Finding the Blind Spots.



Why SC Metro is taking action.

INCIDENTS, 2016–2026



Sources: The Register; PhillyVoice; StateScoop; Comparitech; ABC7 Los Angeles.

Aug 2025 – SEP 2028

IT Strategic Plan

Elevate IT Service Delivery

- Customer Experience First
- Adopt Best Practices (ITIL Framework)
- Enterprise Systems Support
- Strategic Implementation of AI Tools

Strengthen the Network

- Add Redundancy and Reliability
- Rationalize Legacy Technology

Enhance Cybersecurity Posture

- Culture of Security Awareness
- Continuous Risk Management
- Governance and Compliance

Year 1 · Aug 2025 – SEP 2026

IT Strategic Plan Progress

Elevate IT Service Delivery

- Implement ITIL Framework
- Implement an IT service delivery solution (ITSM)
    - Incident management
    - Request management
    - Change management
    - Support portal and service catalog
    - Problem management
- Support enterprise wide

Strengthen the Network

- Added secondary internet service
- Fortinet core firewall upgrade
- Core router replacement
- Domain consolidation

Enhance Cybersecurity Posture

- Threat and vulnerability assessments
- VPN MFA, LDAPS and DMARC/SPF
- Security, DR, IR, PCI and AI policies reviewed/drafted
- Service and system monitoring
- Remote device management

Discoveries and Results

73	33%	67%	1500+	7
Services Identified	On-premise	SaaS	Devices on Network	Security Incidents

IDENTIFY

- ITSM and asset inventory
- Threat and vulnerability assessment
- NinjaOne remote management tool
- Fortinet firewall tools
- Network discovery scans

Physical inventory, software scans, documentation.

SEPARATE

- Fortinet core firewall upgrade
- SD-WAN moves non-business traffic to Comcast
- Deny policy for known internet threats (Teams)
- Isolate legacy system
- DMARC and SPF hardened

New hydrogen station is on a separate network.

DETECT

- Regular logs audit
- Firewall alerts
- M365 reviews
- Vulnerability scans
- LibreNMS and Kuma Uptime system monitoring

Blind Spot: Monitoring the ITS equipment

RESPOND

- All incidents tracked in our ITSM system
- After incidents report generated
- Collect logs and artifacts for forensic analysis

Blind Spot: Incident response plan needs to be created

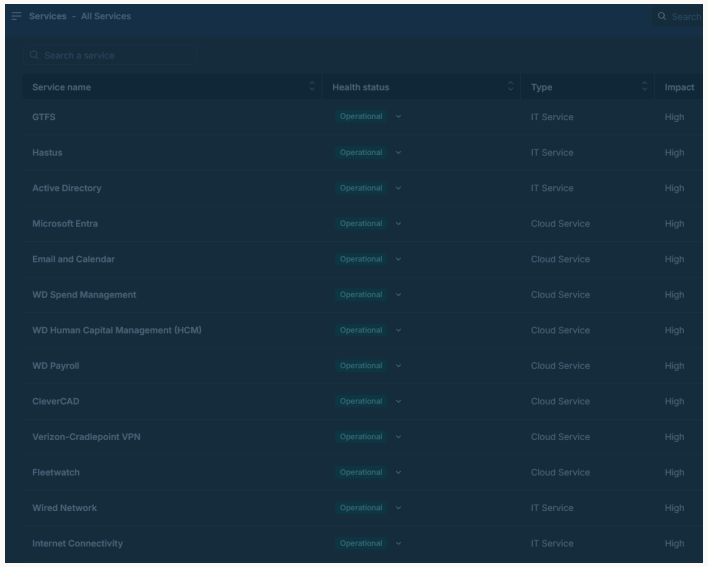
RECOVER

- Second ISP live at Admin
- DR and incident response policies drafted

Blind Spot: Connectivity in remote areas

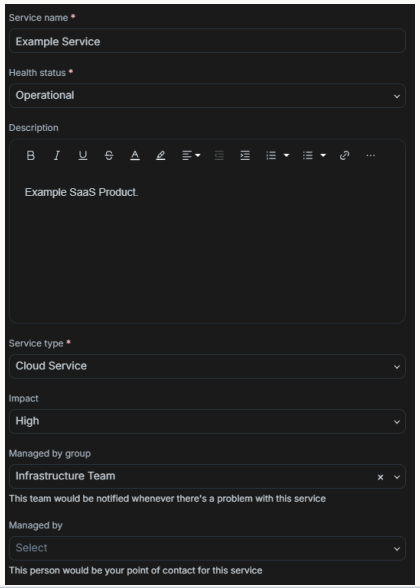
Focus on Mapping Out Services

Service Inventory and Prioritization



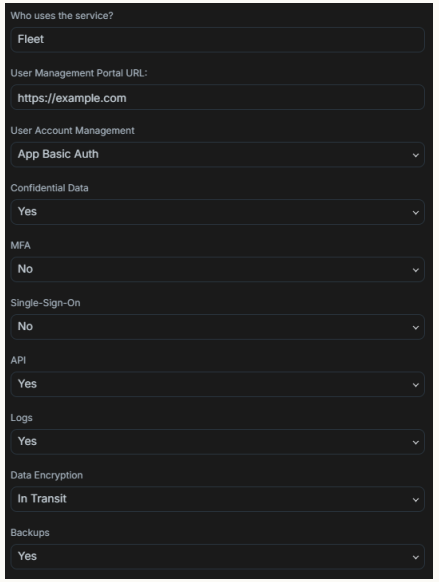
Identify all services (Including IT tools)

Document Key Information



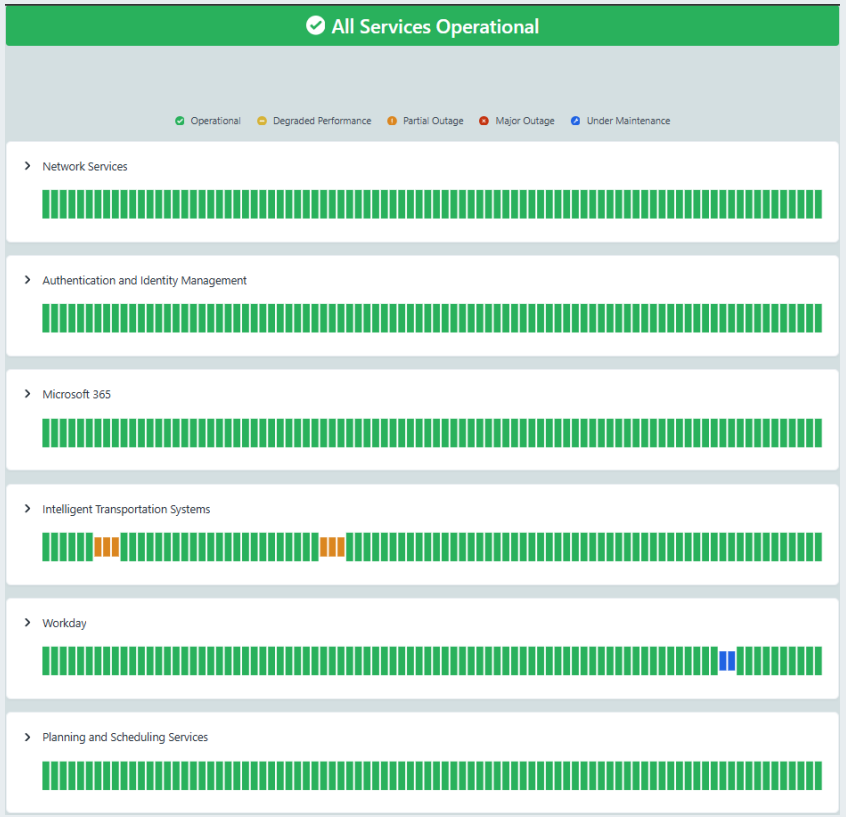
- Service name
- On-premise or SaaS
- Priority
- System owner

Additional Information



- Who uses the service?
- How are users managed?
- Does it contain confidential information?
- Logs, backups, encryption, etc.

Service Uptime, Maintenance and Dependencies



Service Status Page

Urgent Maintenance: Firewall Update. 10/28/2026 @ 7:00 AM – 7:30 AM

Upcoming Oct 28, 07:00 am - Oct 28, 07:30 am (PDT) Estimation Duration: 30 minutes

Firewall Update

IT will be performing urgent maintenance on our primary firewall device. This maintenance is necessary to ensure system security, stability and prevent future disruptions.

Please visit the IT Status page for additional information and updates: Santa Cruz Metro-IT...

Impacted Services

Network Services / Internet Connectivity Wired Network VPN

Scheduled Maintenance for mSET Vehicle Camera System

Oct 12, 01:30 pm - Oct 12, 03:30 pm (PDT) Duration: 2 hours

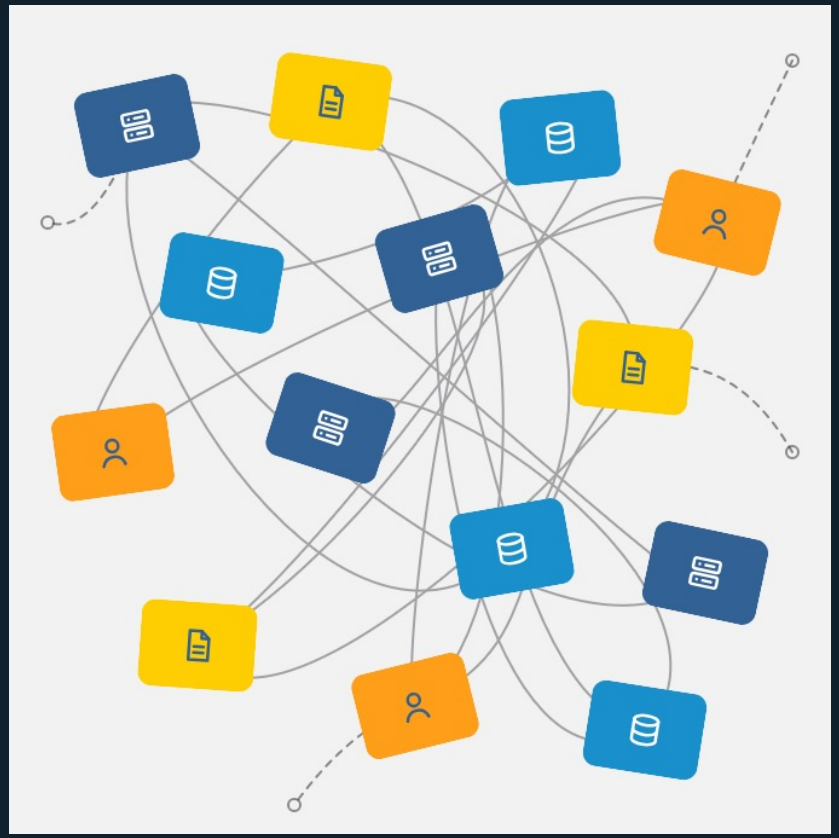
IT and the vendor will be performing an upgrade to mSET vehicle camera video servers. This maintenance is necessary to ensure system stability and update from version 2.1.3 to 2.4.3. The services listed below may be unavailable during the maintenance window.

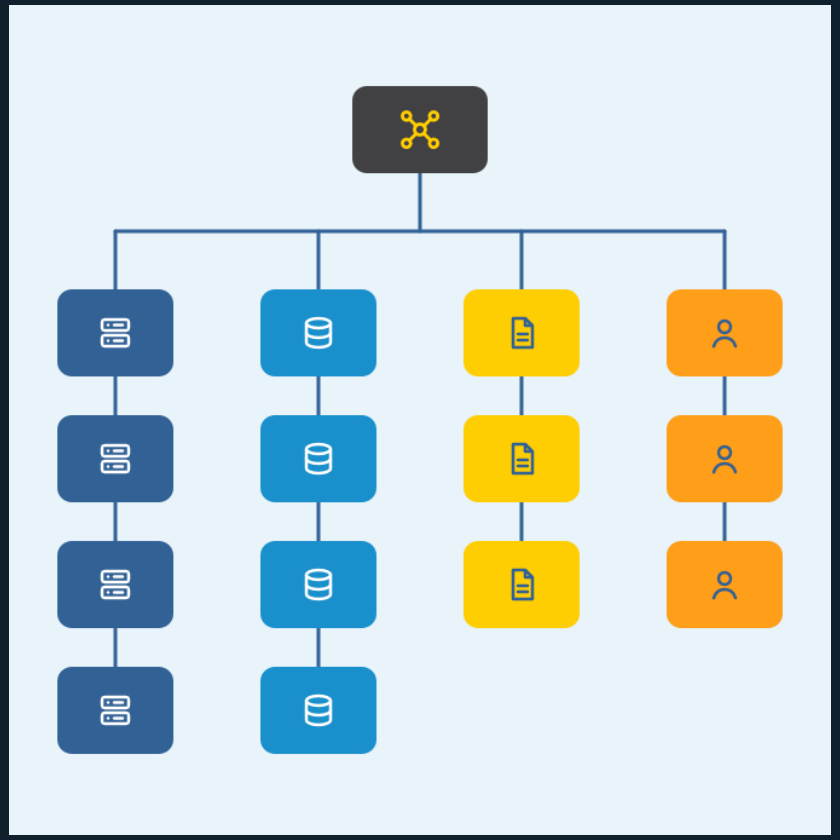
Services Impacted: ...

Impacted Services

Vehicle and Building V... / mSET ParaCruz Cameras mSET Fixed Route Cameras

Maintenance Communication





THANK YOU