



XeneX SOCaaS

With over 12 years of experience and focus on Security Operations Center as a Service (SOCaaS), XeneX delivers a unique cybersecurity solution and unparalleled 7/24/365 SOC experience.

XeneX's software development team continues to extend the capabilities of XeneX platform. A leading industry platform, XeneX integrates several cybersecurity tools to achieve a single pane of glass of cybersecurity for the enterprise.

XeneX security analysts receive extensive training on the XeneX platform and must complete certification before joining the SOC team.



XENEX
SOC - AS - A - SERVICE

People, Process,
Technology.

Disaster Recovery & Business Continuity

Highlights

XeneX has a systematic approach to implementing effective disaster recovery (DR) and business continuity (BC) to ensure that your organization can respond to disruptions and maintain operations. Here are the XeneX's key steps to DR/BC.

- Minimized Downtime and Data Loss
- Enhanced Resilience
- Regulatory Compliance and Risk Management
- Improved Customer and Stakeholder Confidence
- Reduced Financial Impact
- Faster Recovery Time
- Competitive Advantage
- Employee Safety and Well-being
- Effective Communication
- Flexibility for Future Growth

1. Risk Assessment and Business Impact Analysis (BIA)
2. Develop DR and BC Plans
3. Establish a Cross-Functional Team
4. Data Backup and Storage
5. Redundancy and Failover Planning
6. Test and Training
7. Vendor and Supplier Assessment
8. Communication Plan
9. Implement Cybersecurity Measures
10. Establish Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
11. Regularly Review and Update Plans
12. Obtain Executive Support
13. Document Procedures and Contact Information
14. Plan for Different Scenarios
15. Continual Improvement

The screenshot displays the XeneX SOC-as-a-Service dashboard. The left sidebar contains navigation options: MANAGE ACCOUNTS, OVERVIEW, DEVICES, DISASTER RECOVERY (with sub-items: Servers, Runbooks, Connectivity, Credentials store), PLANS, BACKUPS, and SETTINGS. The main content area is titled 'Servers' and features a search bar and a table of server instances. Below the table, a 'Production failover' section shows a multi-step process. On the right, a modal window titled 'DC-Win2016 - recovery' provides details for a specific recovery server, including its status, state, last recovery point, CPU and RAM specifications, IP addresses, and internet access status. A message at the bottom of the modal indicates that a new recovery point has been added to the backup and provides instructions for restoring the original or replacement server.

Name	Server type	Status
Windows 2019	Primary	OK
Windows 2016	Primary	OK
DC-Win2016 - recovery	Recovery	OK
Centos 7 Minimal	Primary	OK
Centos 7	Primary	OK
APP-Win2012R2 - recovery	Recovery	OK

DC-Win2016 - recovery

Original machine: DC-Win2016

Recovery server

Status: OK

State: Ready for failback

Last recovery point: Jul 24, 2019, 4:26 PM

CPU and RAM: 1 vCPU, 4.00 GB RAM, 2 Points

IP address: 192.168.1.110

Test IP address: 192.168.1.234

Internet access: Enabled

The new recovery point was added to the backup. Go to Backups and use it to restore the original or replacement server, or use bootable media. After that, confirm failback to release cloud resources.

Cancel failback Confirm failback

Our Vision

Continuously invest in technology, people and process improvements to deliver the most comprehensive cybersecurity technology platform and world-class white glove service for incident management. To be the leading SOCaaS, protecting our partners and customers, and helping them achieve their cybersecurity goals.



Contact Us

12121 Wilshire Blvd.
Suite 1111
Los Angeles, CA 90025
877-550-2568
info@xenexSOC.com
www.xenexSOC.com

XENEX
SOC-as-a-Service
People, Process,
Technology.