Cybersecurity Assessment Playbook

A strategic roadmap to robust security posture

Security threats amplify with organizational growth

Continued attention, regular upgrades, and prioritizing security as a strategic decision is no longer optional. It's essential!

Rapid expansion & complexity

As organizations scale up, their IT infrastructure grows exponentially, increasing the attack surface and making it difficult to maintain visibility and control.

Data security & compliance

The rise of remote work, cloud adoption, and the increasing sensitive data volumes create significant data security and compliance risks.

Ever increasing threat landscape

Hackers are getting smarter with time and organizations must evolve too. Proactively identifying and responding to emerging threats, vulnerabilities, and security incidents is critical.

Talent shortages

Finding and retaining skilled cybersecurity professionals is a major challenge. This leaves organizations vulnerable to attacks due to limited resources and expertise.

The What and Why of Security Posture Assessment

A **Security Posture Assessment (SPA)** helps an organization understand how secure it is. It evaluates how the organization protects itself from cyber threats by examining its security rules, operations and processes.

WHAT is Security Posture Assessment?

Trending analysis of repeated SPAs

Analyzing existing security vulnerabilities

Recommendations to prevent exploitation

Validating security policy & procedures

Reporting unauthorized data & system access

WHY conduct a Security Posture Assessment?

Identifies and mitigates Risks

Demonstrates due diligence

Enables regulatory compliance

Prioritizes resources

Improves security posture

Security assessment at play

A curated comprehensive execution plan to gauge your organization’s security posture and build a roadmap aligned to your vision.

	Scope and planning	Discovery	Gap assessment	Reporting and recommendation
Activities	• Identify in-scope tech stack, accounts, compliances, services tools and development environments • Access to in-scope environments • Technical Kick-off	• Gather information on client Tech ecosystem like architecture diagram, In-scope components, services and tools, security tools reports and logs, existing security controls and documentation • Review security assessment checklist	• Setup client workshops • Review architecture and details • Identify threats and vulnerabilities • Validate security controls • Analyze and identify gaps in existing security controls, processes, and configurations • Recommended controls	• Executive summary • Gap assessment report • Mitigation and recommendations • Prioritized control
Requirements from customer	• Detail out the business goal and need for this exercise • Setup communication channel with key stakeholders (SME, CISO, IT team etc.) • Defining timelines and workplan	• Documentation and Artifacts • Existing security policies • Architecture diagram, documentation, logs, reports etc.	• Ensure participation of key stakeholders in workshop and related activities.	• Gaps and next steps discussion
Outcomes	• Identify business drivers • Identify scope of assessment • Define boundaries and expectations	• Identify current state and desired state	• Know your security posture • Identify security controls gaps • Recommendations • Compliance evaluation	• Strategic roadmap • Quick wins • Recommendation and guidelines

WHAT WE OFFER

Techniques we use
Trend Analysis, correlation, threat profiling, automated alerting, threat intelligence, Predefined incident response and SOP’s

Processes
Information security processes, policies, SOP’s etc.

Standards we cover
NIST, CIS, CSA, Cloud security benchmarking, MITRE, SIG, SANS etc..

Security maturity stages

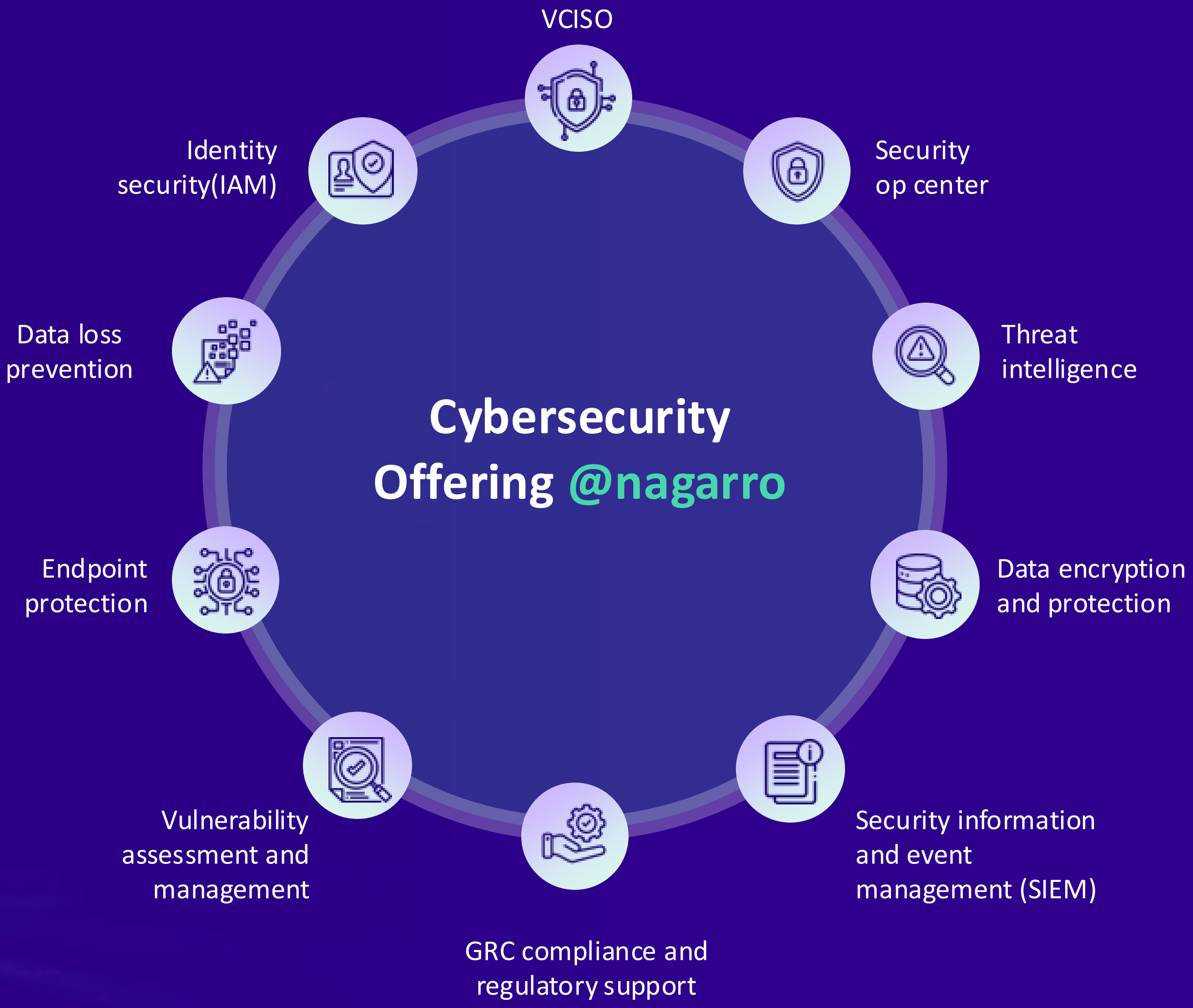
Mapping the current state of the client’s ecosystem in one of the following maturity bucket and therefrom defining the ideal future state.

■ Activities 🟩 Processes 🟦 Technology

	Stage 01 Unaware & non-compliant	*Stage 02* Aware	*Stage 03* Programmatic & aware	*Stage 04* Managed security	*Stage 05* Optimized & sustainable
■	• Lacks Capability • Un-coordinated	• Leaders are risk aware, but the message doesn’t often trickle down the organization.	• Risk aware organization. A capable resource pool with limited clarity of roles and responsibilities	• Risk aware organization. Capable teams with clear roles and responsibilities. A well-defined CISO dept, closely connected to larger organization.	• Culturally transformed organization. Continuously improving organization w.r.t security skills, processes, standards and tech.
🟩	• No formal process	• Basic risk management policies	• Policies, processes defined for a large part of organization with partial adoption	• Defined policies, processes across organization and better adoption.	• Processes automated and mandated across org. Risk and control planning in place along with regular monitoring
🟦	• Open to vulnerabilities	• Only minimally considered during development	• Increased controls for development and enhancements.	• Controls, standards, compliance form the core part of tech related decisions and development.	• Comprehensive controls and automated mechanisms (both offensive and defensive)

Unacceptable → Staying alive → Ideal

We enable our partners to improve their security posture leveraging our cybersecurity and Identity security competencies.


VCISO
Security op center
Threat intelligence
Data encryption and protection
Security information and event management (SIEM)
GRC compliance and regulatory support
Vulnerability assessment and management
Endpoint protection
Data loss prevention
Identity security(IAM)
Cybersecurity Offering @nagarro

nagarro

Bring your most complex problem, its our playground.

Contact us at
cybersecuritypractice@nagarro.com

Together we can
make it happen!

nagarro.com