2023 Cyber Threat Report Analysis:

1) 75% of system vulnerabilities were exploited within about three weeks of being publicly disclosed. For organizations, they should quickly analyze their systems and prioritize the vulnerabilities they find and direct them to close them or take measures to mitigate the consequences of the attack.

2) The high-risk vulnerabilities found are concentrated on operating systems, network infrastructures and web applications. Organizations should intensify security measures especially in these three areas and eliminate their deficiencies.

3) In 2023, the most important MITRE ATT&CK tactics and methods for exploiting the vulnerabilities identified are as follows:

Exploitation of Remote Services (T1210 & T0866): This technique for first access and lateral movement emphasizes the importance of securing remote service protocols against unauthorized access and exploitation.

Exploitation of Public-Facing Applications (T1190 & T0819): This is a preferred first access path for attackers and demonstrates the critical need for robust outward-facing application security.

Exploitation for Privilege Escalation (T1068): The emergence of this technique underlines the need for effective privilege management and monitoring in corporate networks.