CyRadarEDR Safe Deployment Practices

The update process for the CyRadar Endpoint Security product is a critical operation to ensure that the system remains equipped with the latest security enhancements. Improper execution of the update may result in service disruptions, system conflicts, or the introduction of new security vulnerabilities.

This document provides guidance on **Safe Deployment Practices** during the update of CyRadar Endpoint Security, enabling customers to minimize risks and ensure a proper transition. The focus is placed on the following key principles:

- **Development, Planning & Risk Analysis**: develop a comprehensive plan and conduct risk evaluation before deployment.
- **Pilot Testing & Compatibility Check**: conduct update testing in a controlled staging environment to verify stability before production deployment
- **Release**: perform phased updates to control impact and minimize incidents..
- **System Heath Monitoring**: monitor system performance after the update and respond promptly to incidents.
- **Recovery**: prepare a rollback plan in case reverting to a previous version is required.

1. **Development, Planning & Risk Analysis**

- Define the deployment scope: whether to update the entire system, all customers, or only a subset
- Assess the impact of the update on application compatibility and security policies
- Identify potential risks such as loss of connectivity to servers, conflicts with other software, or triggering a “Blue Screen of Death” (BSOD).
- Schedule the update during periods of minimal business impact, ensuring that support teams are available to promptly address critical issues

2. **Pilot Testing & Compatibility Check**

- Prior to a wide-scale update, the new version will be tested in a LAB environment with a flexible timeframe depending on the differences between the new release and the previous one. Once stable results are confirmed in the LAB environment, the deployment will proceed on a limited pilot group

- Verify the functionality of the new features, ensuring they operate as intended without causing system errors
- Evaluate the performance of the update in the testing environments, focusing on resource consumption such as Memory, CPU, and Disk usage

3. **Release**

- The update will be deployed in small phases, targeting one or a few groups within a customer, or one customer at a time
- Begin with a pilot group, then gradually expand to additional device groups if no issues are detected
- If any problem arises, the deployment can be halted immediately to resolve the issue before further rollout
- Collect user feedback at each phase to make timely adjustments

4. **System Heath Monitoring**

- Monitor the effectiveness of the new update after deployment at the customer environment
- Verify that the security features of CyRadar Endpoint Security are functioning correctly, including threat detection, suspicious file isolation, suspicious behavior monitoring, and system log collection.
- Track system performance metrics after the update, such as CPU and RAM utilization, system response time, and error logs.

5. **Recovery**

- The previous version is always retained to enable timely **rollback** if necessary
- The IT team provides detailed instructions to ensure rollback can be performed quickly and safely.
- 24/7 system monitoring and support are maintained.