Breach Preparedness & Response Services

Introduction

Semperis, the pioneer of identity-driven cyber resilience for enterprises, offers breach preparedness and response services, combining insights from battle-tested Active Directory (AD) security and incident response (IR) experts with industry-leading solutions for preventing, remediating, and recovering from AD attacks. These services allow you to tap into Semperis' expertise before, during, and after an attack, so you can benefit from our team's decades of combined experience responding to cyber incidents.

The breach preparedness and response services are highly comprehensive, spanning every stage of an attack. Semperis offers an identity security assessment to proactively address weak points and works hand in hand with your stakeholders to prepare for known and unknown cyber threats.

Semperis is not just another security vendor, but a true partner through and through. With the breach preparedness and response services offering, Semperis provides round-the-clock IR support to help you respond to, recover from, and investigate cyber incidents.

This document highlights the options available to engage the Semperis Breach Preparedness and Response Services team.

PREPAREDNESS

02 **Active Directory Security Assessment**

04 **Active Directory Threat Mitigation**

05 **Active Directory Disaster Recovery Planning and Exercise**

RESPONSE

06 **Cyber-First Active Directory Recovery**

06 **Active Directory Incident Investigation and Attack Forensics**

07 **Active Directory Threat Removal**

Preparedness

Active Directory Security Assessment (ADSA)

Active Directory is a complex system with numerous configurable settings and features, making it hard to secure. Design flaws, operational mistakes, and misconfigurations accumulate over the years to create a technical debt that is often difficult to address and exposes AD to a spectrum of attacks of varying sophistication. These vulnerabilities make AD the path of least resistance for an attacker to reach critical systems and sensitive data.

The Active Directory Security Assessment (ADSA) gives you a clear view of your organization's AD security posture and a report to address security exposures at the strategic, operational, and tactical levels.

The Semperis team conducts the ADSA through a combination of technical and non-technical engagements. We use questionnaires and interviews to elicit architectural and operational information from your team, and we use automated scans and manual tools to collect technical information from AD and auxiliary systems.

While the ADSA offers a comprehensive analysis of the environment and provides a report for thoroughly securing AD, conducting the assessment requires involvement from your team.

ADSA is available with or without purchase of Semperis products.

The assessment includes the following efforts:

Security Architecture Review

The Security Architecture Review is a high-level review of the environment and the considerations that led to the current design. The Semperis team conducts interviews with your key team members and a walkthrough of relevant artifacts, such as architectural diagrams, if available.

The primary aspects captured in this stage are:

- AD forest structure
- Trust relationships
- Security boundaries
- Tier 0 assets and security dependencies
- Disaster recovery infrastructure

Operational Procedures Review

The Operational Procedures Review is an evaluation of your current operational procedures. The Semperis team conducts this review through interviews with your key team members and a walkthrough of relevant artifacts, such as flow diagrams, scripts, etc.

The primary elements captured or produced in this stage are:

- Provisioning and de-provisioning process for Tier 0 assets
- Management and maintenance procedures for Tier 0 assets
- Privileged access management procedures
- Access procedures for Tier 0 security dependencies
- Discovery of additional Tier 0 assets
- Disaster recovery procedures and their dependencies

Security Configuration Review

In the Security Configuration Review, the Semperis team uses automated tools (such as Purple Knight) and manual methods to identify indicators of exposure (IOEs) and indicators of compromise (IOCs) in your AD environment.

The elements captured or produced in this stage are:

- Indicators identified by the Purple Knight scan
- Manual review of indicators not currently implemented in Purple Knight
- GPO review using open-source tools
- Automated identification of hidden accounts

Attack Path Analysis

The Attack Path Analysis aims to identify dangerous or unintended attack paths to Tier 0 assets and other critical assets. Attackers could abuse these paths to elevate privileges and could introduce these paths to install domain persistence and regain privileged access.

In this stage, the Semperis team collects and analyzes data using open-source and internal tools.

The elements captured or produced in this stage are:

- Attack paths from outside of Tier 0 into Tier 0
- Abnormal delegated rights
- Admin "hotbeds"
- Hosts and objects with high reachability, i.e., exposed to many users

Analysis and Reporting

In the Analysis and Reporting phase, the Semperis team digests the data and findings captured in the assessment into an actionable report that describes the current state, provides an achievable recommended state for the environment, and offers a report for achieving the recommended state.

In addition, the report includes a detailed list of findings, each with a concise description of the identified issue, the risk it imposes, a severity rating, and guidelines for remediation.

Report outline

- Executive Summary
- Scope and Methodology
- Summary of Findings
- Current State Description
- Recommended State Description
- Detailed Findings

Presentation

After submitting the report, the Semperis team will deliver an executive/technical presentation of the results and address any questions or concerns.

Remediation Planning (Optional)

Semperis offers optional remediation planning workshops with our AD security experts. In these interactive consulting sessions, Semperis experts work with your AD team to plan and implement remedial actions, explore alternatives, and identify other remediation tactics.

These workshops might take place after or during the assessment to promptly address "low-hanging fruit" and critical issues.

Active Directory Threat Mitigation

The Active Directory Threat Mitigation service helps Directory Services Protector (DSP) customers prevent and prepare for an attack. This service includes an annual Standard ADSA, quarterly attack surface reduction sessions, and tailored optimization for your DSP deployment.

You can purchase the Active Directory Threat Mitigation service with or without a Semperis professional services deployment bundle. We recommend that you acquire the DSP Intelligence module, as it helps optimize incident preparation and minimizes the impact of a potential incident. The DSP Intelligence module also significantly reduces the forensics and investigation time in case of an incident. If you don't have the DSP Intelligence module, you can't track security posture changes over time, set relevant notification and response rules, and conduct other threat mitigation activities.

This offering is available only with Semperis DSP, and the scope of services might vary based on the DSP modules acquired.

This service offering includes the following efforts:

Attack Surface Reduction

The Attack Surface Reduction service is a periodic effort that involves an annual Standard ADSA (described above), as well as quarterly sessions in which Semperis experts work with you to analyze IOCs, IOEs, and indicators of attack (IOAs) gathered by DSP, as well as data collected with other tools. The Semperis team will provide recommendations for reducing the attack surface and eliminating security exposures in the AD environment.

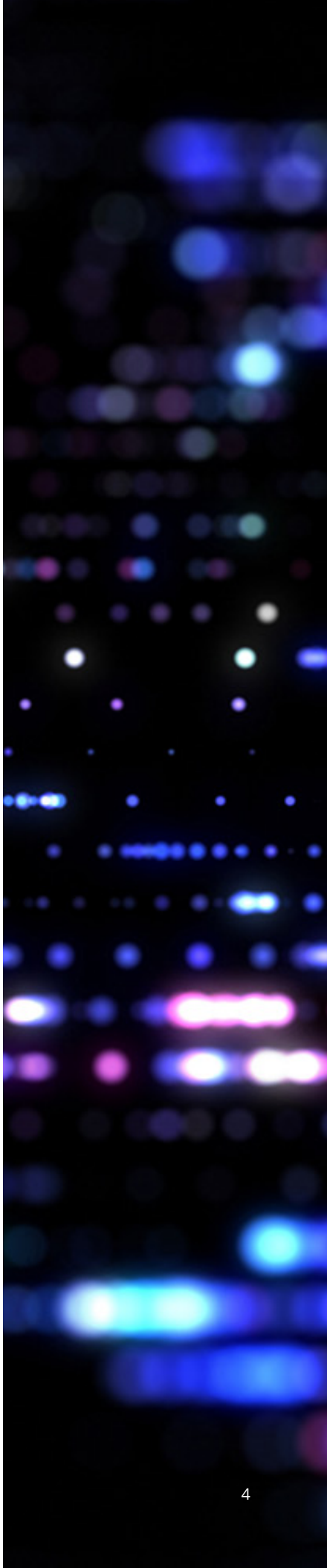
In addition, the Semperis team might perform an attack path analysis to identify dangerous or unintended attack paths to Tier 0 assets and other critical assets, as well as abnormal delegated rights.

If you don't have the DSP Intelligence module, the scope of this service offering is limited to indicators gathered by the Purple Knight security assessment tool.

Detection and Protection Optimization

Semperis experts work with you to ensure the DSP deployment is optimized to meet your AD protection requirements. The goal is to optimize your security posture outcome, ensuring the DSP platform is used to its full extent to provide protection tailored to your environment. This optimization review aligns with Semperis best practices, which include:

- Configuration review of your DSP deployment, notifications setup, database configuration, auto-response rules, integrations with third-party solutions (e.g., SIEMs), and environment-specific definitions (e.g., sensitive accounts, response policy)
- Analysis of the data gathered by DSP to identify indicators of suspicious activity and potential compromise
- Execution of a DSP test plan to understand all the product's capabilities (see DSP Test Plan for additional information)



Active Directory Disaster Recovery Planning and Exercise

The Semperis Active Directory Disaster Recovery Planning and Exercise service helps ADFR customers ensure the ADFR deployment is optimized, aligns their recovery time objective (RTO) and recovery point objective (RPO) parameters, and identifies implicit dependencies that might hinder the plan execution during an incident.

This offering is available with the Semperis Active Directory Forest Recovery (ADFR) solution, with or without the Semperis professional services deployment bundle.

This service offering includes:

Recovery Plan Review

Semperis experts review your existing AD disaster recovery plan to understand the business goals, SLA, disaster scenarios, and methods currently in place to recover AD in the event of a disaster.

Planning Workshop

Semperis experts work with you to ensure the ADFR deployment aligns with your AD recovery requirements. In the workshop, Semperis experts work with you to analyze your business goals in a disaster, such as recovery point/recovery time objectives, remote sites, number of users requiring initial access, and environment recovery priority in case of a multi-forest disaster. The workshop also aims to thoroughly map the dependencies for the recovery process.

The Semperis team will help you plan different cyber and operational disaster scenarios as part of the workshop, including reviewing offline storage/offsite backups, recovering backups online when required, and similar recovery activities.

The workshop deliverable is a documented set of best practices for your AD recovery plan that leverages ADFR and is ready to present to business owners for inclusion to your Disaster Recovery or Business Continuity team.

AD Disaster Recovery Exercise

We recommend conducting a full test of your AD disaster recovery plan at least annually or when a major change occurs. The Active Directory Disaster Recovery Exercise includes a table-top simulation to validate your staff have the necessary knowledge and skills to perform a recovery with ADFR. During the exercise, the Semperis experts will work hand-in-hand with your team to recover your production backups into an isolated lab environment.

At the end of the exercise, the Semperis team provides a report that describes the test results and documents issues. You can use this report to help meet governance and compliance requirements.

Response

Cyber-First Active Directory Recovery

If your AD environment is severely damaged, Semperis experts can leverage the Semperis ADFR solution to perform a partial or full forest recovery into new, isolated infrastructure, without carrying over executable code from the DCs' operating system. This approach eliminates the reintroduction of any host-based persistence or malware.

After AD is recovered into an isolated environment, the attackers can no longer tamper with it. The isolated AD replica also allows you to perform cleanup activities outside the reach and visibility of the attacker, maintaining the element of surprise for the moment when production is switched over to the clean environment.

Where applicable, the recovery process includes restoring AD functionality based on the procedures developed in the Active Directory Disaster Recovery Planning offering.

Under certain conditions, if AD is sufficiently functional, this offering might be available to you even if you don't have the ADFR solution.

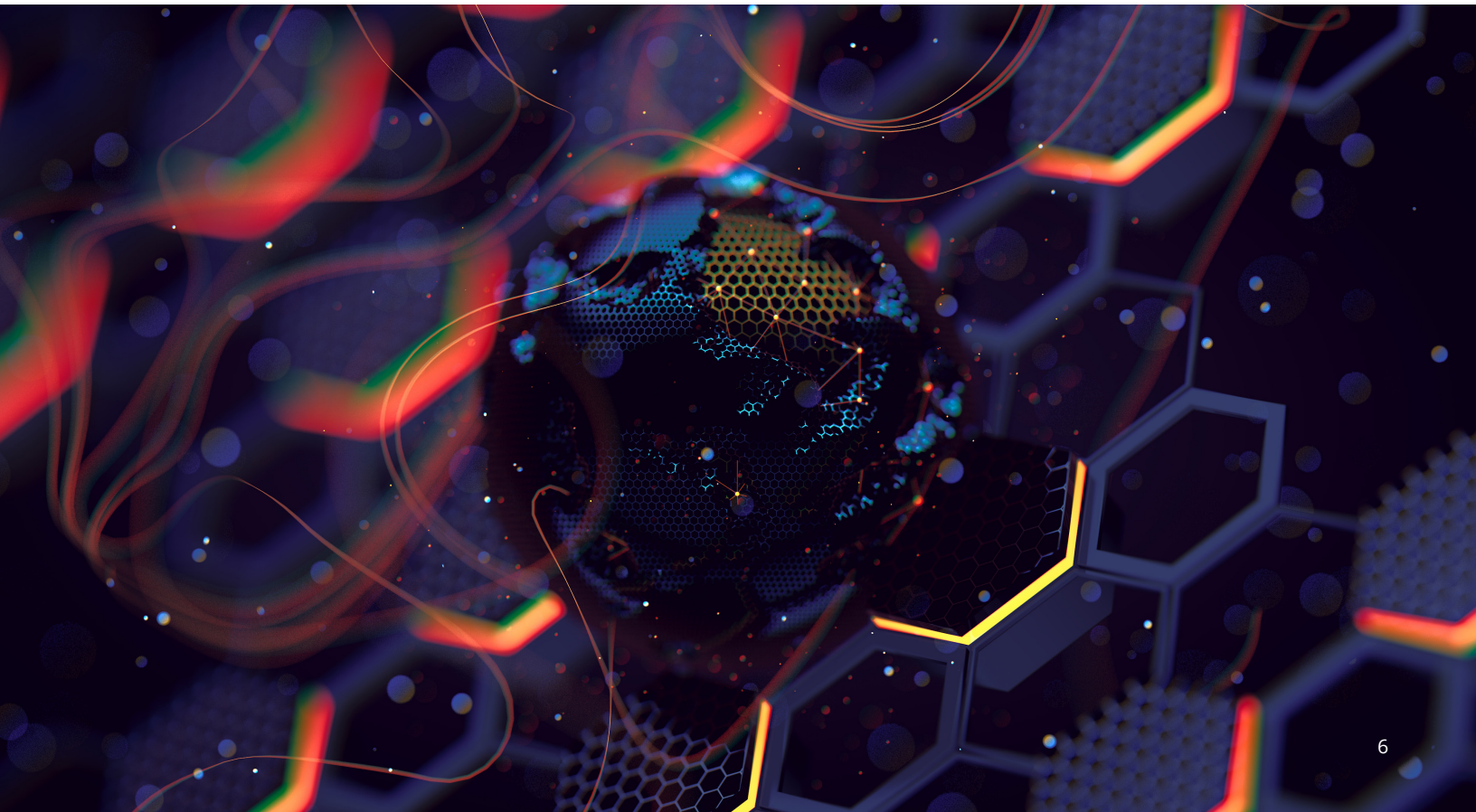
Active Directory Incident Investigation and Attack Forensics

Following a security incident that adversely impacts AD, the first crucial recovery step is investigating whether malicious intent and intelligence were behind the incident, constituting an attack.

Semperis experts can leverage the Semperis DSP platform and other tools to analyze the AD replication data and corresponding event logs. This information helps our experts determine whether an attack is underway, unroll the chain of events, and assess the impact on the environment. This analysis is the basis for effective containment of an attack and helps identify the best course of action for fully eradicating the threat from the AD environment.

This offering is available only to Semperis Directory Services Protector platform (DSP) customers, and service varies based on the DSP module.

If you don't have DSP, this offering might be available to you, but the outcome will depend on the availability of the required audit trail.



Active Directory Threat Removal

Following a forensic investigation of an AD attack, Semperis experts can recommend one or more courses of action to regain control of the AD environment and remove the threat, including:

- Eradicating threat actors and compromised/exposed objects (e.g., domain persistence) to prevent the attacker from regaining control
- Performing a security assessment to identify vulnerabilities and exposures post-containment
- Providing mitigation steps for attack surface reduction for the organizational AD

The Semperis team might conduct activities in this stage against the production environment or against an isolated replica of the environment to prevent the attacker from interfering with the effort and to maintain the element of surprise.

This offering is available only to Semperis Directory Services Protector customers. Service might vary based on the DSP modules acquired.

This offering might be available to you even if you don't have the DSP solution, but the outcome will depend on the availability of the required audit trail.

semperis

info@semperis.com
www.semperis.com

Semperis Headquarters
221 River Street
Hoboken, NJ 07030

ABOUT SEMPERIS

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures the integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid Active Directory environments, Semperis' patented technology protects over 100+ million identities from cyberattacks, data breaches, and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress, and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in Hoboken, New Jersey, and operates internationally, with its research and development team distributed throughout the United States, Canada, and Israel.

Semperis hosts the award-winning Hybrid Identity Protection conference and podcast series (www.hipconf.com) and built the community hybrid Active Directory cyber defender tools, Purple Knight (www.purple-knight.com) and Forest Druid. The company has received the highest level of industry accolades, recently named to Inc. Magazine's list of best workplaces for 2023 and ranked the fastest-growing cybersecurity company in America by the Financial Times. Semperis is a Microsoft Enterprise Cloud Alliance and Co-Sell partner and a member of the Microsoft Intelligent Security Association (MISA).

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