Framework di sicurezza e compliance

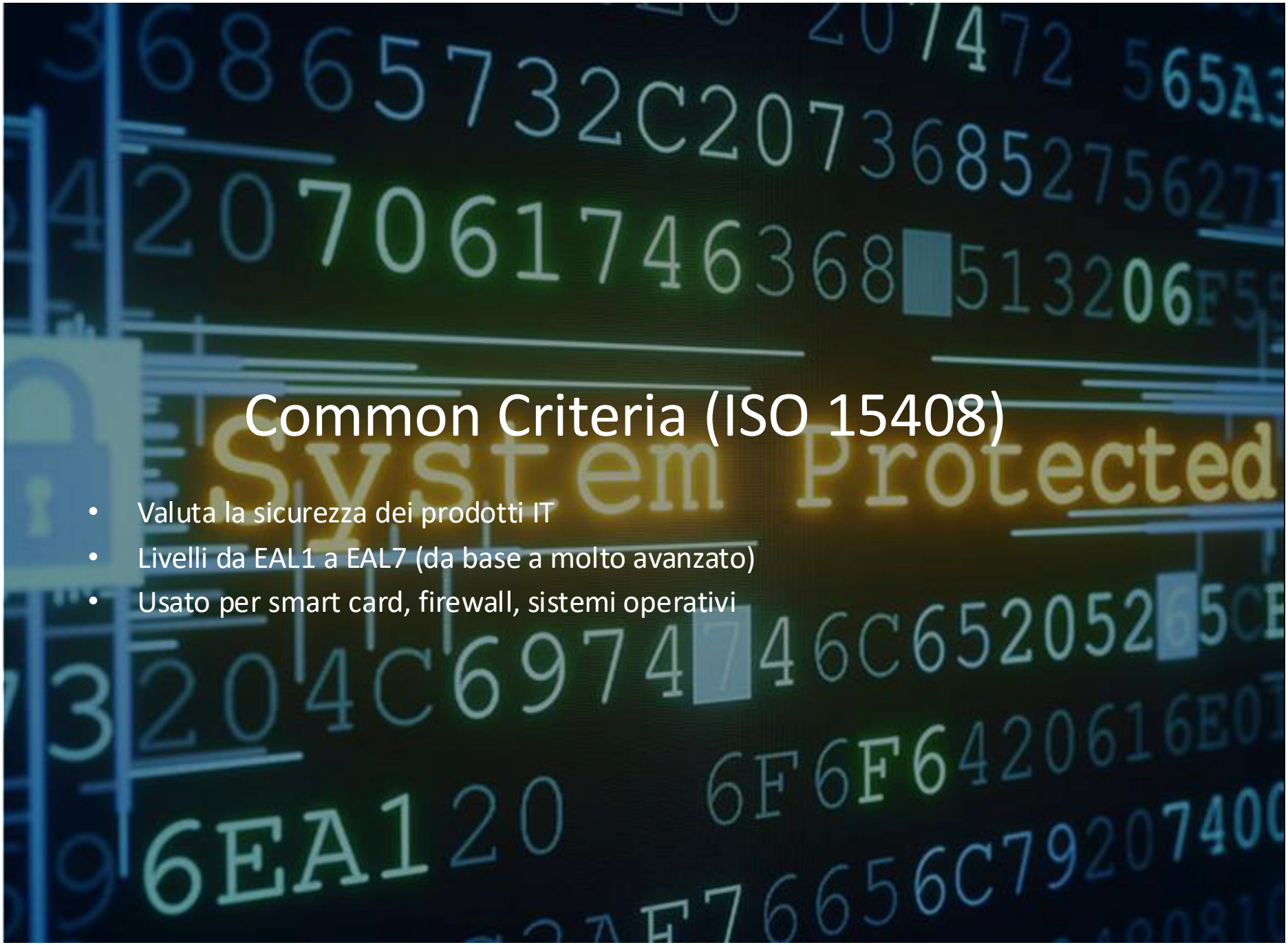
- Obiettivo: capire come proteggere reti e dati con regole e tecnologie
- Focus su: ISO 27001, NIST, audit e aspetti etici

ISO/IEC 27001

- Standard per la gestione della sicurezza delle informazioni (ISMS)
- Approccio basato sul rischio, con ciclo PDCA (Plan-Do-Check-Act)
- Include requisiti, controlli e miglioramento continuo

NIST Cybersecurity Framework

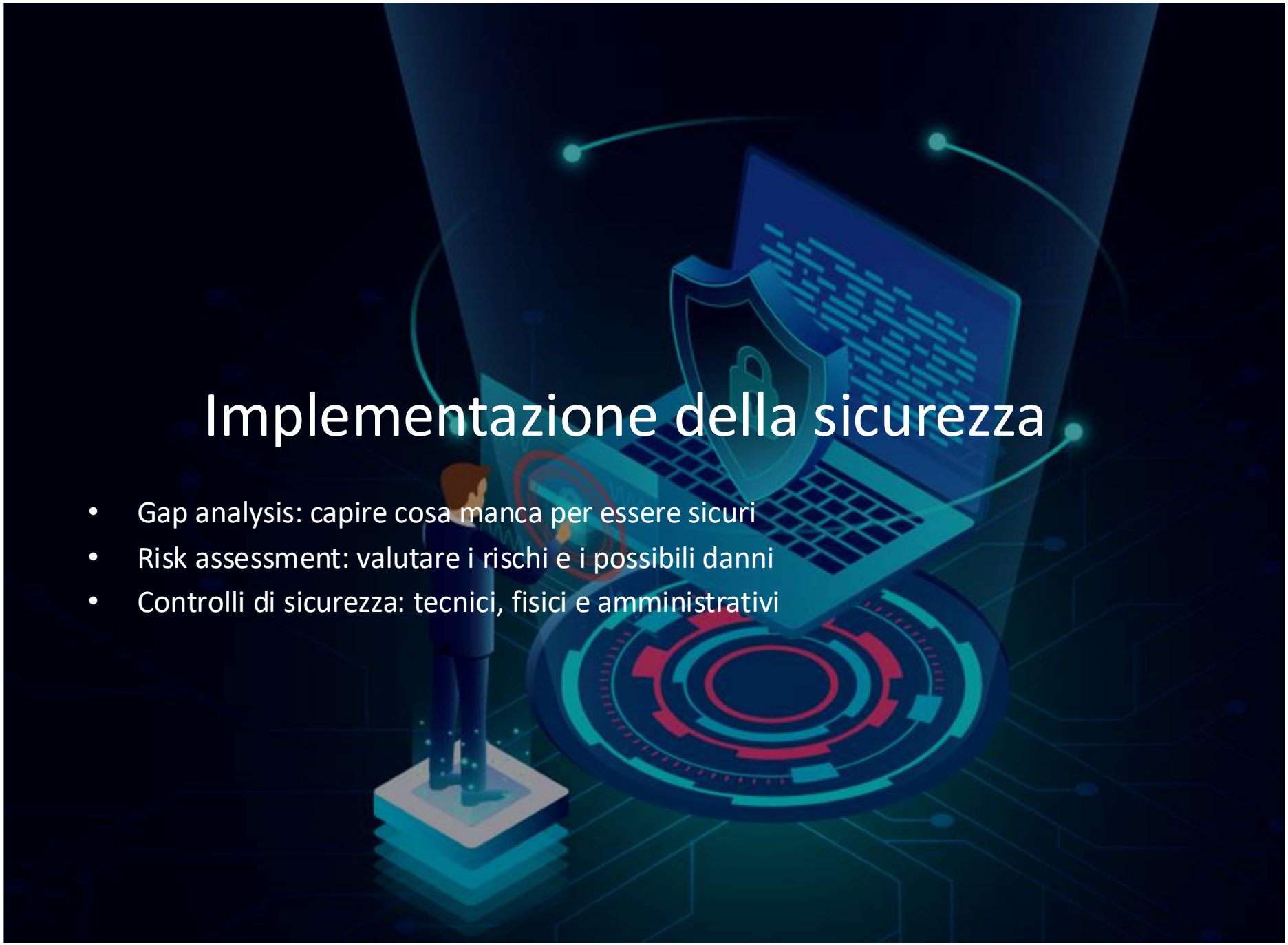
- Creato negli USA, volontario ma molto usato
- 5 funzioni base: Identify, Protect, Detect, Respond, Recover
- Aiuta a gestire i rischi informatici nelle aziende



Common Criteria (ISO 15408)

- Valuta la sicurezza dei prodotti IT
- Livelli da EAL1 a EAL7 (da base a molto avanzato)
- Usato per smart card, firewall, sistemi operativi

Implementazione della sicurezza



- Gap analysis: capire cosa manca per essere sicuri
- Risk assessment: valutare i rischi e i possibili danni
- Controlli di sicurezza: tecnici, fisici e amministrativi

Audit e certificazioni

- Audit interno o esterno per verificare la sicurezza
- Serve per ottenere certificazioni come ISO 27001
- Include test, interviste e controllo documenti

Aspetti etici

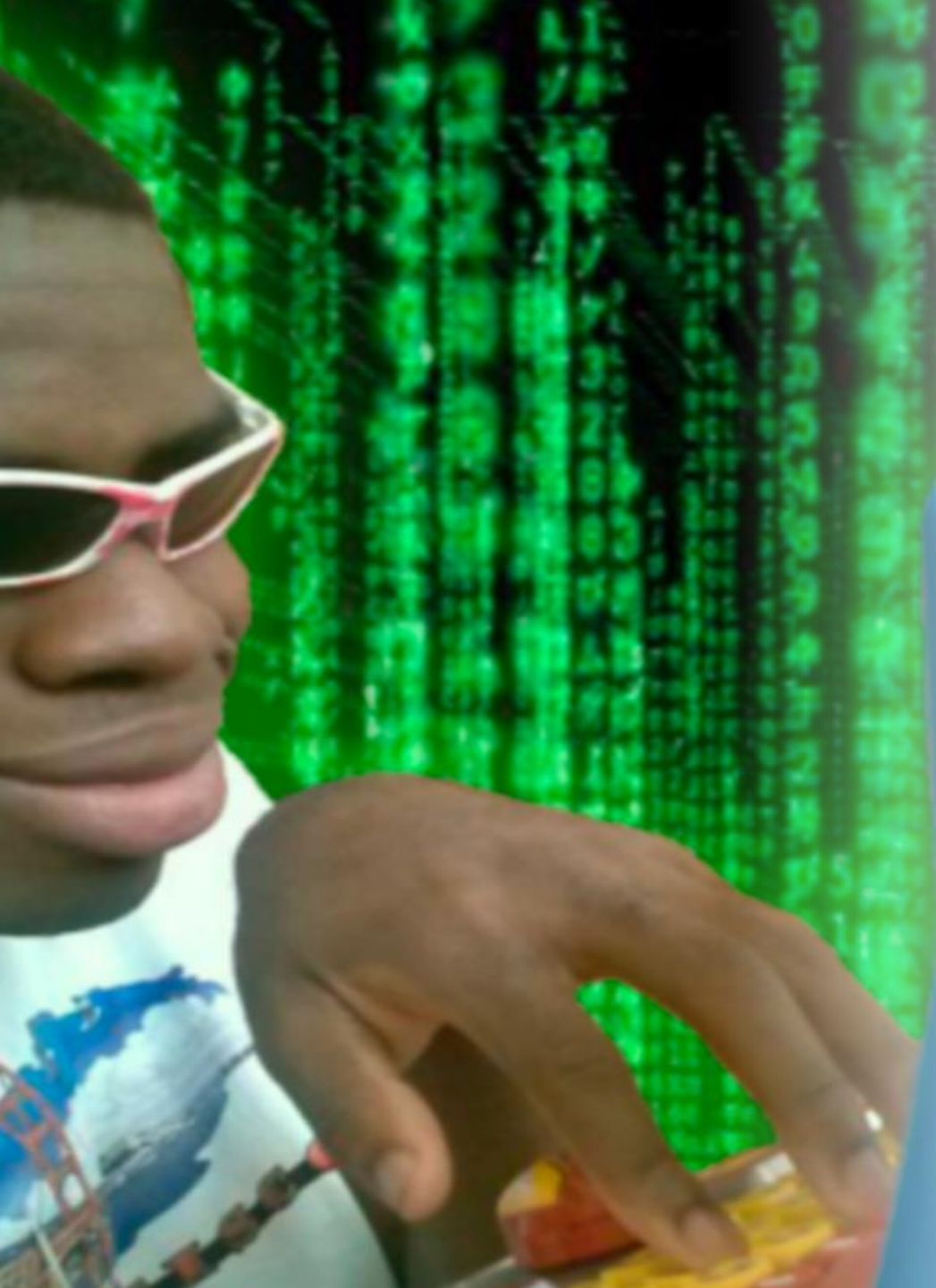
- La sicurezza deve rispettare anche privacy e diritti
- Esiste un equilibrio tra protezione e libertà dell'utente
- Responsabilità delle aziende e dei professionisti IT

Sfide e opportunità future

- Aumento delle minacce (es. attacchi mirati)
- Servono soluzioni più automatizzate e intelligenti
- Importanza della formazione continua

Raccomandazioni e best practices

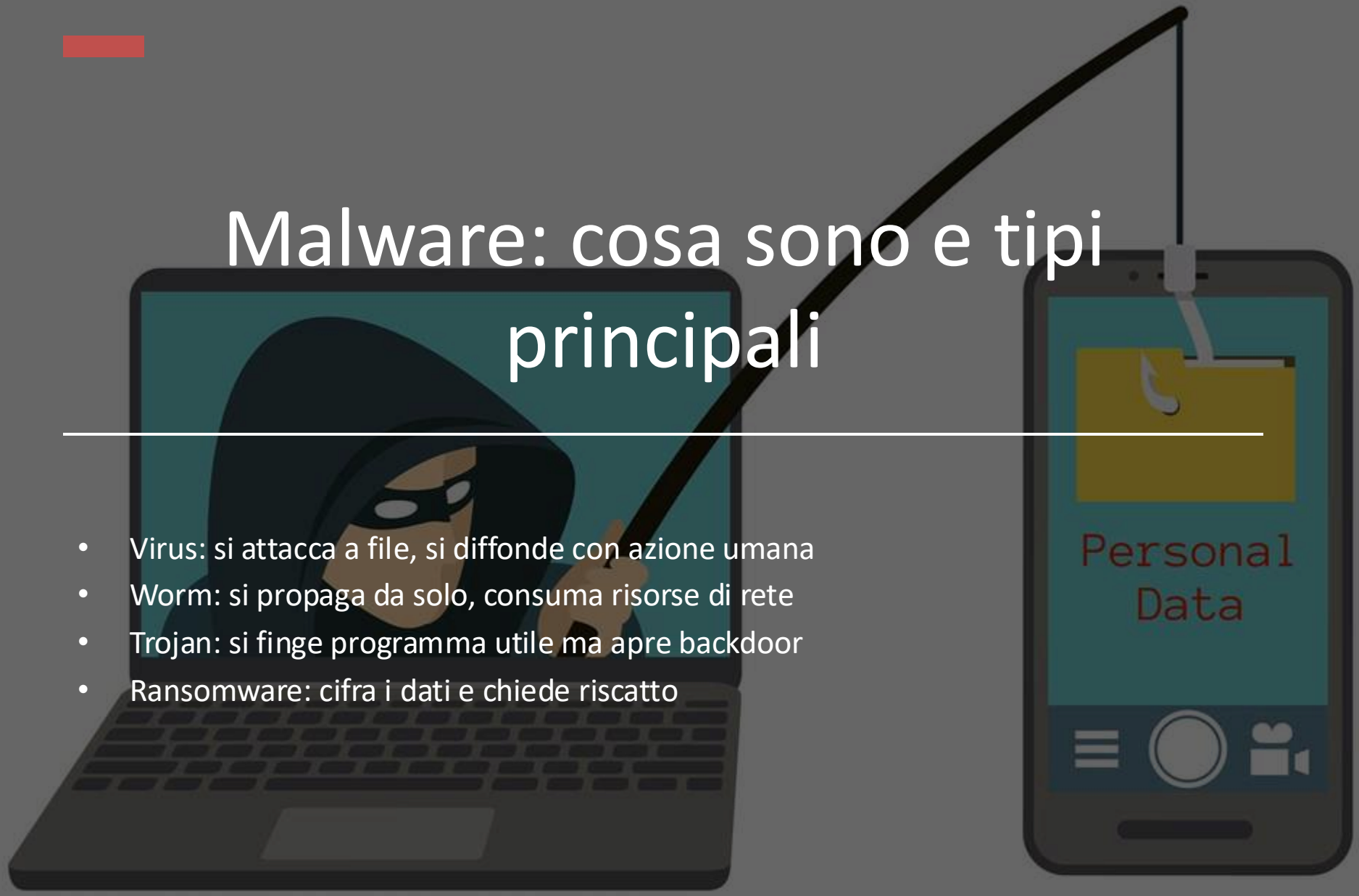
- Adottare standard riconosciuti (ISO, NIST)
- Fare backup, aggiornare software, formare il personale
- Monitorare continuamente reti e sistemi



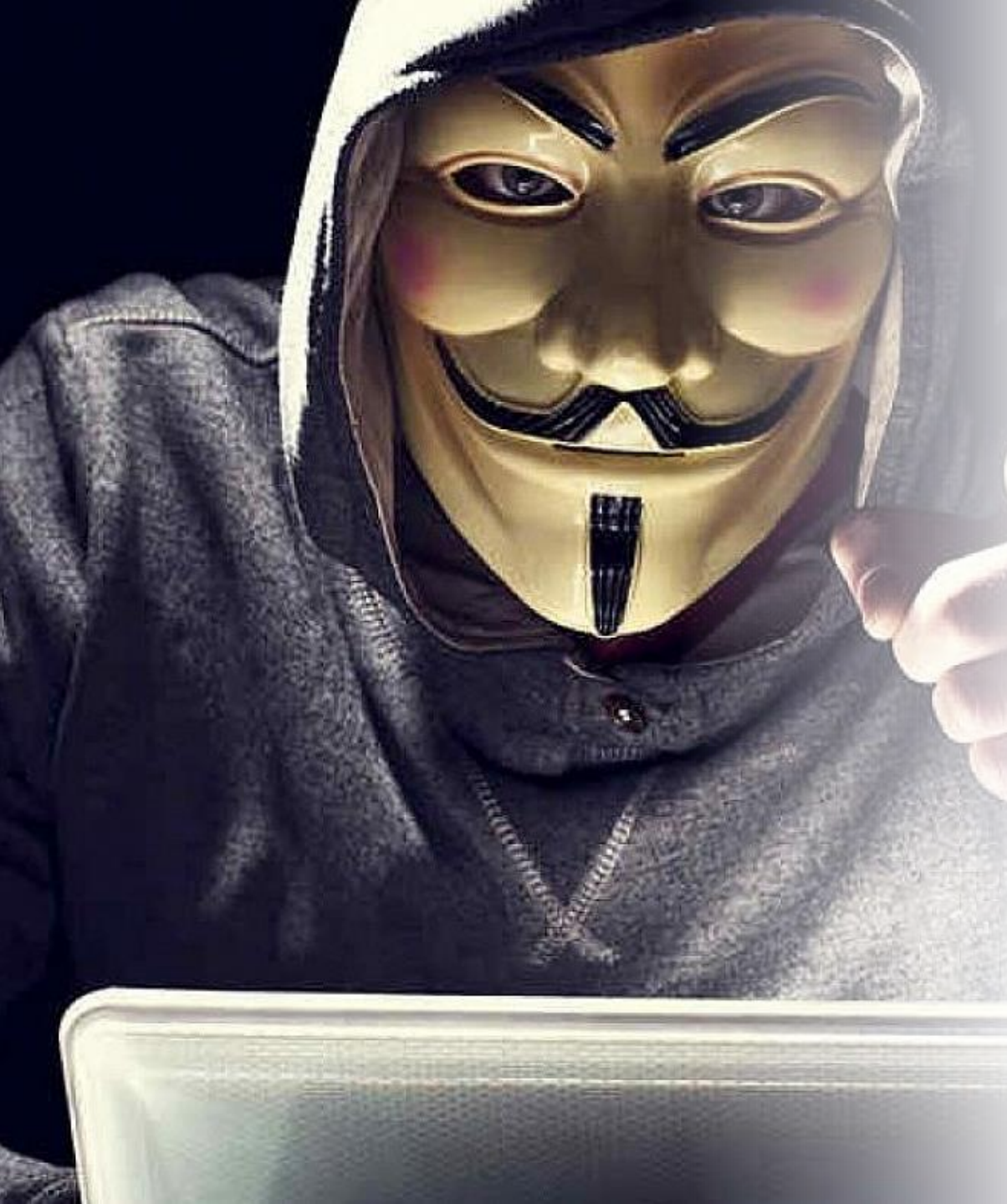
MALWARE

- I malware (abbreviazione di “malicious software”, ovvero software dannoso) sono programmi progettati per compromettere, danneggiare o ottenere accesso non autorizzato a sistemi informatici, dispositivi o reti. Possono causare una vasta gamma di problemi, dalla perdita di dati alla compromissione della sicurezza personale e aziendale.

Malware: cosa sono e tipi principali



- Virus: si attacca a file, si diffonde con azione umana
- Worm: si propaga da solo, consuma risorse di rete
- Trojan: si finge programma utile ma apre backdoor
- Ransomware: cifra i dati e chiede riscatto



Esempi Di Malware

- Backdoor: fornisce accesso remotoVettori di infezione
- Downloader: scarica altro malware
- Banker: ruba credenziali bancarie
- RAT (Remote Access Trojan): controllo completo
- Spyware: raccoglie informazioni
- Keylogger: registra ciò che viene digitato
- FakeAV: finto antivirus


FINE