5 Cybersecurity Steps to Operational Resilience

Organizations and analysts now acknowledge that identity is today's security perimeter. In every industry, a comprehensive identity-first security strategy is an essential part of operational resilience.

Ready to get started? Here are five steps that our experts recommend for forward-thinking security teams.

semperis

01.

Secure the identity infrastructure

TO DO:

Make hybrid AD security a core component of your operational resilience plan.

Simon Hodgkinson, former CISO at bp and Strategic Advisor at Semperis, says that operational resilience should be top of mind for both security and business leaders. Enabling such resilience involves much more than a generic disaster recovery plan.

"Operational resilience [includes] aspects like the sort of governance you've put in place; how you manage operational risk management; your business continuity plans; and cyber, information, and third-party supplier risk management.... Resilience must be built into everything."

A good place to start: Implement strong security for your identity infrastructure. For most organizations, that means securing Microsoft Active Directory (AD).

Explains Hodgkinson, "Active Directory is at the very core of your ability to operate and deliver business outcomes, and it needs to be part of your operational resilience strategy."

Whether you use AD or a combination of AD and Entra ID (formerly Azure AD) or another system, such as Okta ... if your identity systems aren't working, neither is your business.

02.

Build a comprehensive ITDR strategy

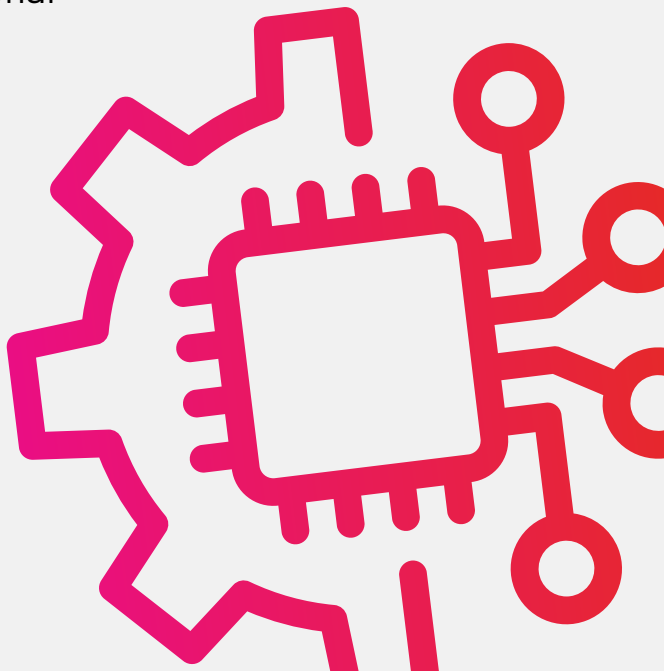
"Gartner drew a lot of attention late last year to identity threat detection and response (ITDR) solutions," says Semperis Principal Technologist Sean Deuby. "There are many ways to strengthen your defenses, but the most productive step that organizations can take this year is to prioritize identity-focused security."

Such a strategy should:

- **Specify** procedures, processes, and responsibilities for protecting your hybrid identity infrastructure across the AD attack lifecycle: before, during, and after an attack.
- **Include** a plan for AD-specific backup and recovery and regular monitoring to identify identity-related vulnerabilities.
- **Identify** interdependencies between your identity systems and operational technology (OT).

TO DO:

Build an ITDR strategy that covers all stages of the AD attack lifecycle.



03.

Audit your identity attack surface

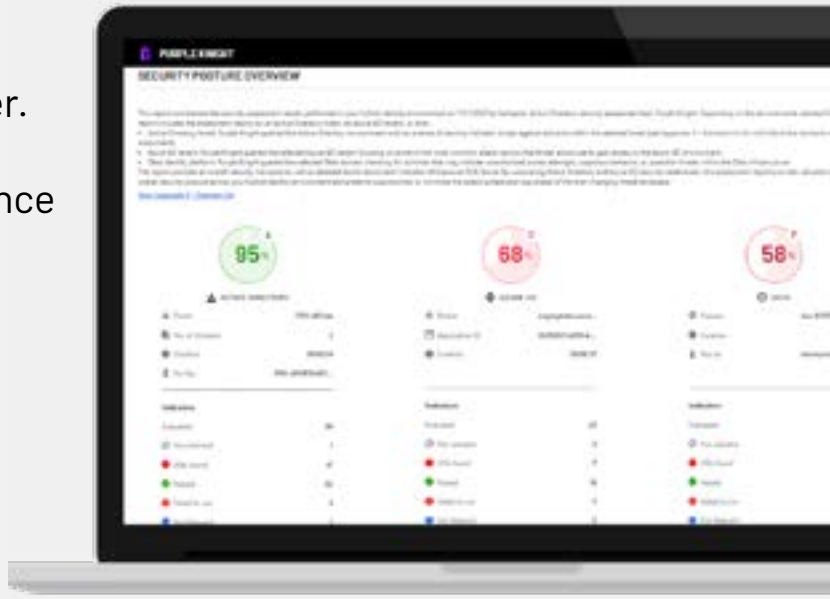
TO DO:

Download and run **Purple Knight** and **Forest Druid** for a snapshot of your AD attack surface.

"Most attacks involve identity and, regardless of their initial access point, threat actors typically go through AD to gain ground in your environment," explains Deuby. "So, a great place to start is evaluating and reducing your AD attack surface."

This necessary step needn't be difficult or expensive. Powerful tools like Purple Knight, which helps you spot gaps and vulnerabilities that often have existed for years, and Forest Druid, which helps you identify your most important identity assets and the access paths to them, are available for free.

No installation or special permissions are required, and the tools provide a clear snapshot of potential vulnerabilities—and indicators that attackers might already have breached your identity perimeter. You also get actionable guidance for closing existing gaps.



04.

Automate identity protection

TO DO:

Request a demo of **Semperis DSP** or **ADFR**.

"Automation and an API-first approach can help streamline processes, reduce the risk of human error and improve the efficiency of cybersecurity teams," Forbes[1] notes. "This includes the use of automation in tasks such as vulnerability management, incident response, and compliance checks."

Automation can reduce the workload on resources as well as reduce human error and speed incident response. And when it comes to protecting your Tier 0 identity assets, speed is of the essence.

During the infamous Maersk NotPetya attack, for example, ransomware spread across the network at record speed. "By the second you saw it, your data center was already gone," Craig William, Cisco's Talos division's Director of Outreach, told Wired.[2]

This is why expert ITDR solutions like Semperis Directory Services Protector (DSP) enable automated rollback of changes to AD. DSP automates remediation and enables customized triggers and alerts, so that organizations can respond to cyber threats as quickly as possible.

Automating AD recovery is another vital capability. Manual recovery can take days or even weeks, compared with as little as under an hour with Semperis Active Directory Forest Recovery (ADFR).

[1] Forbes: Novikov, Ivan. "The Top Five Priorities for Enterprise CISO in 2023." Forbes, January 11, 2023.
[2] Wired: Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired, August 22, 2018.

05.

Expect attacks

TO DO:

Develop and regularly test an AD-specific backup and recovery plan.

"I suspect that we're going to see continued growth in cybercrime," warns Deuby. "Ransomware attacks can have catastrophic consequences on businesses, resulting in millions of dollars of losses and C-level resignations.

"The FBI recommends that organizations maintain backup data files and maintain a recovery plan," Deuby points out. "Organizations need to know what their critical systems are (including infrastructure such as AD) before attacks occur and build in resiliency."

Don't just rely on a traditional backup, which includes AD along with the OS and can reintroduce malware through hidden back doors. Maintain both an AD-specific backup and detailed AD recovery plan—and test both regularly. After all, the last thing you need is to discover flaws in your backup or recovery plan during an active cyberattack.