Accedere

Cyber Security Operation Center

Cyber Security Operation Center (CSOC)

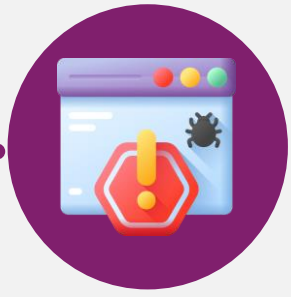
Cybersecurity tailored to your unique needs

Need for having a CSOC

1. Cybersecurity nerve center: Prevent, Monitor, detect and respond.

2. Always on watch, 24/7 cybersecurity vigilance

3. Swift action against threats, rapid response.



4. Data-driven insights, threat intelligence inform defense.

5. Frontline defense, guarding against cyber threats.

6. Coordinating incident response efforts and making informed decisions.

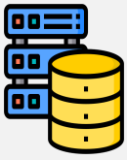
Log Management

Data Collection

Log systems collect diverse user, system, network, and security data.

Log data, centrally stored, aids historical analysis, forensics etc

Storage



Analysis

Log data is analyzed to detect malicious activities using SIEM systems.

Log systems alert on patterns, crucial for swift and precise incident response.

Alerting

Retention and Archiving

Organizations need log retention for compliance, often with extended archives.

Log Management with respect to Compliance

Regulatory Compliance

Regulations mandate log practices for data protection, transparency, etc

Compliance ensure securing sensitive log data, including PII or financial information.

Data Privacy

Auditing and Reporting

Compliance mandates regular log auditing and reporting to meet standards.

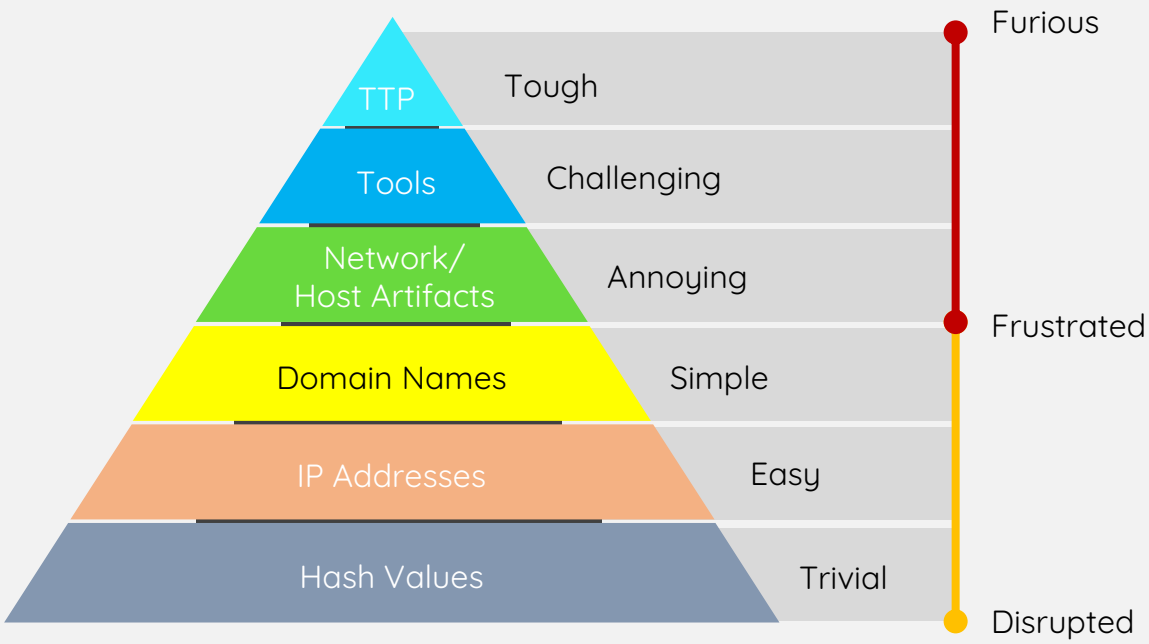
Organizations must document log processes, outlining data collection, storage, and protection.

Cataloging

Penalties

Non-compliance risks fines, legal actions, and reputation damage.

MITRE ATT&CK Framework



Alignment with ATT&CK Framework

Challenges of having a CSOC

1

Ever-Evolving Threat Landscape

Cyber threats evolve with new tactics, demanding continuous learning and adaptation.

2

Shortage of skilled workforce

Global shortage of skilled cybersecurity professionals poses major challenges.

3

Integration of Security Technologies

CSOCs use diverse security tools, integrating seamlessly for efficiency despite compatibility challenges.

4

Data Overload and Alert Fatigue

CSOCs manage vast security data, facing challenges in filtering for threats without alert fatigue.

5

Lack of Standardization

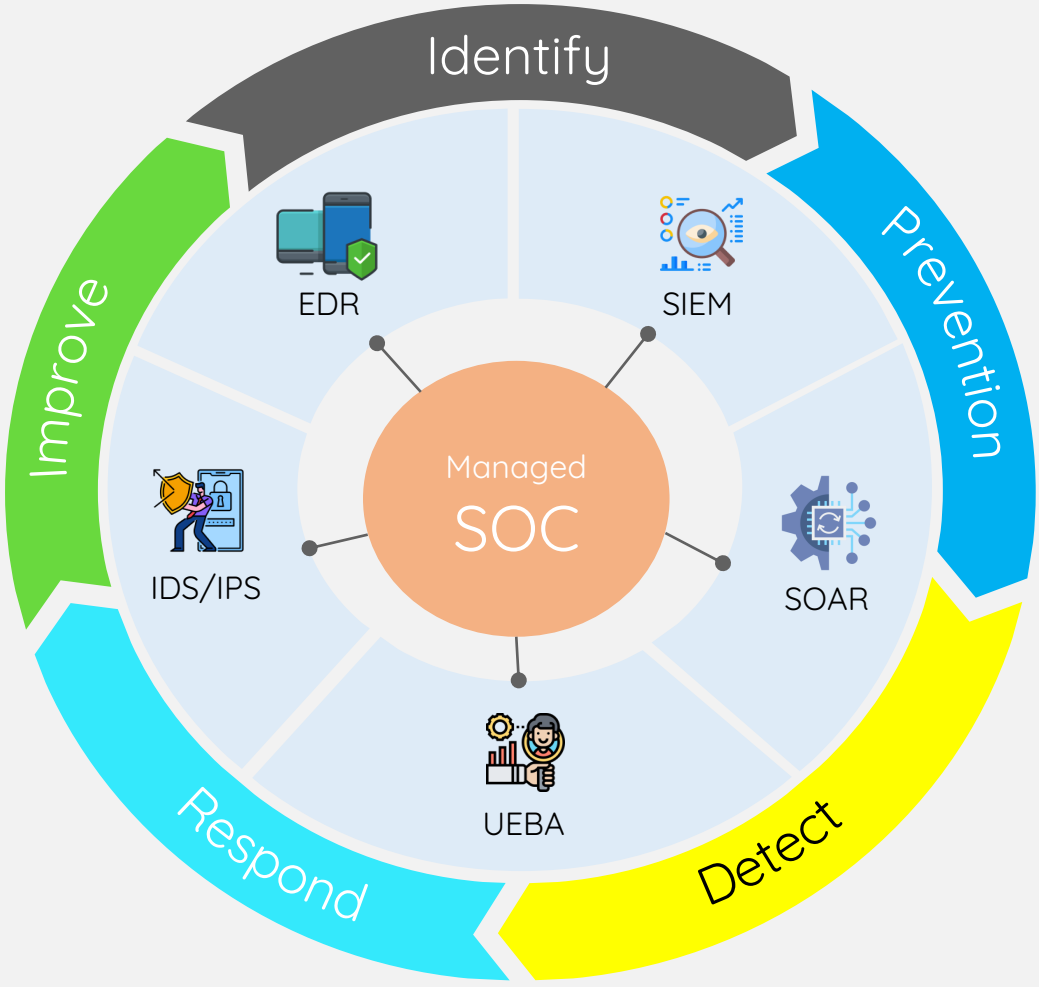
Lack of standardization in security tools, platforms hinders analysis and event correlation.

6

24/7 Availability

SOCs require 24/7 availability for continuous security monitoring and response.

Overview of Our CSOC Services



Dark Web Monitoring

Threat Identification

Risk Assessment

Security Strategy Development

Collaboration and Communication

Real-Time Monitoring and Threat Intelligence

01 Continuous Network and System Monitoring

02 Behavioral Analysis

03 Continuous Updating of Threat Intelligence

04 Correlation of Events

05 Threat Intelligence Sharing and Collaboration

Security Tools and Technologies

1.

Real-Time Monitoring and Threat Intelligence

SIEM solutions for log analysis, threat intelligence platforms for curated threat feeds, and network traffic analyzers.

2.

Threat Hunting

Threat hunting platforms, advanced analytics tools, and machine learning algorithms for anomaly detection..

3.

Integration with Security Technologies

SIEM, EDR, threat feeds, and incident response orchestration enhance security integration.

4.

Integration with MITRE Framework

Tools that provide visibility into various stages of the cyber kill chain, such as penetration testing tools, EDR solutions, etc.

5.

Customizing Security Controls

Application firewalls, data loss prevention (DLP) solutions, and other security policy enforcement tools.

Incident Response Capabilities

Forensic Analysis

Forensic analysis uncovers incident scope, gathers evidence, and refines response strategies

Eliminating incident root cause involves removing malware, closing vulnerabilities, and mitigating impact

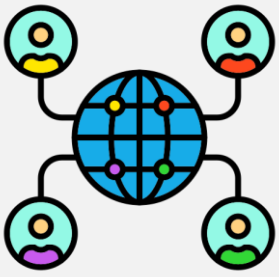
Eradication of Threats

Containment Strategies

Implementing measures to contain the impact of an incident, preventing it from spreading more.

Post-incident reviews, lessons learned and updated response procedures

Continuous Improvement



Clear Communication

Clear communication: Notify internal teams, management, and, if needed, regulatory bodies.

Understanding your threat landscape

A

User Behaviour Analysis

Analyze user behaviour for insider threats, addressing inadvertent or malicious contributions.

B

Risk Assessment and Prioritization

Prioritizing identified threats based on their likelihood and potential impact to guide resource allocation and response strategies.

C

External Threat Landscape Analysis

Assessing global threats, considering geopolitics and trends for anticipating impacts

D

Industry and Sector-Specific Threat Intelligence

Industry-specific threat intel tailors defences to prevalent sector threats.

E

Threat Modelling

Custom threat models consider industry, location, and data nature for anticipating threats.

Integrating with your environment

SIEM Configuration

Collect, analyze logs, customize dashboards and focus on key event.

Endpoint Security

Integrate CSOC with endpoint security for real-time activity data.

Incident Procedure

Define procedure based on severity, collaborate for aligned response.

Continuous Monitoring

Continuous monitoring adapts config, rules, to evolving threats

Network Security

Collect, analyze logs, customize dashboards, and focus on key events.

Defining Incident according to your environment

Customized Incident Definitions

Define tailored incident criteria aligning with risk, business, and compliance.

Behavioral Anomalies

Define incidents from abnormal behaviour, spotting deviations signalling potential security threats.

User Activity Monitoring

Incorporate user activity monitoring into incident definitions for insider threat detection.

Incident Severity Levels

Establishing incident severity hierarchy guides SOC in prioritizing responses by impact

Key Components of CSOC

SIEM

SIEM analyses log data, offering real-time monitoring, event correlation, and security incident alerts from diverse sources.

UEBA analyses user behaviour for anomalies, identifying insider threats or compromised accounts.

UEBA

SOAR

SOAR platforms automate security processes for efficient incident response, reducing manual intervention.

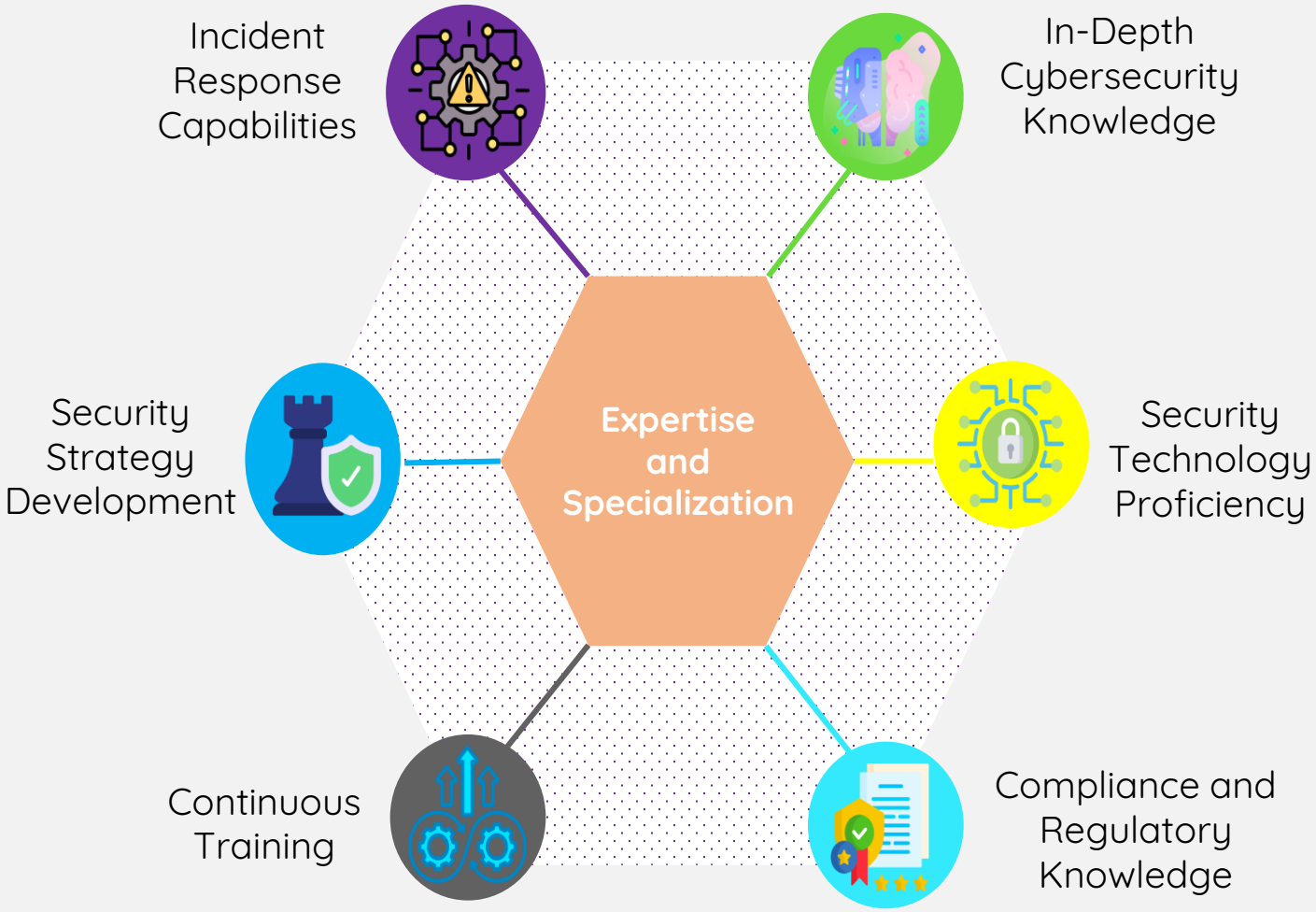
Firewalls and IPS control network traffic with security rules, preventing unauthorized access and blocking known attack patterns.

IDS/IP

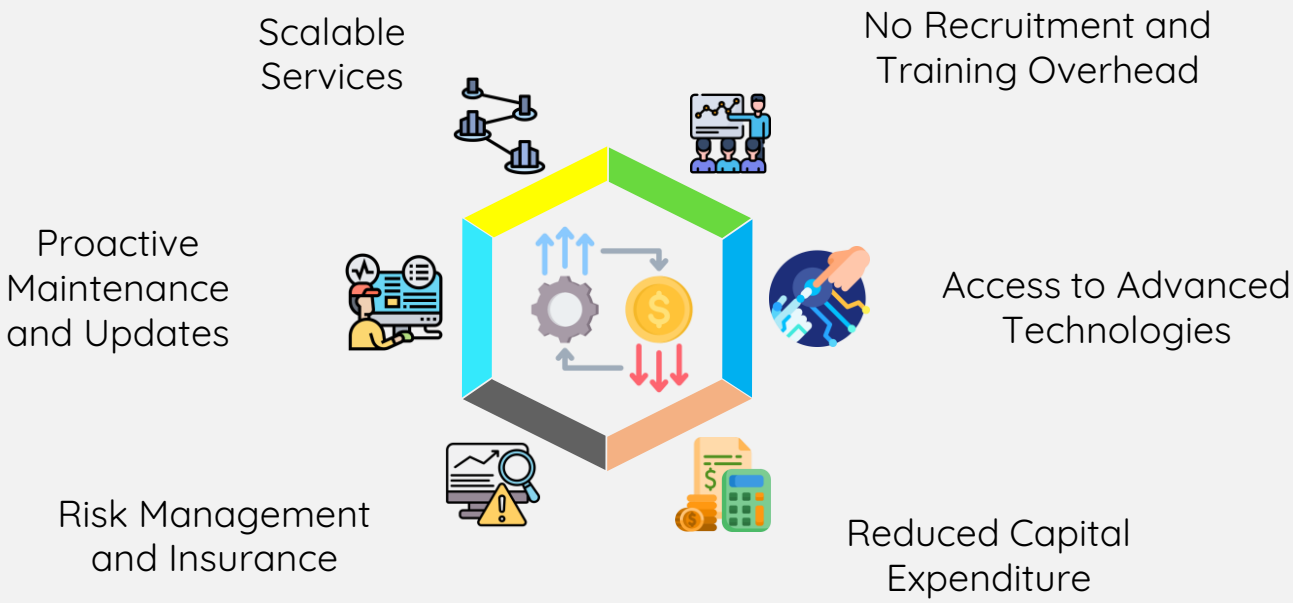
EDR

EDR focuses on securing endpoints, detecting and mitigating threats on individual devices.

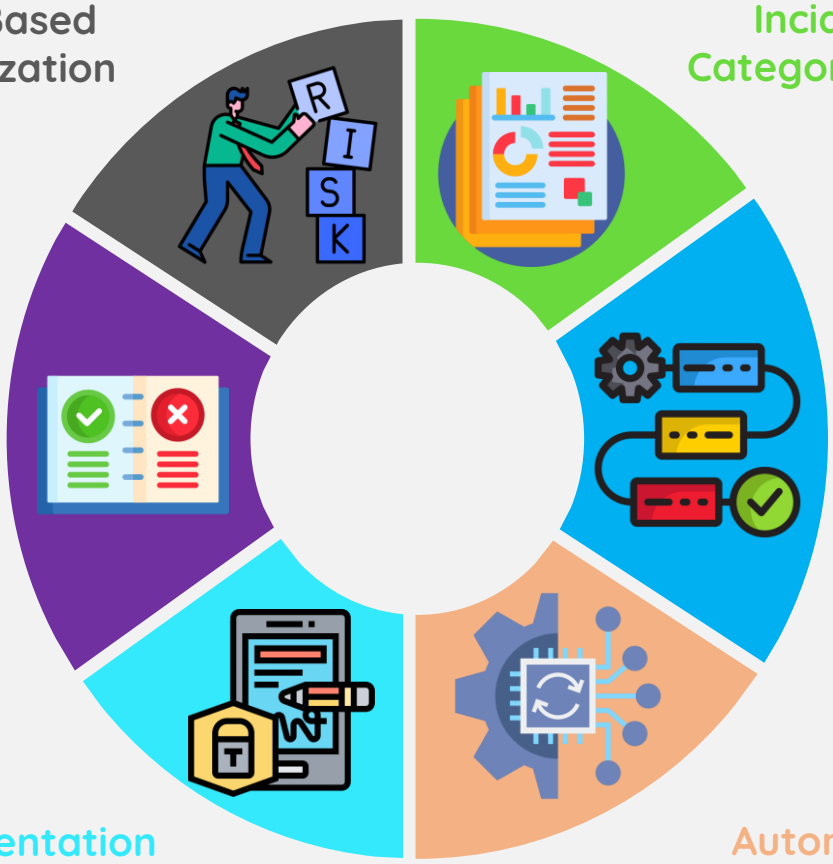
Expertise and Specialization



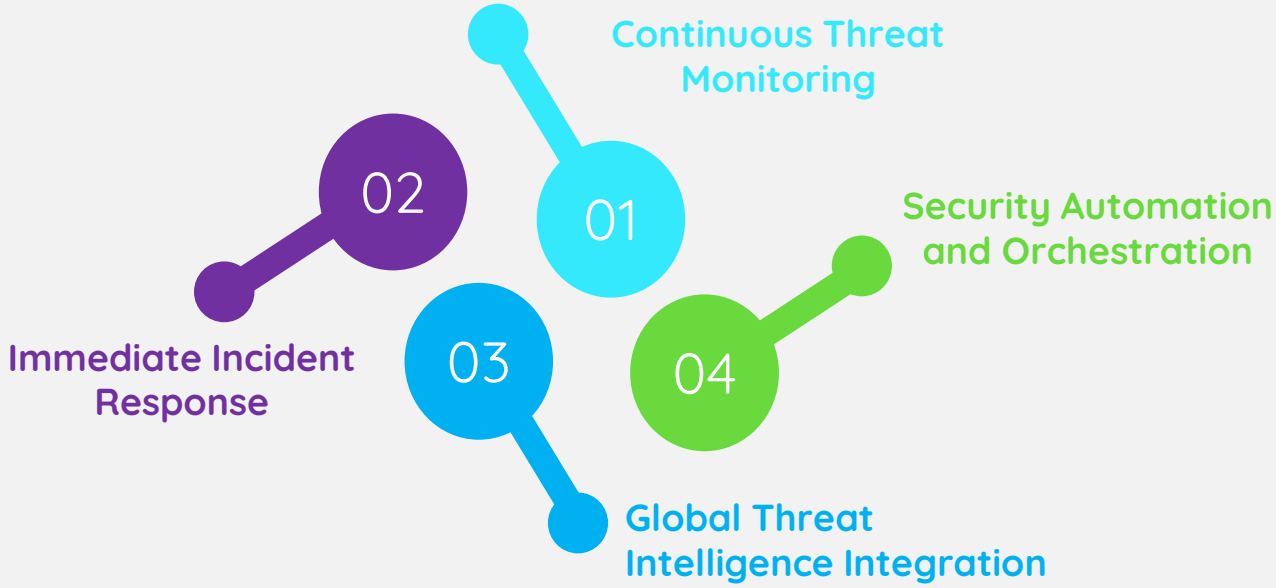
Cost Efficiency and Assets Optimization



Creating rules and workflows



24/7 Monitoring and Response

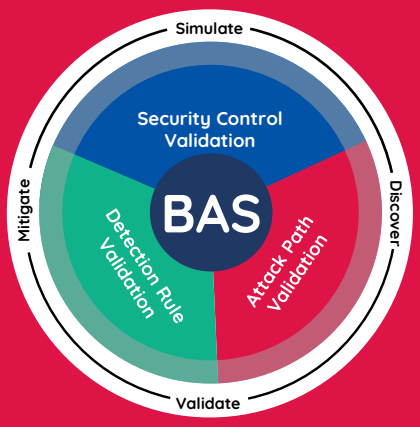


Need help choosing the right services? Check the following use cases:

WHY CSOC?

If you're seeking comprehensive 24/7/365 security monitoring from a remote location, consider CSOC services.

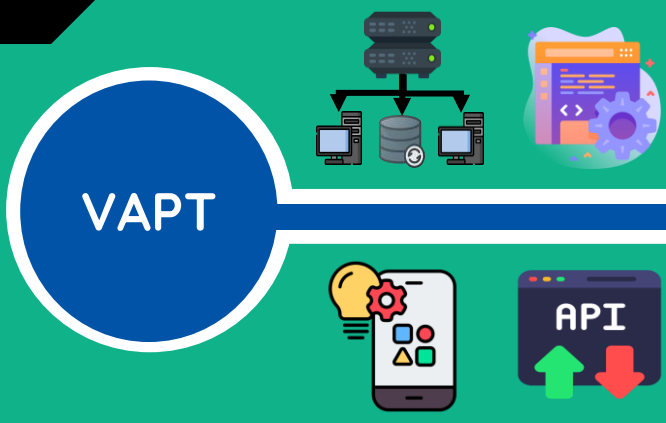
WHY BAS?



If you want to validate the effectiveness of your entire security controls including CSOC by simulating breaches and attacks, BAS services are ideal.

WHY VAPT?

If you're looking for a targeted assessment to identify vulnerabilities in specific areas of your IT infrastructure, VAPT services are the right choice.



Why Accedere?

- Colorado Licensed CPA Firm
- PCAOB Registered Auditors
- CSA STAR Empaneled Auditors
- ISO/IEC Accredited Certification Body
- SOC 1, 2, and 3 Reports, SOC Report for Cloud Security & SOC Report for Privacy
- Cert-In Empaneled Auditors
- Cloud Vulnerability Assessment and Penetration Testing (Cloud VAPT)
- 24x7x365 CSOC Service (Remote)
- Breach and Attack Simulations (BAS)

PCAOB
Public Company Accounting Oversight Board

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations ™

cloud security alliance®

IAS ACCREDITED
Management Systems Certification Body

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
IAF

certin
Handling Computer Security Incidents

Accedere

Contact us today to know more about how BAS can help you safeguard your organization and achieve a proactive approach to cybersecurity. Our team of experts is ready to assist you in developing a comprehensive security validation plan that aligns with your specific needs and goals.