1. According to the ENISA Threat Landscape report for 2023, what emerges as the primary threat within cyberspace? Why is this particular threat deemed particularly alarming? Furthermore, based on the insights provided in the document, what strategies are recommended to effectively mitigate this threat?

ANSWER:

1. **Primary Threat:**
   * The ENISA report identifies the top threats within cyberspace, and in 2023, **supply chain attacks** emerge as the primary threat.
   * **Why Alarming?** Supply chain attacks target the interconnected web of suppliers, vendors, and partners that provide critical components or services. When attackers compromise a trusted supplier, they gain access to multiple downstream organizations. This ripple effect amplifies the impact and makes supply chain attacks particularly alarming.
   * Imagine a seemingly harmless software update containing a hidden backdoor—once installed, it infiltrates countless systems. That’s the power of supply chain attacks.
2. **Mitigation Strategies:**
   * To effectively mitigate supply chain threats, consider these strategies:
     + **Vendor Risk Assessment:** Scrutinize suppliers’ security practices. Assess their risk posture and evaluate their security controls.
     + **Secure Development Practices:** Encourage suppliers to follow secure coding practices. Regularly audit their software development processes.
     + **Software Bill of Materials (SBOM):** Demand transparency. Ask for an SBOM—a detailed inventory of software components used by your suppliers.
     + **Zero Trust Architecture:** Assume nothing. Implement zero trust principles—verify every interaction, even with trusted partners.
     + **Incident Response Plans:** Prepare for the worst. Collaborate with suppliers on incident response plans.
     + **Continuous Monitoring:** Vigilance pays off. Continuously monitor your supply chain for anomalies.

2. Visit the website www.csk.gov.in and outline some of the recommended best practices for securing personal computers.

ANSWER:

The CSK, operated by the Indian Computer Emergency Response Team (CERT-In), provides essential guidance to enhance our digital safety. Here are the recommended practices:

1. **Use Licensed and Genuine Software:**
   * Opt for legitimate software. Avoid pirated or cracked versions—they often harbor vulnerabilities.
2. **Keep Your System Updated:**
   * Regularly apply security patches and updates. These fix known vulnerabilities and strengthen your defenses.
3. **Install and Maintain Antimalware Solutions:**
   * A robust antivirus or antimalware program is your digital shield. Keep it updated and perform regular scans.
4. **Disable Autoplay/Autorun for Removable Drives:**
   * Autoplay can execute malicious code from USB drives automatically. Disable it to prevent unintended infections.