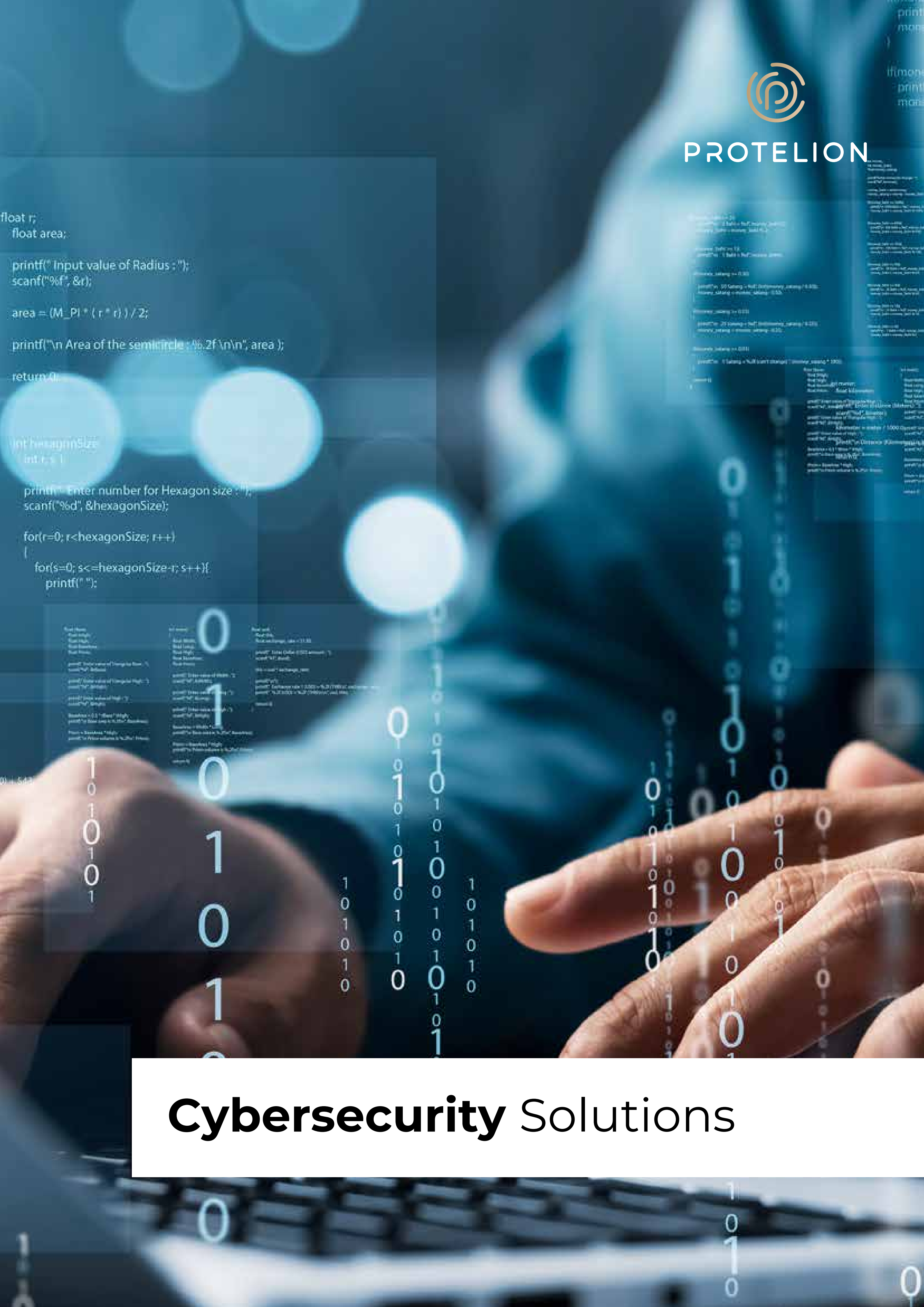


```
float r;
  float area;

  printf(" Input value of Radius : ");
  scanf("%f", &r);

  area = (M_PI * ( r * r) ) / 2;

  printf("\n Area of the semicircle : %.2f \n\n", area );

  return 0;

 int hexagonSize
   int r, s ;

   printf(" Enter number for Hexagon size : ");
   scanf("%d", &hexagonSize);

   for(r=0; r<hexagonSize; r++)
   {
     for(s=0; s<=hexagonSize-r; s++){
       printf(" ");
```

PROTELION

Cybersecurity Solutions

What is Cybersecurity?

Cybersecurity is the capability to defend and protect digital assets, including networks, communication, systems, computers and data, from cyberattacks.

Modern cybersecurity strategies make use and combine advanced technologies and human resources to prevent, detect and eliminate a variety of digital threats and adversaries.

What are the Threats?

Today organizations, no matter if they are governmental, military, civil or private, have to deal with an uncountable number of any kind of attacks like:

- Social Engineering, of which the main part are Phishing E-Mails
- Ransomware, which is a data-encrypting program that demands payment to release the infected data
- Denial of Service Attacks (DoS/DDoS)
- Malware (Virus, Trojans, Spyware, Botnets, Adware etc.)
- Third party software, web and cloud computing vulnerabilities
- Remote access, as well as internal security breaches

What do you have to protect?

As a general rule of thumb, there are the following elements, which have to be protected to maintain cybersecurity in an organization:

Endpoint Protection
Endpoints are the most vulnerable components of any IT-infrastructure. Almost every endpoint contains sensitive data. An endpoint security solution must protect:

Data – from any modification, stealing or encrypting attempt

Software – from unsafe or unauthorized access due to malicious code

Network Connection – by "controlling" inbound and outbound traffic.
Any modern Endpoint Security Solution includes modules, like anti-malware or antivirus, application control, "firewall", host intrusion prevention system and more

Network and Channel Protection
Network and Channel Protection as a security element provides secure data transfer and communication by protected backbone channels between all connected sites and locations.

Perimeter and Application Firewall Protection
A Perimeter and Application Firewall is the first line of defense in your network. It defends the boundary between your private and a public network. The Perimeter Firewall filters both, internal and external traffic. It implements appropriate control policies, technology to prevent accidental or intentional data leakage and network intrusion prevention capabilities to provide real-time protection against a wide array of threats.

Threat Detection and Response Protection
The TDR as a security element focuses on perimeter security and assets within the network and correlates network and endpoint events. It decreases significantly detection time of events and provides guidelines for responses and forensic information to investigate threats.

Infrastructure and Cloud Protection
It protects websites and web based applications from different kinds of cyber threats which exploit vulnerabilities in a source/programming code.

Information Protection
It is the security process and/or policy to prevent unauthorized access, use, disclosure, disruption, modification or destruction of information.

This is commonly known as the CIA (Confidentiality, Integrity and Availability) principle to protect your Information.

Operational Protection
OPSEC is a risk management process that identifies the critical information and develops a protection mechanism to ensure the security of your sensitive data.

End User Protection
There are many reasons, how such threats can be created, mainly through the use of Social Media, Text Messaging, App Downloads, E-Mails and bad Password creation or usage. It is therefore of high importance to educate the staff by periodically occurring Security Awareness Training Programs.

How to protect?

As a guide line how to implement a comprehensive cybersecurity solution one can follow a simple 5-point strategy:

Choose a Framework
There are different frameworks which are principally similar with some more focused on different industries. One of the most common is the NIST Framework
(NIST – National Institute of Standards and Technology of the USA).

NIST Cybersecurity Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Responce Planning	Recovery Planning
Business Environment	Awarencess and Training	Security Continuous Monitoring	Communications	Improvements
Covernance	Data Security	Detection Processess	Analysis	Communications
Risk Assesment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strtegy	Maintenance		Improvements	
	Protective Technology			

Get together with peer organizations
When it comes to developing a program, don't be on an island. Peer up with related organizations and join regional or international organizations.

Collaborate with other departments
Cybersecurity policies, procedures, and plans are often written by a single person or small team of people. It is important to get other business and technology leaders across departments or affiliated "organizations" involved in creation of policies.

Assign Responsibilities and hold Accountability
It is in the organization's best interest to identify responsibilities and accountabilities for various aspects of the cybersecurity program across the entire organization.

Measure Program-Metrics and Share Results
Identify measurements for as many aspects of the program as you possible can and share the results with your superiors or stakeholders frequently. That way you can visualize the success of the program.

What Protelion GmbH can do for you?

Protelion GmbH, together with its global partners, provides Solutions, Products and Services to identify the necessary steps towards an establishment and implementation of your comprehensive cybersecurity strategy.

What can you expect from Protelion GmbH?

Protelion GmbH provides solutions to all aspects as described and focusing its deliveries on a People, Process, Technology approach.

People

- End User Education and Awareness Seminars
- Cyber Range Training for Security Operation Center operators
- Operational Training on Products and Cybersecurity Tools

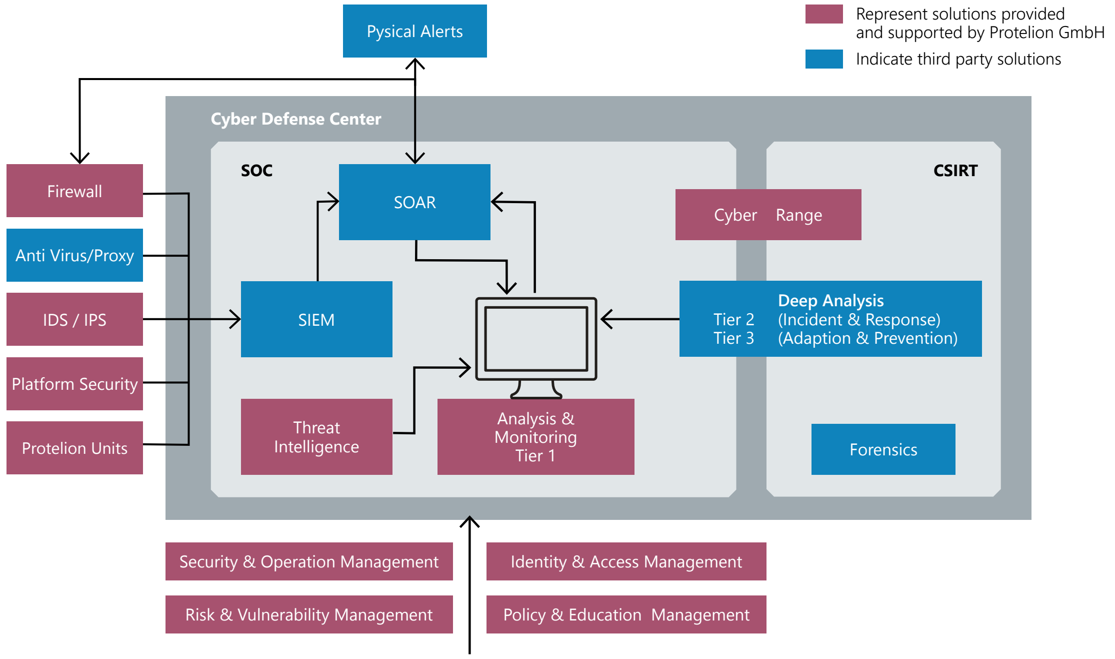
Process

- General Cybersecurity Consulting (ICT Security Architecture)
- Identity and Access Management
- Vulnerability and Risk Assessment
- Support in Process and Policy development, Strategy layout

Technology

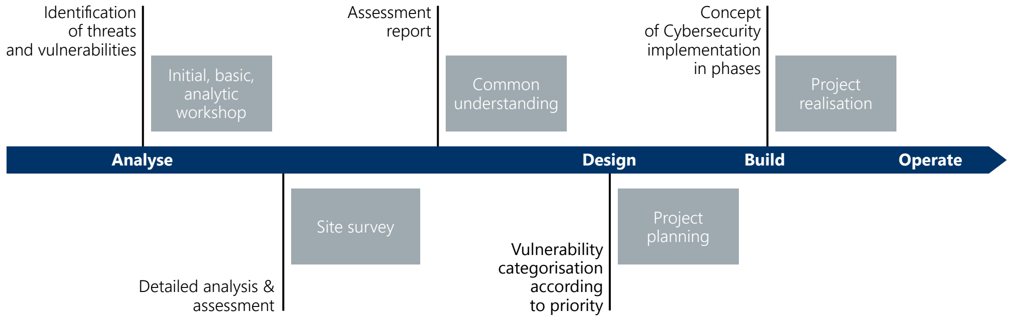
- Analysis and Monitoring Environment
- TDR (Threat Detection and Response)
    - Treat Intelligence
    - Intrusion Detection Systems (IDS)
    - Intrusion Prevention Systems (IPS)
- Next Generation Firewalls
- Platform Security
- Encryption for backbone, distribution networks and End User devices
- Protelion technology supports third-party appliances like: NG-Antivirus, Proxy-Servers etc.

Cybersecurity landscape


🟥 Represent solutions provided and supported by Protelion GmbH
🟦 Indicate third party solutions
Pysical Alerts
Cyber Defense Center
SOC
CSIRT
Firewall
Anti Virus/Proxy
IDS / IPS
Platform Security
Protelion Units
SOAR
SIEM
Threat Intelligence
Analysis & Monitoring Tier 1
Cyber Range
Deep Analysis
Tier 2 (Incident & Response)
Tier 3 (Adaption & Prevention)
Forensics
Security & Operation Management
Identity & Access Management
Risk & Vulnerability Management
Policy & Education Management

Protelion GmbH shares a long time working together philosophy to support our clients in the best way possible.

Working together


Identification of threats and vulnerabilities
Initial, basic, analytic workshop
Assessment report
Common understanding
Concept of Cybersecurity implementation in phases
Project realisation
Analyse
Design
Build
Operate
Detailed analysis & assessment
Site survey
Vulnerability categorisation according to priority
Project planning

Common defined milestone towards a complete cybersecurity solution

PROTELION

Protelion GmbH
Oberwallstrasse 24
D-10117 Berlin
+49 30 206 43 66-0
info@protelion.de
gov.protelion.com

Disclaimer. The information contained herein has been prepared solely for the purpose of providing general information about Protelion and its products. Protelion has taken care in the preparation of the content of these materials. Such information presented is believed to be reliable but is subject to change at any time without notice Protelion disclaims all warranties, express and implied, with respect to such content. Protelion does not represent that the information contained herein is accurate or comprehensive and shall accept no liability for the information contained herein or for any reliance placed by any person on the information. All brands and product names that are trademarks or registered trademarks are the property of their owners. The ™ and ® symbols are omitted in this document.