assessment

Config monitoring / Vulnerability Assessments / PenTests / Tabletop exercises, etc

Command Center Operations

Reports / Budgets / Daily management

THE CYBERSECURITY OPERATIONS MODELS

Virtual SOC

Multifunction SOC/NOC

Co-managed SOC

Dedicated SOC (in-sourced)

Command SOC

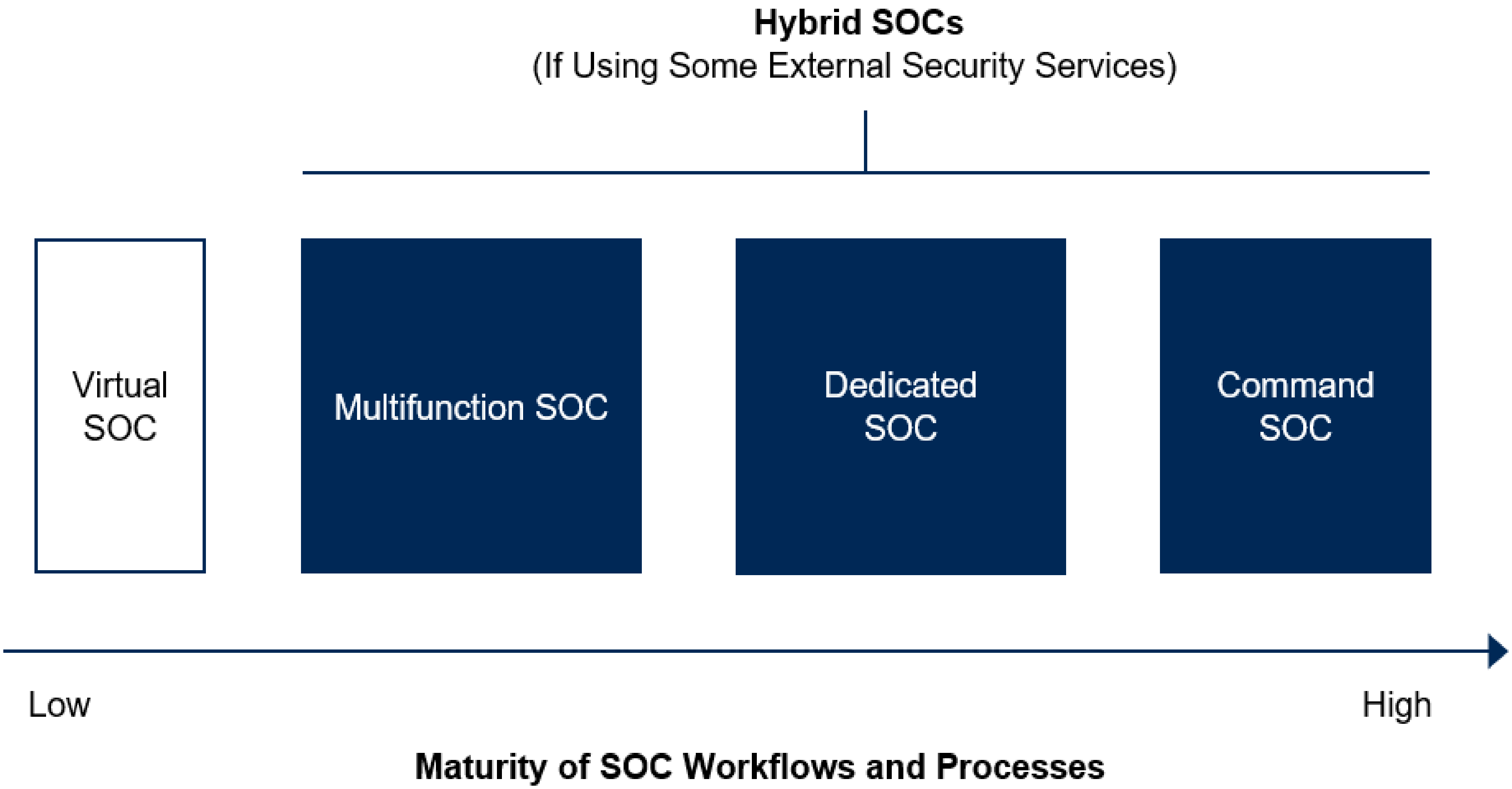
SOC-as-a-Service

State of Texas Hybrid Model

More as marketers are able to create them

THE CYBERSECURITY OPERATIONS MODELS

Five Models of SOC



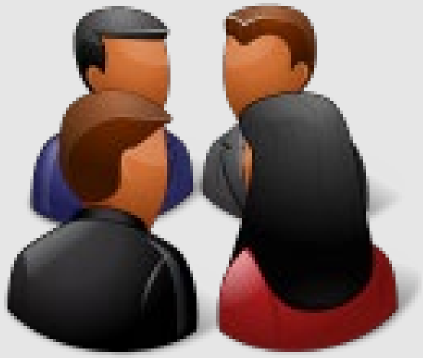
Hybrid SOCs
(If Using Some External Security Services)
Virtual SOC
Multifunction SOC
Dedicated SOC
Command SOC
Low
High
Maturity of SOC Workflows and Processes

Source: Gartner
ID: 464962_C

ALL IN-HOUSE: PROS AND CONS

Expensive

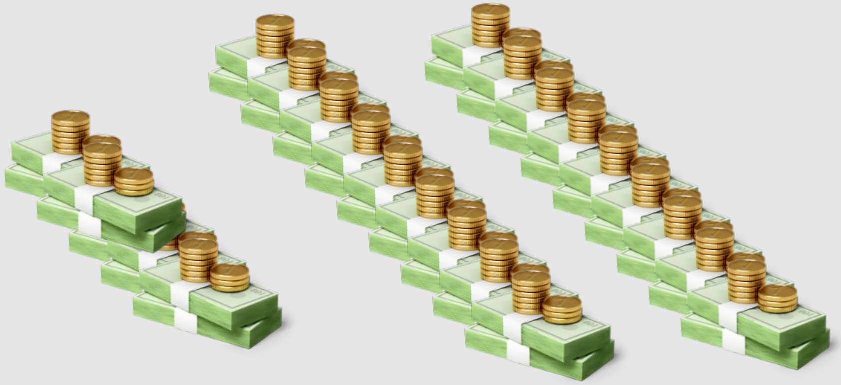
Talent



ALL IN-HOUSE: PROS AND CONS

OUTSOURCED: PROS AND CONS

Cheaper



Talent

OUTSOURCED: PROS AND CONS

- Lack of ownership: You’re company is a ‘one-of-many’ client that may not have the priority you think you do.
- Depending on where you are on your organizational chart, others may dictate your policies and/or your monitoring strategy

The ad-hoc, 1-off, custom model

© Randy Glasbergen
glasbergen.com

"This is a major project of utmost importance, but it has no budget, no guidelines, no support staff, and it's due in 15 minutes. At last, here's your chance to really impress everyone!"

HYBRID: BUILT TO NEED

DIR

Dept. of Information Resources

SUBCHAPTER C. NETWORK SECURITY CENTER

Sec. 2059.101. NETWORK SECURITY CENTER. The department shall establish a network security center to provide network security services to state agencies.

- NSOC was authorized by the Texas Legislature in 2007

HYBRID: BUILT TO NEED

CISCO
Freeit™
DATA SOLUTIONS
IBM®
Insight®
FutureCom
Cybersecurity Delivered.
INGRAM
Technologies
RSA
KPMG
ixia
flashback data®
netskope
salty cloud™
Akamai
Experience the Edge
CRITICALSTART
TANIUM™
Trustwave®

TXDOT: NEITHER OF THE PREVIOUS MODELS FIT

- Hybrid model to build a “best of both worlds”

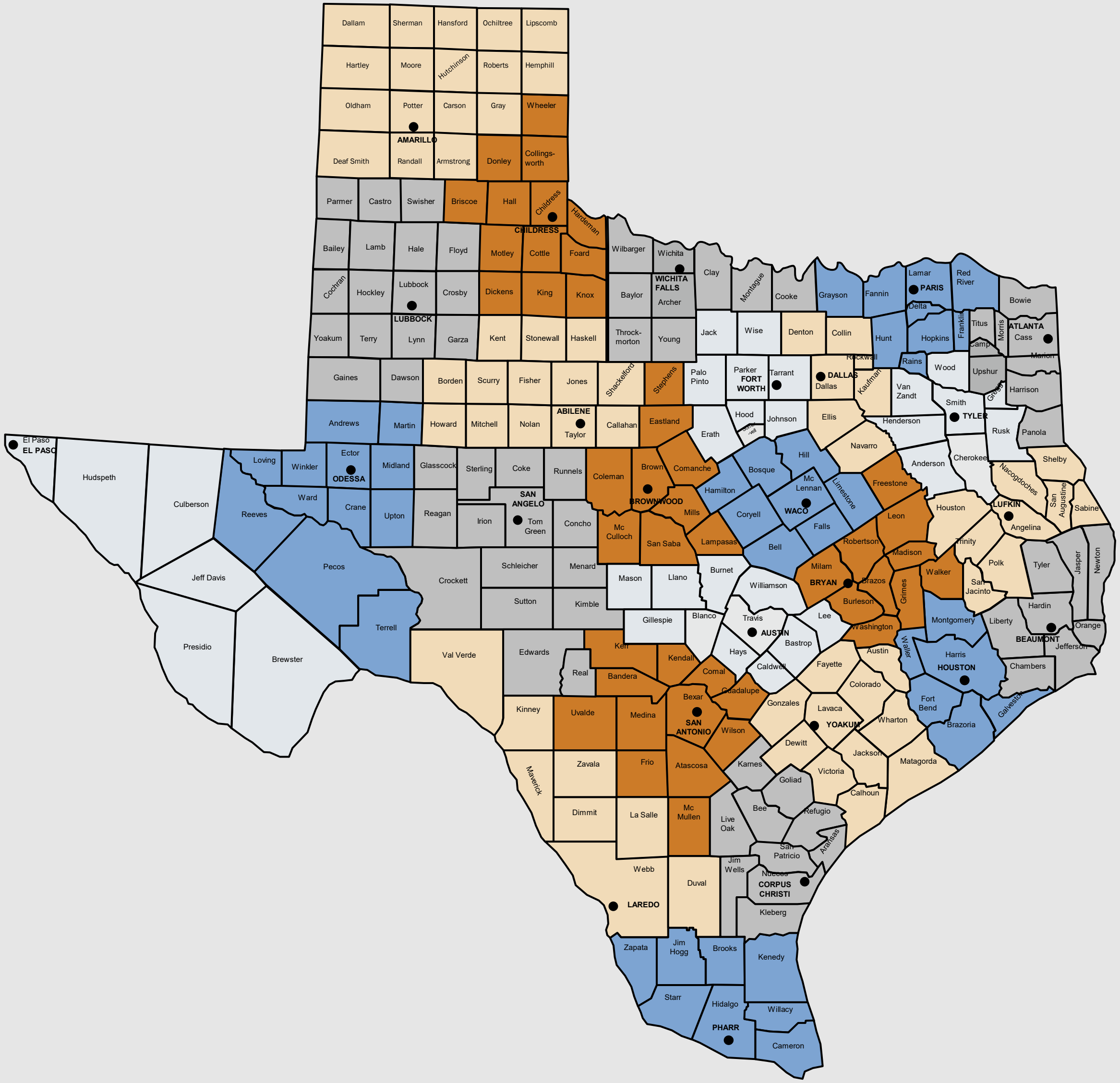
YES – THAT’S HANNA MONTANA

- Hybrid model to build a “best of both worlds”

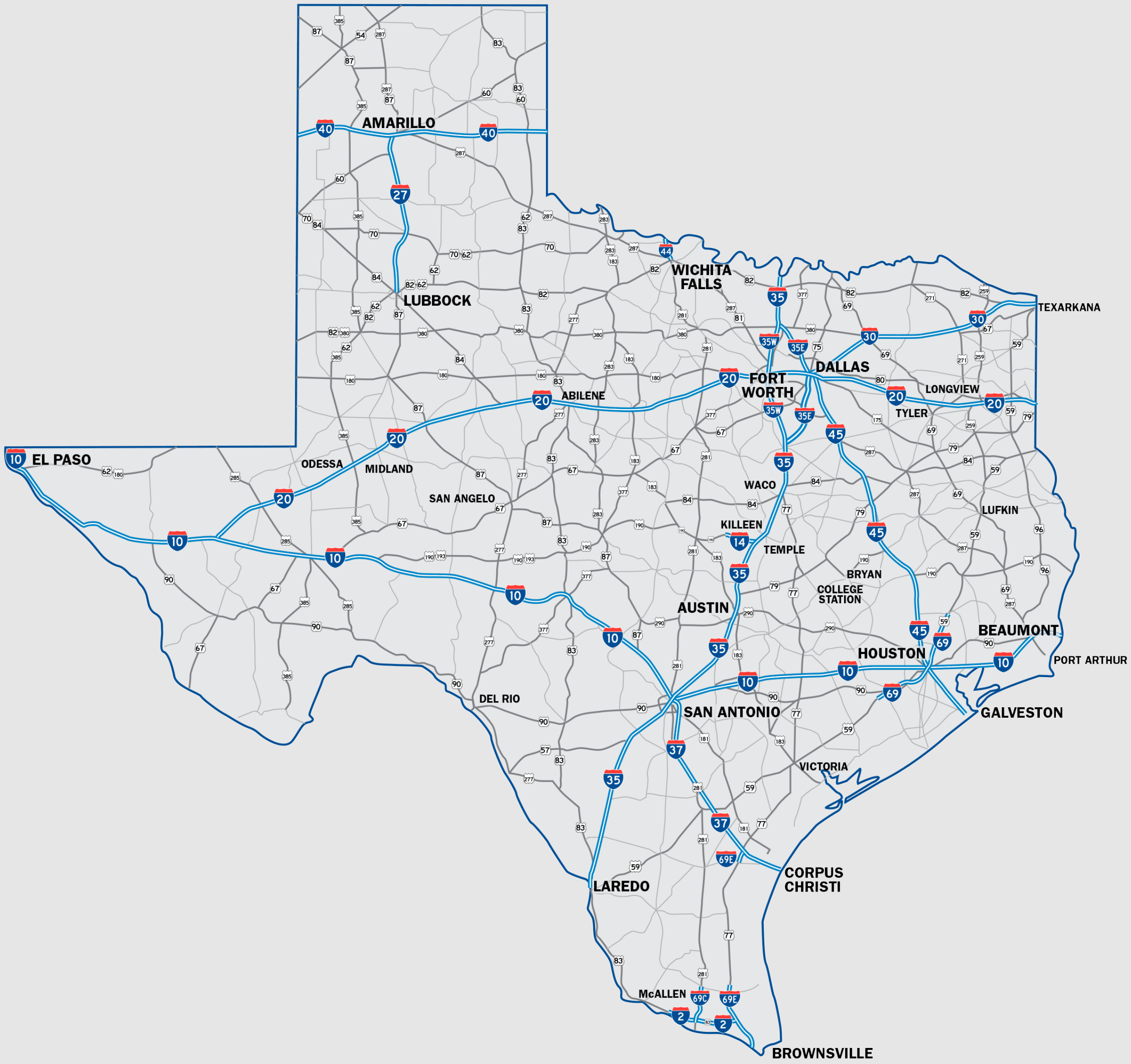
TXDOT: NEITHER OF THE PREVIOUS MODELS FIT

- Hybrid model to build a "best of both worlds"
- Scalable cost applicable to our mission/funds
- We wanted on-site personnel (ownership) that could be incorporated into the business
- Also wanted affordable 24/7 operations
- Apparently, the bad guys don't only attack while we're at work
  - Rude

TxDOT districts

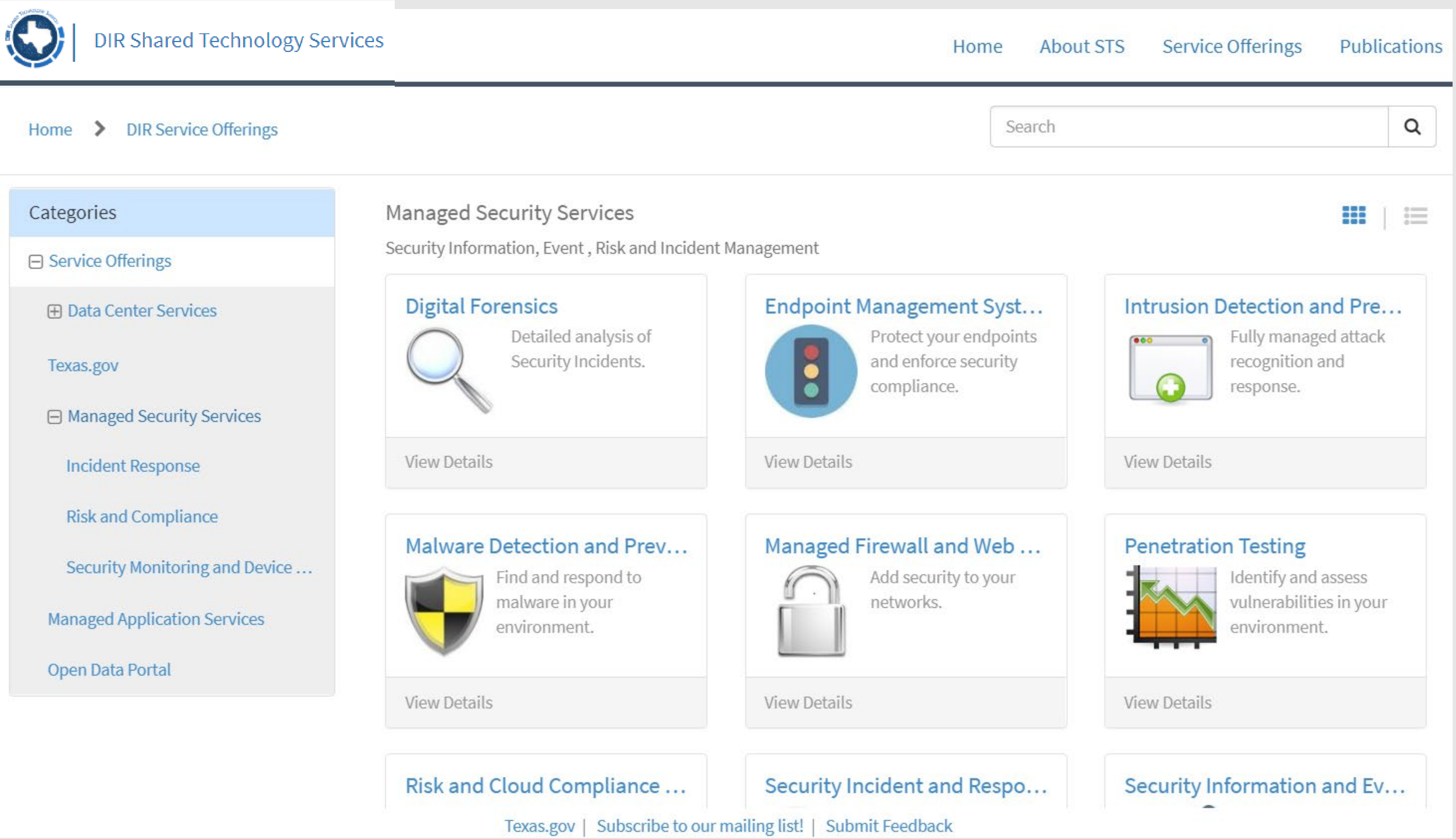


Texas Transportation System



DIR MANAGED SECURITY SERVICES TO THE RESCUE

DIR MANAGED SECURITY SERVICES TO THE RESCUE



Managed Security Services

Security Information, Event , Risk and Incident Management

Digital Forensics
Detailed analysis of Security Incidents.

Endpoint Management Syst…
Protect your endpoints and enforce security compliance.

Intrusion Detection and Pre…
Fully managed attack recognition and response.

Malware Detection and Prev…
Find and respond to malware in your environment.

Managed Firewall and Web …
Add security to your networks.

Penetration Testing
Identify and assess vulnerabilities in your environment.

Risk and Cloud Compliance …

Security Incident and Respo…

Security Information and Ev…

DISCUSSION