GIAC Security Essentials (GSEC) Cheat Sheet

One-page cram sheet for practical security basics across network, endpoint, cloud, monitoring, and resilience.

Best for	Focus	Use with
Last review before drills or course revision	Practical security concepts + secure defaults + visibility	Use with ports sheet and commands sheet

1. Security foundations

CIA triad	Confidentiality, integrity, and availability still anchor control selection and risk thinking.
Threat surface	Users, endpoints, networks, cloud, identity, and third parties all expand exposure.
Defense in depth	Strong security uses layered controls, not a single device or tool.
Least privilege	Apply it to users, services, devices, and data paths.

2. Network security basics

Segmentation	Use VLANs, ACLs, firewalls, and trust boundaries to reduce blast radius.
Secure protocols	Prefer SSH, HTTPS, SFTP, LDAPS, and SNMPv3 over plaintext alternatives.
Monitoring sources	Logs, flows, alerts, and packet captures answer different questions.
Remote access	VPNs, MFA, and secure administrative access are recurring essentials.

3. Endpoint and system security

Hardening	Disable unused services, patch regularly, encrypt where needed, and reduce local privileges.
Malware awareness	Know common behavior patterns, not just names: persistence, lateral movement, exfiltration.
Authentication	Strong passwords help, but MFA and proper identity design add much more value.
Backups	Recovery is a security control when ransomware or destructive change hits.

4. Cloud and operational security

Shared responsibility	Cloud providers do not remove the need for customer identity, logging, and config security.
Logging and baselines	Normal behavior helps you spot anomalies in cloud and on-prem environments.
Change management	Secure changes need testing, rollback planning, and validation.

Incident readiness	Preparation, contacts, tools, and evidence handling matter before a real incident.

5. Practical security mindset

Visibility first	If you cannot observe a system, you cannot defend it well.
Business context	The best control fits both the risk and the environment.
Integrated controls	Identity, segmentation, monitoring, and recovery work best together.
Hands-on orientation	GSEC expects more than memorized terms; it expects practical understanding.