INCIDENT RESPONSE USE CASE

Remote Admin Access Into Government IT Systems

An incident response use case showing how REMI turns enterprise IT event logs and source records into a cyber SITREP with confirmed findings, unresolved questions, and immediate next steps.

At 7:08 AM, the help desk manager at Riverside County Services noticed that several user lockout tickets arrived before business hours. The network was operating, but the pattern was wrong: an administrator account showed overnight VPN access, a domain controller recorded unusual directory queries, and a file server showed access to folders tied to public records operations.

The help desk manager reported it to the county IT director, who reviewed the remote-access console and saw a VPN session from **admin.mercer** at **2:13 AM**. The account belonged to a county systems administrator, but the login came from **203.0.113.54**, a source IP outside the normal access baseline. The session first reached **10.60.18.22** on the internal network, then traffic appeared later toward **DC-02** and **FILES-PUBLIC-04**.

That changed the concern from routine lockouts to state-actor credential use against government IT systems. The warning signs were connected behaviors: off-hours administrator VPN access, a new source location, domain controller queries, file-server access, and user account changes that did not line up with the approved support window.

Investigator Arrives Onsite

Later that morning, the investigator arrives onsite at **Riverside County Services**. The investigator speaks with the help desk manager who noticed the lockout pattern, the county IT director who reviewed the VPN session, the identity administrator responsible for **DC-02**, and the records systems owner responsible for **FILES-PUBLIC-04**.

After those conversations, the investigator requests copies of the available event logs and source records so they can be analyzed in REMI. The goal is to determine how the administrator account, remote VPN session, internal destination, domain controller queries, account changes, and file-server activity fit together as a cyber attack path. The more complete the log package is, the wider the investigative coverage becomes.

Event Logs to Request

- **VPN and remote-access logs** showing sessions, source IPs, timestamps, device posture, destination systems, and session duration.
- **Identity and domain controller logs** showing logons, directory queries, privilege use, group changes, lockouts, Kerberos activity, and account modifications.
- **MFA and conditional access records** showing approvals, device state, location signals, token activity, and access policy results.
- **Firewall and network flow logs** showing internal destinations, lateral movement, blocked traffic, allowed traffic, and outbound connections.
- **EDR telemetry** showing process activity, command shells, file creation, credential access, scripts, callbacks, and persistence.
- **File-server access logs** showing folder enumeration, reads, exports, writes, and timestamps.
- **Change tickets, admin work orders, asset-owner records, and support schedules** showing whether the activity matched authorized work.

REMI Flagged

- **Remote administrator VPN login** by **admin.mercer** at **2:13 AM**.
- **New source IP** of **203.0.113.54** for that administrator account.
- **Internal network access** to **10.60.18.22** after the VPN connection.
- **Domain controller queries** involving **DC-02** during the same overnight window.
- **File-server activity** involving **FILES-PUBLIC-04** after the domain activity.
- **Shared evidence links** across account, IP address, timestamp, internal destination, domain activity, file access, and support records.

Correlation and SITREP Output

The raw logs are imported into REMI for analysis. REMI identifies the flagged behaviors inside the evidence package, then correlates records that share the same administrator account, source IP, session window, internal destination, domain controller event, file-server record, and support timestamp.

REMI Correlated

- **VPN session and administrator account** linked through **admin.mercer**, the **2:13 AM** session window, and remote-access records.
- **New source IP and internal destination** linked from **203.0.113.54** to **10.60.18.22** through VPN and firewall records.
- **Internal access and directory activity** linked by timestamp to **DC-02** domain controller queries.
- **Domain activity and file-server access** linked through the same administrator session and later movement toward **FILES-PUBLIC-04**.
- **Shared evidence path** connecting account, source IP, VPN session, internal destination, domain controller, file server, and support records.

SITREP Output Includes

- **Confirmed findings** showing what the evidence proves.
- **Unresolved questions** showing what still needs confirmation.
- **Additional source data needed** to close specific answer gaps.
- **Questions to ask IT, security, cloud, identity, vendors, and system owners.**
- **Artifacts to preserve or sandbox** before cleanup.
- **Malware paths, generated scripts, services, or scheduled tasks to remove** after preservation.
- **Verification steps** to confirm the activity does not return.

How REMI Reconstructs It

The following simulated incident response excerpt shows the level of case-specific detail REMI can produce inside a SITREP. Names, accounts, IP addresses, systems, files, and records are examples, but the structure reflects the level of detail REMI is designed to generate from the evidence package.

Remote Admin Access Into Government IT Systems

REMI confirmed that **admin.mercer** established a VPN session at **2:13 AM** from **203.0.113.54**. The session reached **10.60.18.22** on the internal network, and firewall records later showed traffic from that path toward **DC-02** and **FILES-PUBLIC-04**.

REMI correlated the **administrator login**, **source IP**, **internal destination**, **domain controller queries**, **account lockout events**, and **file-server activity** into one evidence path. The activity occurred during the same overnight window in which help desk records showed account issues outside the approved support schedule.

The SITREP identified confirmed findings, including the **VPN session**, **administrator account**, **source location**, **internal destination**, **domain controller activity**, and **file-server access**. It also identified unresolved questions: who controlled **admin.mercer** during the access window, whether MFA was approved by the assigned administrator, whether **10.60.18.22** was used as an intermediate system, and whether files were exported from **FILES-PUBLIC-04**.

REMI generated immediate next steps: preserve VPN logs, MFA records, domain controller logs, firewall flows, EDR telemetry, file-server audit logs, and help desk ticket history; disable exposed tokens tied to **admin.mercer**; isolate **10.60.18.22** after preservation when EDR confirms tool execution; review **DC-02** changes; and verify that account activity and file-server access return to expected behavior.