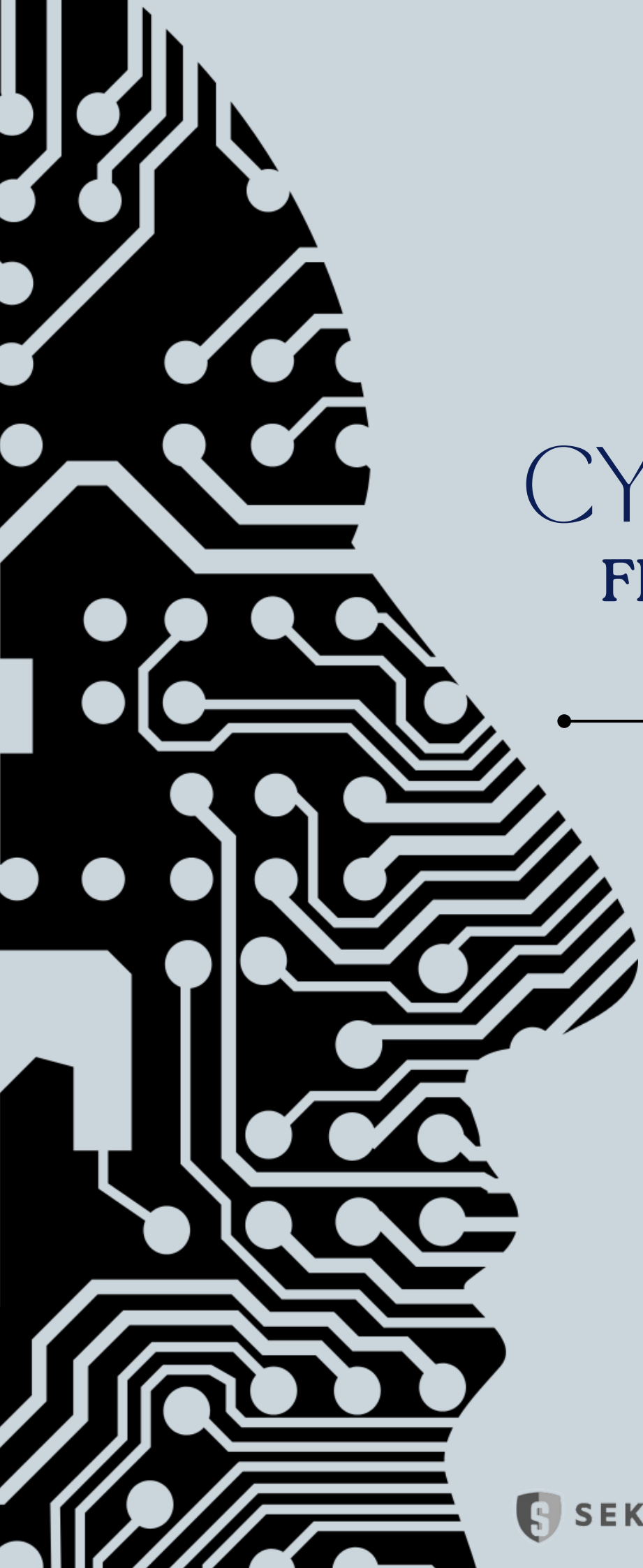

CYBERSEC
FRAMEWORKS

SEKURENET

WHAT IS A CYBERSECURITY FRAMEWORK?

A CYBERSECURITY FRAMEWORK IS A STRUCTURED SET OF GUIDELINES, STANDARDS, AND BEST PRACTICES THAT ORGANIZATIONS CAN USE TO MANAGE AND MITIGATE CYBERSECURITY RISKS.

WHY ARE CYBERSECURITY FRAMEWORKS IMPORTANT?

1. **RISK MANAGEMENT:** FRAMEWORKS HELP ORGANIZATIONS IDENTIFY, ASSESS, AND PRIORITIZE CYBERSECURITY RISKS.

2. **COMPLIANCE:** MANY INDUSTRIES HAVE SPECIFIC REGULATIONS AND STANDARDS THAT REQUIRE ORGANIZATIONS TO IMPLEMENT CYBERSECURITY MEASURES. FRAMEWORKS CAN HELP MEET THESE REQUIREMENTS.

3. **BEST PRACTICES:** FRAMEWORKS OFFER PROVEN STRATEGIES AND TECHNIQUES FOR IMPROVING CYBERSECURITY POSTURE.

4. **COMMUNICATION:** FRAMEWORKS PROVIDE A COMMON LANGUAGE FOR STAKEHOLDERS, MAKING IT EASIER TO DISCUSS AND ADDRESS CYBERSECURITY ISSUES.

POPULAR CYBERSECURITY FRAMEWORKS

NIST CYBERSECURITY FRAMEWORK (CSF): DEVELOPED BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), THE CSF PROVIDES A VOLUNTARY, FLEXIBLE FRAMEWORK FOR IMPROVING CYBERSECURITY.

ISO 27001: AN INTERNATIONAL STANDARD THAT PROVIDES A SYSTEMATIC APPROACH TO MANAGING INFORMATION SECURITY RISKS.

CIS CONTROLS: A SET OF PRIORITIZED SECURITY CONTROLS DEVELOPED BY THE CENTER FOR INTERNET SECURITY (CIS) TO PROTECT IT SYSTEMS AND DATA.

COBIT 5: A FRAMEWORK FOR GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT THAT INCLUDES A CYBERSECURITY COMPONENT.

HITRUST CSF: A FRAMEWORK SPECIFICALLY DESIGNED FOR THE HEALTHCARE INDUSTRY TO PROTECT PATIENT HEALTH INFORMATION.

PCI DSS: A SET OF SECURITY STANDARDS DESIGNED TO PROTECT CARDHOLDER DATA.