CYRISMA

RISK MITIGATION

CREATE AND TRACK MITIGATION PLANS

Risk Mitigation involves taking the appropriate measures to fix security weaknesses and vulnerabilities in enterprise systems, following the vulnerability assessment process.

We understand that establishing accountability is critical to the success of any risk mitigation plan, so we've made it easy for CYRISMA users to create mitigation plans, set due dates and assign specific mitigation tasks to team members based on scan results. Mitigation tasks can be assigned to either IT and InfoSec team members or to actual end users in departments such as HR, finance, etc. Each assigned mitigation task is given a start and finish date to hold people and organizations accountable.

In order to meet regulatory compliance, organizations need to show proof that they are regularly assessing their risks and mitigating identified vulnerabilities. Internal and external assessors and auditors need to examine this proof from time to time to evaluate organizations' security posture. CYRISMA has the built-in ability to generate the details of mitigation tasks, the rationale behind these tasks, and the actions taken to reduce risk in near real time. All of this information can be exported as evidence or proof of compliance and due diligence.

The goal, as with other risk management processes, is to reduce cyber risk and with mitigation plans in place, bring the organization's attention to the risks identified and the steps being taken to handle those risks.

The Power of CYRISMA

1 **DISCOVER** what the mitigation methods to fix the security weaknesses and vulnerabilities in your systems, devices and network assets. Generate detailed mitigation plans based on scan results and risk assessments.

2 **UNDERSTAND** the rationale behind suggested mitigation actions and choose from various possible remedial actions based on detailed information about affected targets, and the root cause of specific vulnerabilities.

3 **MITIGATE** specific vulnerabilities in systems, protect sensitive data, and make configuration changes to ensure you are following OS security best practices based on CI Security's benchmarks.

4 **MANAGE** risk mitigation by creating detailed mitigation plans, assigning tasks to team members, monitoring plan progress, generating alerts when plans are overdue, and creating sub-plans within teams or departments.

sales@cyrisma.com
(585) 460 - 1352
CYRISMA
www.cyrisma.com
AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations