Identity Forensics & Incident Response (IFIR) Services

When organizations experience a cyberattack, identity systems are often the primary target—especially Active Directory (AD) and Entra ID, used by over 90% of enterprises worldwide. Attackers commonly go after highly privileged identities and embed backdoors to maintain access. Historically, recovery required a full AD rebuild—a costly, months-long effort with serious operational impact.

Semperis Identity Forensics & Incident Response (IFIR) addresses the entire lifecycle of an identity-layer attack. Our specialized team provides rapid containment, forensic investigation, and secure recovery to minimize downtime and prevent reinfection.

Why IFIR?

Traditional Digital Forensics & Incident Response (DFIR) typically focuses on endpoint and network activity. IFIR addresses a critical layer—the identity system—where attackers most often establish persistence. With identity systems like AD and Entra ID, recovery and containment are just as critical as investigation. Semperis IFIR helps you restore operations securely and minimize the chance of attackers regaining access.

- Analyze precisely what attackers did within AD and Entra ID
- Quickly lock down identified compromised accounts to contain the attack
- Detect and remove hidden backdoors and dangerous misconfigurations within AD
- Restore AD to a trusted, hardened state—without requiring complete rebuilds

IFIR Services Components

Our experts don't just clean up the mess—they reduce your long-term risk.

Identity-specific forensics

- **Triage and lockdown**: Immediately restrict admin access to known, trusted personnel and isolate critical identity infrastructure
- **Investigation**: Analyze the lifecycle of compromised accounts and trace attacker behavior within AD, if available
- **Containment**: Address identity-specific vulnerabilities and misconfigurations to prevent attacker re-entry
- **Recovery**: Remove potentially malicious changes and ensure the AD environment is clean and trustworthy
- **Post-incident review**: Provide recommendations to improve long-term identity security posture

Reducing attack surface

- **Hunt for backdoors**: Identify and eliminate persistence techniques such as ACL abuse, SID history injection, and Group Policy manipulation
- **Strengthen defenses**: Proactively identify and remediate weak configurations based on AD security best practices

Incident response integration

- **Containment and recovery**: Seamlessly integrate identity-layer response with broader DFIR workflows
- **Secure restoration**: Ensure AD is restored to a known-good, hardened state to prevent follow-on attacks

> "Attackers often target critical infrastructure components such as Active Directory and configuration data associated with devices such as storage arrays. If successful, these attacks make recovery without paying the ransom more difficult and time-consuming."
>
> **Gartner**
>
> "How to Protect Backup Systems from Ransomware Attacks"

Recovery Options

Brownfield (preferred approach)

Restore and secure your existing AD environment without a complete rebuild. This approach balances security, speed, and business continuity—enabling rapid recovery while reducing risk.

Greenfield (extreme cases)

In extreme cases, starting fresh with a new AD forest might be necessary. While this approach removes all legacy threats, it also demands reconfiguring applications, migrating users, and rebuilding integrations—making it costly and disruptive.

With Semperis IFIR, most organizations can avoid greenfield recovery by taking a secure brownfield approach that eliminates attacker persistence and misconfigurations.

IFIR Outcomes

- **Accelerated recovery:** Restore AD in hours—not days or weeks
- **Reduced business disruption**: Maintain operations during recovery
- **Risk elimination**: Identify and remove misconfigurations and backdoors
- **Future-proof hardening**: Minimize future breaches with proactive defenses
- **Specialized expertise**: Get identity-layer expertise not covered by typical IR vendors

IFIR Services vs Standard and Premium Support

Capability	Standard Support	Premier Support	IFIR Services
General Semperis product support	✓	✓ (24/7)	X (unless bundled)
AD recovery support and post-breach assessment	✓ Next business day response, includes basic investigation	✓ 1-hour response, includes catastrophic AD outage basic investigation	✓ Full AD recovery including investigation and remediation support
Restore AD in an isolated environment (if required)	✓	✓	✓
Active Directory Security Assessment (ADSA)	X	ⓘ	✓
Identify indicators of compromise or exposure	X	ⓘ Limited	✓
Review AD, SIEM, and system logs	X	X	✓
Lock down AD and reduce the attack surface	X	X	✓
Analyze short-, medium-, and long-term exposures	X	X	✓
Identify potential compromised accounts	X	X	✓
Support remediation of exposures (if required)	X	X	✓
Conduct threat hunting in live/production AD environment	X	X	✓
Transition isolated AD back into production (if needed)	X	X	✓
SLA for incident response	N/A	N/A	1-2 hours (with retainer)

Unmatched global identity forensics and incident recovery experience

To learn more about IFIR, visit
Semperis.com/solutions/identity-forensics-incident-response

90+ years' identity-related incident response experience

25+ former Microsoft Premier Field Engineer (PFEs) on staff

170+ combined years of Microsoft MVP experience

30+ years' data analysis for insider threat & risk monitoring

Microsoft Partner
Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-sell
Microsoft Intelligent Security Association (MISA)

Gartner Peer Insights. Customer First

Semperis
IT Resilience Orchestration
5.0
Source: Gartner Peer Insights

Leader SPRING 2024

Semperis
Directory Services Protector
4.7
Source: G2.com

Semperis Headquarters
5 Marine View Plaza
Suite 102
Hoboken, NJ 07030