

DIR Shared Technology Services Outreach and Growth Webinar

Managed Security Services:
Security Monitoring and Device Management

August 25, 2021



Agenda



- | | |
|---|--------------------------------|
| 1. Introductions and STS Overview | Carrie Davie, Capgemini |
| 2. Managed Security Services | Mark Hooper, AT&T |
| 3. Security Monitoring and Device Management | Mark Hooper, AT&T |
| 4. MSS SMDM: Customer Experience | Mario Chavez, TDI |
| 5. Learn More and Join Us | Carrie Davie, Capgemini |

DIR Shared Technology Services Model



Multi-sourcing Services Integrator (MSI)

- Marketplace
- Service Management
- Business Management
- Operations Management
- Customer Relationship Management

Data Center Services

- Texas Private Cloud (TPC)
- Public Cloud Manager (PCM)
- Mainframe Services
- Technology Solution Services (TSS)
- Print, Mail, & Digitization

Texas.gov

- Payment Services
- Application Services

Managed Security Services

- Security Monitoring and Device Management
- Incident Response
- Assessments

Open Data Portal

- Official State Repository of Publicly Available Electronic Data

Managed Security Services

Mark Hooper

Client Solutions Executive - Cybersecurity, AT&T



Managed Security Services



AT&T is the Solution Component Provider (SCP) for Managed Security Services (MSS), a Program of DIR's Shared Technology Services with oversight from the MSI (Multi-sourcing Services Integrator). Through MSS, AT&T facilitates the provisioning of necessary security services for STS Customers.

MSS is comprised of three functional services, each containing multiple offerings to meet your IT security needs.



Security Monitoring and Device Management



Risk and Compliance



Incident Response

DIR's MSS offerings - billed and branded as DIR solutions - **include** AT&T services complemented by technology from select vendors.

DIR Shared Technology Services:

Managed Security Services

Multi-sourcing Services Integrator (MSI)

Capgemini

- Marketplace
- Service Management
- Business Management
- Operations Management
- Customer Relationship Management

Security Monitoring & Device Management

AT&T

- End-Point/EDR
- Intrusion Detection/Prevention
- Malware Detection/Prevention
- Managed Firewall/IPS
- Security Operations Centers
- SIEM
- Advanced Threat Hunting

Incident Response

AT&T

- Response Preparedness
- Incident Response and Resolution
- Digital Forensics

Compliance & Risk

AT&T

- Penetration Testing
- Vulnerability Assessments
- Security Risk Assessments
- Web Application Vulnerability Scanning
- Industry Focused Risk Assessments

STS Managed Security Services



Note: Many of these defined services can be custom-fit to customer needs

Security Monitoring and Device Management

Security Monitoring

- Security Information & Event Management (SIEM)
- 24x7 Security Operations Center (SOC)
- Threat Research
- Darknet Intelligence Monitoring
- Darknet Intelligence Assessment

Device Management

- Endpoint Detection & Response (EDR)
- Advanced Threat Hunting (ATH)
- Managed Next Gen Firewall Services (Small & Advanced)
- Web Application Firewall Services (WAF)
- Remote Rate Card Services for Network Device Installation
- Managed Secure Sensor + Setup
- Intrusion Detection/Prevention System Services (IDS/IPS)
- Host-based Intrusion Prevention Services (HIPS)

New Services

Risk and Compliance

- Penetration Testing
- Risk Assessments – HIPPA, PCI, NIST, IoT, BAC, Custom
- Industry Focused Risk Assessments
- Cloud Compliance
- Vulnerability Scanning
- Web Application Scanning
- Web Application Penetration Testing
- Texas Cybersecurity Framework Assessment (TAC 202)
- Election Systems Risk Assessments
- Election Systems Assessment Remediation

DIR-funded for state agencies, public colleges and universities as budget is available

Incident Response

- Security Incident Management
- Digital Forensics
- Response Preparedness

No Incident Response retainer is necessary for DIR MSS Customers

Can support an existing IR plan, or provide standalone service

MSS: Security Monitoring and Device Management

Mark Hooper

Client Solutions Executive – Cybersecurity, AT&T



Security Monitoring and Device Management



We help you **manage devices you own**

We **provide devices** that we manage and own

We help you **maintain continuous monitoring** of systems and networks 24/7 (SIEM)

We can provide a **full Security Operations Center**

We can provide services that are **custom tailored** to meet your security needs

SMDM Services



Next Generation
Firewall Services
(NGFW)

Intrusion Detection
and Prevention
Services (IDS/IPS)

Security
Information and
Event Management
(SIEM)

Web Application
Firewall Services
(WAP)

End Point Detection
and Response (EDR)

Advanced Threat
Hunting (ATH)

Security Operations
Center (SOC)

Darknet Assessment
and Monitoring



Next Generation Firewall Services (NGFW)

- Managed Next Generation Firewall (NGFW) is a managed solution that replaces an existing firewall with a system that combines traditional firewall functionality (i.e., access control lists, IP and domain blacklisting and whitelisting) with advanced network security capabilities including:
 - Intrusion detection and prevention
 - Anti-malware protection
 - Web filtering
 - SPAM protection
 - Data loss prevention
 - SSL inspection
- Service includes initial implementation as well as patching and maintaining the firewall and the enabled services

Security Information and Event Management (SIEM)



- Unique event correlation insights leveraging all State of Texas shared network data traffic at the DIR NSOC
- Fully staffed 24x7 SOC support in Austin, TX
- Next-gen threat hunting & investigation capacities powered by AT&T's fully managed SIEM
- Real-time threat response for all alerts from AT&T analysts
- Advanced threat feeds
- Detailed reporting
- SLA protections built into the DIR MSS contract
- Monthly touchbase meetings

Endpoint Detection and Response (EDR)



- The Endpoint Detection and Response solution allows for automatic detection and policy actions against Client's assets in accordance with Client's predefined security policy.
- Threat detection:
 - Provide the ability to detect malicious activity and anomalies on endpoints beyond just looking for file-based malware in accordance with Customer's security policy/requirements utilizing some of the following:
 - On-devices Static Artificial Intelligence (AI)
 - On-devices Behavior AI
 - Detection of Exploits and Malicious Scripts
 - Lateral Movement
 - Upon detection of a malware infection, immediately, as defined by the applicable Security Incident Severity Level, notify and respond to Malware infections as directed by Customer policy
 - The solution includes implementation and tuning as well as patching and updates. Client receives monthly reporting of activity (e.g., events, blocked, responded to, etc.)

Advanced Threat Hunting (ATH)



- Threat hunters begin from the premise that a breach has already occurred and proactively work to find those compromises. Typically focused on data mining and analysis of system event and security logs, 'traditional' threat hunting techniques rely heavily on the capabilities and expertise of the Threat Hunters alone.
- Advanced Threat Hunting (ATH) adds automated tools to increase the efficiency and effectiveness of the threat hunter
- Provides 24x7 monitoring of customer endpoints for known malware and other potentially suspicious or unwanted software stored or running on the device
- Leverages the State cloud based SIEM and the knowledge acquired through other MSS services
- Two Service Options
 - Single scan
 - Ongoing service
- Service includes implementation, tuning, scanning, real-time monitoring, and monthly reporting of IoCs and findings

Darknet Intelligence

Members of attacker communities have developed expansive networks and systems to support their needs in preparing for and executing cyber-attacks. These networks take the form of hidden and/or closed communities, forums, and marketplaces, often referred to as “The Darknet”.

One Time Scan (Assessment)

- Typically lasts 4-8 weeks
- Perspective of a cyber criminal
- Checking for vulnerabilities and malware
- Goes back ~1 year
- Deliverable is a report that explains analyst activities, vulnerabilities, and findings

Monthly Service (Monitoring)

- Similar to single scan, but with a focus on what is happening now
- Ongoing analysis of threats
- Monthly report on findings and recommendations

MSS: SMDM Customer Experience

Mario Chavez

Chief Information Security Officer, Texas
Department of Insurance (TDI)



Learn More and Join Us

Carrie Davie

MSI Communications Manager, Capgemini



STS External Portal

<https://dirsharedservices.service-now.com/dir>



- Designed for prospective STS customers, including governance (city, county, and state) and higher education
- STS Service Offerings catalog with high-level views and drill-down details
- Publications page featuring previous webinars and other helpful articles
- Eligibility details and sample agreements

The mission of the [Texas Department of Information Resources \(DIR\)](#) is to serve Texas government by leading the state's technology strategy, protecting state technology infrastructure, and offering innovative and cost-effective solutions for all levels of government. You can use the buttons, to the right or below, to gather more information about some of our service offerings such as Data Center Services or Managed Security Services.

What is STS?

The objective of DIR's Shared Technology Services Program is to supply access to managed IT as a Shared Service, allowing Customers to focus on supporting their mission and business functions rather than directly managing IT services.

STS Values

- Diverse Technology Solutions - Meeting customer needs today while anticipating future demands through proven industry best practices and research.
- Assurance - Services are competitively procured with secure, reliable, and scalable solutions provided by private sector industry leaders and designed to meet customer requirements.
- Customer Support - From procurement through operations, STS solutions offer flexibility, accountability, and agility to meet evolving business needs, while minimizing risk and maintaining business continuity. The STS program provides customers with technical expertise and responsive support using a single platform and enterprise governance structure.

Managed Security Services Webinar

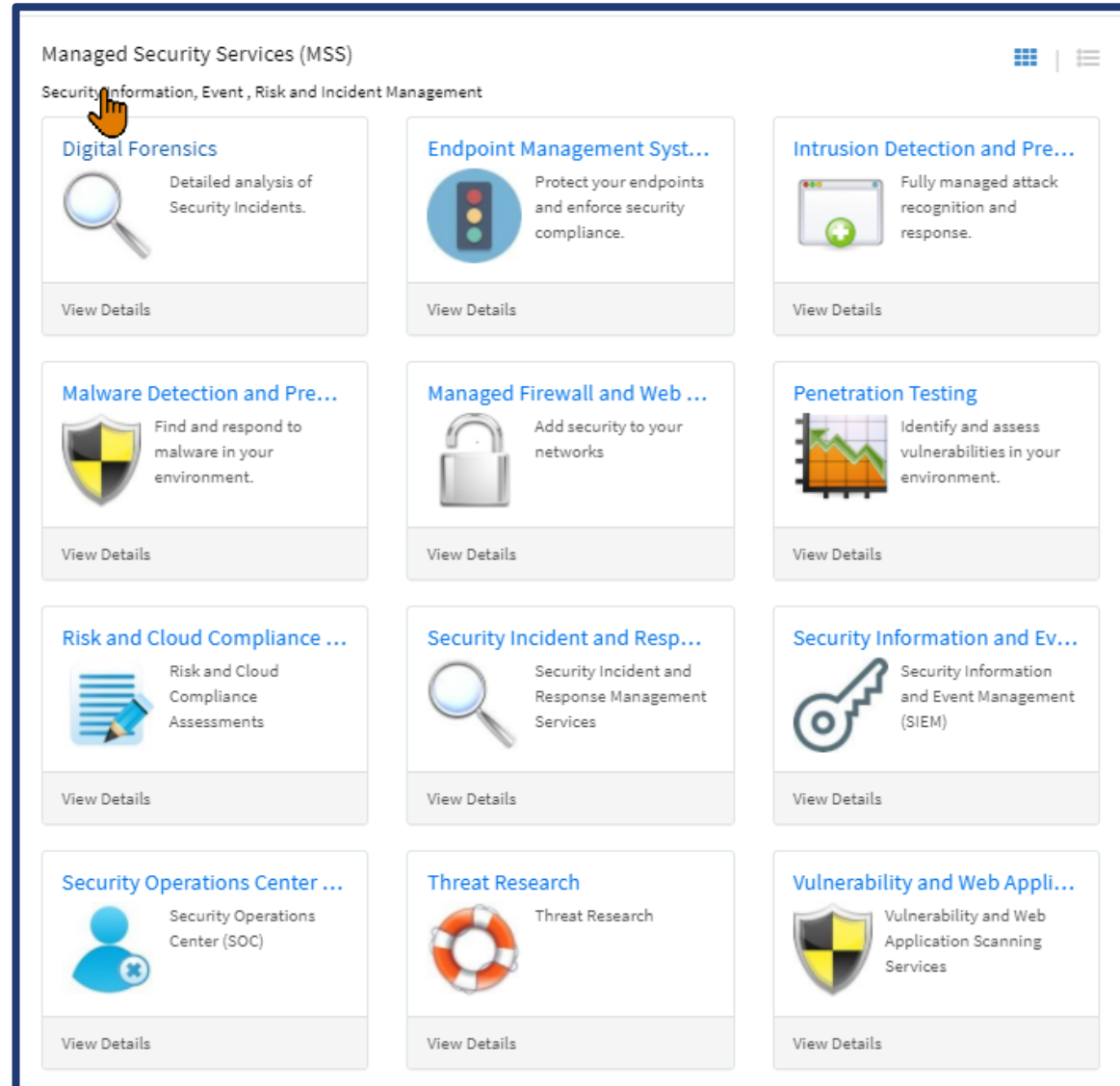
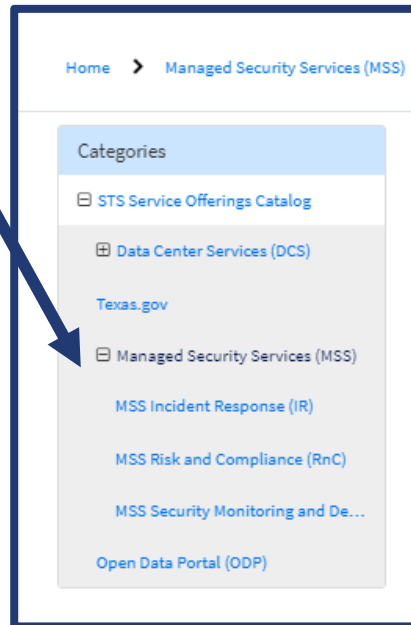
DIR Shared Technology Services

Texas.gov | [Subscribe to our mailing list!](#) | [Submit Feedback](#) | [Sitemap](#)

STS Service Offerings: Managed Security Services



Managed Security Services (MSS)

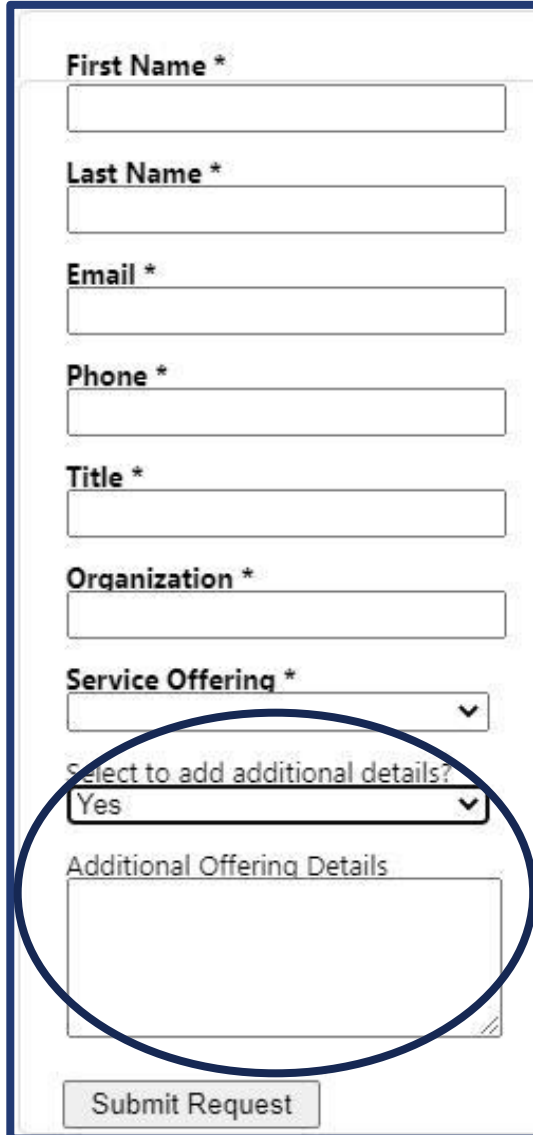


Request More Information about Service Offerings

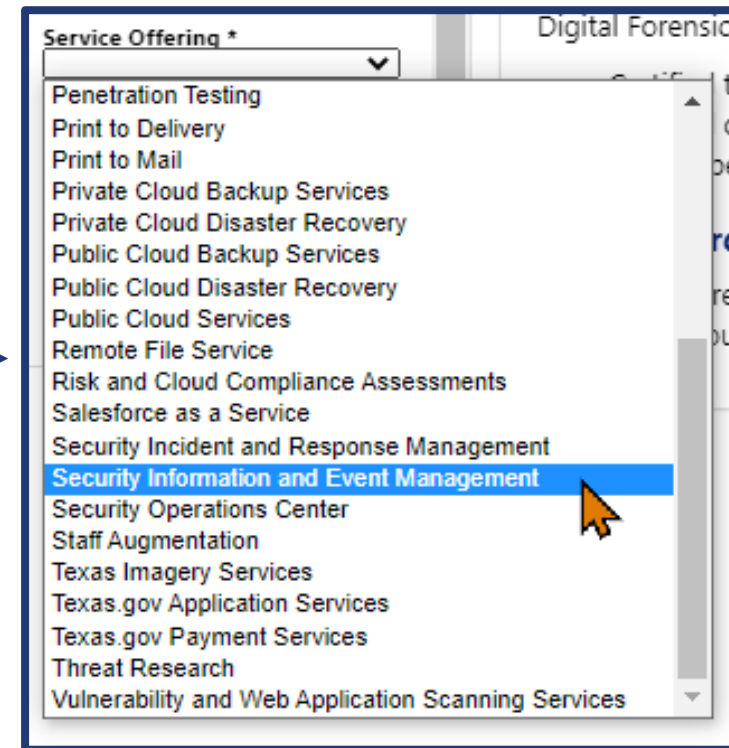
- Prospective Customers can submit a request on the offerings page to be contacted by our team.
- Current Customers should submit a Request For Solution (RFS) via the Service Catalog.

Mandatory fields

Provide additional information about your needs to help get your request to the right person faster.



A screenshot of a web form titled "Request More Information about Service Offerings". The form contains several input fields: "First Name *", "Last Name *", "Email *", "Phone *", "Title *", "Organization *", "Service Offering *" (a dropdown menu), "Select to add additional details?" (a dropdown menu with "Yes" selected), and "Additional Offering Details" (a text area). A blue circle highlights the "Additional Offering Details" text area. A "Submit Request" button is at the bottom. A bracket on the right side of the form groups the first six fields under the label "Mandatory fields".



A screenshot of a dropdown menu titled "Service Offering *". The menu lists various service offerings: Penetration Testing, Print to Delivery, Print to Mail, Private Cloud Backup Services, Private Cloud Disaster Recovery, Public Cloud Backup Services, Public Cloud Disaster Recovery, Public Cloud Services, Remote File Service, Risk and Cloud Compliance Assessments, Salesforce as a Service, Security Incident and Response Management, Security Information and Event Management (highlighted with a blue background and a mouse cursor), Security Operations Center, Staff Augmentation, Texas Imagery Services, Texas.gov Application Services, Texas.gov Payment Services, Threat Research, and Vulnerability and Web Application Scanning Services. The dropdown is part of a larger form with a "Digital Forensic" tab visible.



Eligibility and Contract Requirements

Prior to receiving Shared Technology Services from DIR, all customers must sign either an Inter-Agency Contract (IAC) or an Inter-Local Contract (ILC). In addition, each Program has Terms and Conditions that must be accepted.

Who is eligible?

- State Agencies
- Public Institutions of Higher Ed
- Local Governments
- Public School Districts
- LCRA

Note: Public community colleges are eligible to participate only in Managed Security Services (MSS) and Texas.gov.

Contract Document Previews

- [Shared Technology Services IAC](#)
- [Shared Technology Services ILC](#)
- [Data Center Services Terms and Conditions](#)
- [Texas.gov Terms and Conditions](#)
- [Managed Security Services Terms and Conditions](#)
- [Open Data Portal Terms and Conditions](#)

(Find these on the External Portal's Eligibility page.)

Service Offering of the Month and Email Subscriptions



2021	Topic	SCP Presenter
August	MSS Security Monitoring and Device Management	AT&T
September	Open Data Portal	Socrata & DIR
October	DCS Technology Solution Services - Application Services	Deloitte
December	MSS Incident Response and Risk & Compliance	AT&T

Find past webinar recordings and decks on the External Portal, where you can also subscribe to our mailing list:



Our campaigns include weekly emails about our offering of the month and are sent to a wide base of potential Customers. Only those who subscribe will receive invitations to our webinars.

Contact Us

Carrie Davie

MSI Communications Manager, Capgemini

carrie.davie@capgemini.com

Mark Hooper

Client Solutions Executive - Cybersecurity, AT&T

mark.hooper@att.com





STS is powered by the
following providers:

Atos

Capgemini 

rackspace
technology

 Socrata

xerox™

 **AT&T**

Deloitte.

SAIC
Redefining Ingenuity

TEXAS  **NIC**