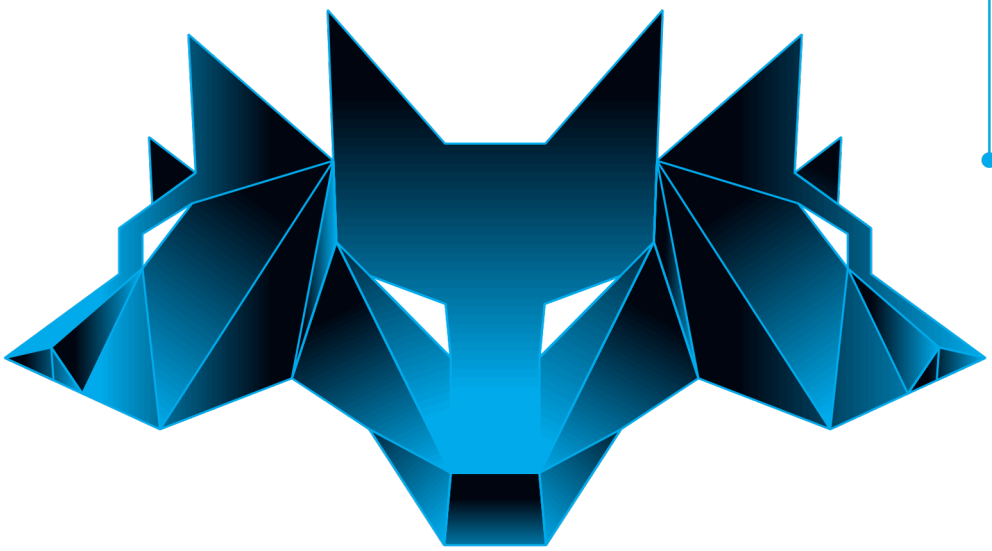
NCS EDR

SAFE DEPLOYMENT PRACTICES

1. INTRODUCTION AND PURPOSE

The update process for the NCS EDR product suite is a critical operation designed to ensure systems remain equipped with the latest security enhancements. We recognize that improper execution of updates may result in service disruptions, system conflicts, or the introduction of new vulnerabilities. This policy provides comprehensive guidance on **Safe Deployment Practices (SDP)**, enabling our customers to minimize risks and ensure a stable transition during every update cycle.



NCSEDR

2. DEVELOPMENT, PLANNING & RISK ANALYSIS

Before any deployment, we conduct a rigorous planning and evaluation phase to prevent unforeseen system impact:

- **Deployment Scope Definition:** We clearly define whether an update impacts the entire global infrastructure, specific customer segments, or only a subset of devices.
- **Impact Assessment:** Our engineers evaluate the update's effect on application compatibility and existing security policies to ensure no degradation of protection.
- **Risk Identification:** A core component of our planning is identifying critical risks such as loss of server connectivity, software conflicts, or the potential for system-level failures like the "Blue Screen of Death" (BSOD).
- **Strategic Scheduling:** Updates are scheduled during periods of minimal business impact, ensuring our 24/7 support teams are fully available to address any critical issues immediately.

3. MULTI-STAGE PILOT TESTING & COMPATIBILITY

Prior to a wide-scale production update, every new version must pass through a controlled staging environment:

- **Controlled LAB Environment:** New releases are first tested in an isolated LAB environment with a flexible timeframe depending on the complexity of the changes.
- **Limited Pilot Group:** Once stability is confirmed in the LAB, deployment proceeds to a restricted pilot group to verify behavior in real-world scenarios.
- **Functional Verification:** We verify that all new features operate as intended without causing unexpected system errors or stability regressions.
- **Resource Performance Check:** Testing focuses heavily on resource consumption, specifically monitoring Memory, CPU, and Disk usage to prevent performance bottlenecks.

4. PHASED RELEASE AND ROLLOUT STRATEGY

We perform updates in incremental phases to control impact and minimize the scale of any potential incident:

- **Granular Deployment:** Updates are deployed in small, managed phases, targeting specific groups within a customer environment or one customer at a time.
- **Gradual Expansion:** We begin with a small pilot group and only expand to additional device groups if no anomalies are detected during the initial hours.
- **Immediate Halt Protocol:** If any problem arises during any phase, the deployment is halted immediately to resolve the issue before further rollout occurs.
- **User Feedback Integration:** We actively collect and analyze user feedback at each phase to make timely adjustments to the deployment plan.

5. CONTINUOUS SYSTEM HEALTH MONITORING

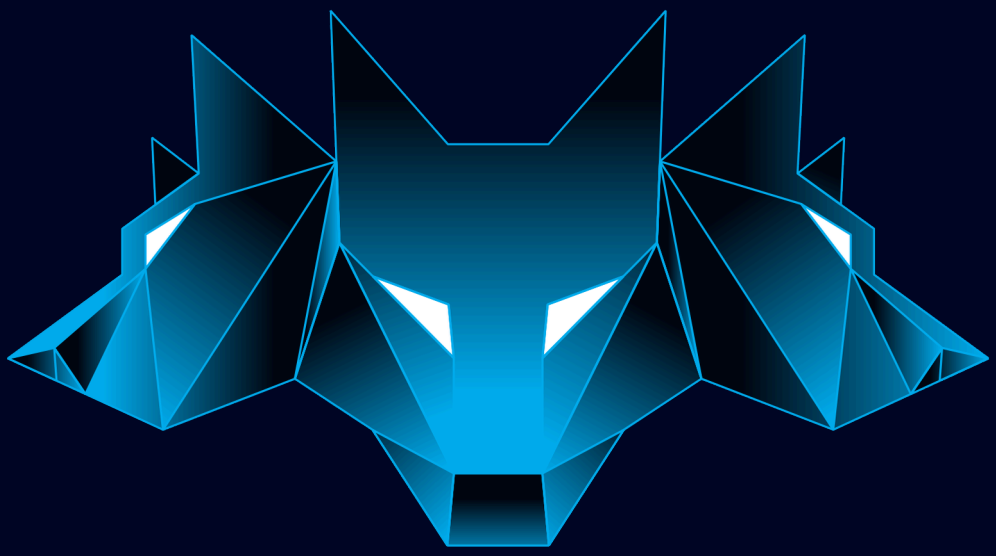
Post-deployment, we maintain intensive monitoring to ensure the update's effectiveness in the customer environment:

- **Security Feature Verification:** We ensure all core security features—including threat detection, suspicious file isolation, behavior monitoring, and log collection—are functioning correctly.
- **Performance Metric Tracking:** Our systems track real-time metrics such as CPU/RAM utilization, system response times, and error log generation.
- **Stability Monitoring:** Constant oversight of system performance is maintained to respond promptly to any post-update incidents.

6. RECOVERY AND ROLLBACK PROCEDURES

In alignment with safety standards, we prepare a comprehensive rollback plan for every release:

- **Version Retention:** The previous stable version of our software is always retained to enable a rapid and safe rollback if a critical failure occurs.
- **Technical Guidance:** Our IT and support teams provide detailed, step-by-step instructions to ensure recovery can be performed quickly and safely by the customer.
- **24/7 Global Support:** We maintain constant system monitoring and support availability to assist customers during the recovery process.



NCSEDR

VIETNAM NATIONAL CYBER SECURITY TECHNOLOGY CORPORATION

Tel: 024 85 888 000 **Email:** info@ncsgroup.vn **Website:** http://ncsgroup.vn

Headquarters: Trang An Complex, No. 1 Phung Chi Kien, Nghia Do, Cau Giay, Hanoi

Ho Chi Minh City Office: 131 Tran Huy Lieu, Ward 8, Phu Nhuan District, Ho Chi Minh City