ATS Security Incident Response Team (SIRT)

Operating out of our Security Operations Center in Atlanta, GA, ATS's Security Incident Response Team (SIRT) acts as a critical first line of defense against cyber threats. Offering 24/7 support, SIRT engages advanced technologies and methodologies to promptly identify, address, and mitigate incidents.

Endpoint Detection and Response (EDR)

Purpose: Enable real-time threat response across the network.

Functionality: Detects, isolates, and responds to threats as they emerge, helping protect critical assets and limit potential impact.

Advanced Digital Forensics

Purpose: Identify root causes of incidents and detect vulnerabilities.

Functionality: Uses technical expertise to uncover attack vectors, enabling thorough analysis and mitigation of threats.

ATS IR Tools

Digital Forensic Imaging

Purpose: Preserve digital evidence for reliable incident analysis.

Functionality: Secures data integrity for forensic investigations, supporting data recovery and incident timeline accuracy.

Security Information and Event Management (SIEM)

Purpose: Provide centralized oversight of IT environments for swift incident detection.

Functionality: Utilizes proactive monitoring, event correlation, and detailed incident visibility for comprehensive threat management.