ACS Security *Operations*

ACRISURE® CYBER SERVICES

Endpoints & Devices (R7 Agent, MDE)

SaaS Applications (Meraki, O365, etc)

All Servers (R7 Agent, MDE)

Network Devices (Meraki, R7, MDE)

Identity Providers (Entra ID)

Email Systems (O365)

Threat Intel Scraping

Agent-based telemetry: file/process activity, registry, login, network connections, full process context.

Logs, endpoint telemetry, network data, user authentication logs, cloud configs, cloud alerts & vulnerability scans.

API-based access to cloud email systems; ingests messages, metadata, attachments, user behavior, directory.

Clear and Dark Web crawling of client identifiers (identities, key words, public assets, etc.).

Log & Telemetry Ingestion

Endpoint Detection & Response
SentinelOne

Advanced AI Email Security
Abnormal

Vulnerability Management
RAPID7

***ACS* Threat Intelligence**
ACRISURE CYBER SERVICES

Alert & Investigation Generation

Account Takeover Notifications
Abnormal

Automated remediation (Session Revocation, Account Disablement) for high-confidence Account Takeover alerts immediately to reduce dwell time.

***Acrisure Cyber Services* SOAR & MDR Team**

1. Case Creation
2. Context Enrichment
3. Investigation

Disposition Assignment

True Positive (Malicious)
Confirmed threat actor behavior or malicious infrastructure.

Unknown Suspicious
Anomalous activity; unable to correlate to user/device.

Unknown Benign
Anomalous activity; correlated to user device/location but unauthorized or unrecognized.

Informational
Validated behavior (e.g., known travel, VPN use).

False Positive
Non-threat. Case Closure.

Endpoint Remediation
MDE Live Response
Device Isolation
(MDE/R7)

Identity Remediation
Account Disablement
Session Revocation
Password Reset

Respond

Incident Response

Detect

Threat Hunting
Active hunting of identified IoCs across the client environment

Recover

Client Communications
Ongoing Collaboration and communication between the ACS MDR team and the client.

Request for Information
Inform client of activity, share identified context & behaviors and request confirmation of the activity.

Informational Alert
Inform client of activity if it may break internal policy or followup is recommended.

Incident Notification
Inform client of Security Event, communicate remediation actions already taken and provide remediation guidance.

Learn More at
www.acrisurecyber.com