Defensive.Network - Security Architecture Stack

Comprehensive Threat & Control Mapping

SECURITY LAYER	ATTACK VECTORS	DEFENSIVE MEASURES	EXAMPLE TOOLS
DATA LAYER			
Data Store	SQL injection, NoSQL injection, unauthorized access, data exfiltration, ransomware	Encryption at rest, access controls, database firewalls, input validation, principle of least privilege	PostgreSQL w/ pgcrypto, MongoDB encryption, AWS RDS encryption, dm-crypt
Application Data	Data tampering, injection attacks, sensitive data exposure, insecure deserialization	Data validation, sanitization, secure coding, encryption in use, integrity checks	OWASP validation libraries, protobuf, Apache Avro, data masking tools
Secrets Management	Hardcoded credentials, secret sprawl, credential stuffing, secret leakage in logs/repos	Centralized secret storage, rotation, encryption, access auditing, short-lived credentials	HashiCorp Vault, AWS Secrets Manager, CyberArk, Bitwarden, git-secrets
APPLICATION			
Services Dependency	Supply chain attacks, malicious packages, dependency confusion, typosquatting	Dependency scanning, SCA, package verification, private registries, SBOM	Snyk, OWASP Dependency-Check, Trivy, npm audit, Renovate
Applications	OWASP Top 10 (XSS, CSRF, broken auth), business logic flaws, command injection	Secure SDLC, code review, SAST/DAST, WAF, input validation, output encoding	ModSecurity, SonarQube, Burp Suite, OWASP ZAP, Semgrep
API Security	Broken authentication, excessive data exposure, rate limiting bypass, API abuse	API gateway, OAuth2/OIDC, rate limiting, API schema validation, API keys rotation	Kong, Apigee, AWS API Gateway, Tyk, 42Crunch
Identity & Access Mgmt	Credential theft, privilege escalation, session hijacking, broken access control	MFA, RBAC/ABAC, SSO, PAM, password policies, session management, zero trust	Keycloak, Okta, FreeIPA, OpenLDAP, Authelia, oauth2-proxy
INFRASTRUCTURE			
Application Framework	Framework vulnerabilities, misconfigurations, insecure defaults, outdated versions	Framework hardening, security updates, secure configuration, CSP headers	Spring Security, Django security middleware, Express Helmet
Runtime System	Runtime vulnerabilities, memory corruption, code injection, deserialization attacks	Runtime hardening, sandboxing, resource limits, security policies	JVM security manager, seccomp, cgroups, AppArmor profiles
Libraries & Supply Chain	Vulnerable libraries, backdoored packages, build system compromise	Library scanning, version pinning, signature verification, SBOM generation	OWASP Dependency-Track, Grype, Syft, in-toto, Sigstore
OS Kernel	Privilege escalation, kernel exploits, rootkits, local attacks	Kernel hardening, LSM (SELinux/AppArmor), syscall filtering, kernel modules control	SELinux, AppArmor, grsecurity, LKRG, sysctl hardening
Memory Protection	Buffer overflow, ROP/JOP attacks, memory disclosure, use-after-free	ASLR, DEP/NX, stack canaries, CFI, memory tagging (MTE)	LLVM SafeStack, Clang CFI, ARM MTE, Intel CET
Container Orchestration	RBAC misconfiguration, exposed API, privilege escalation, supply chain attacks	RBAC/ABAC, network policies, admission controllers, pod security standards	Kubernetes RBAC, OPA/Gatekeeper, Kyverno, Falco
Container Runtime	Container escape, privileged containers, insecure runtime, namespace bypass	Rootless containers, seccomp profiles, AppArmor, capability dropping, read-only FS	containerd, CRI-O, gVisor, Kata Containers, Podman
Container Images & Registry	Malicious images, vulnerable base images, image tampering, registry compromise	Image scanning, signing, minimal base images, private registries, admission control	Trivy, Clair, Notary, Cosign, Harbor, Anchore
Network Segmentation	Lateral movement, flat networks, VLAN hopping, unauthorized access	Microsegmentation, VLANs, VXLANs, zero trust network, network policies	VMware NSX, Cisco ACI, Calico, Cilium, OpenStack Neutron
Firewalls / IDS / IPS	Port scanning, network attacks, DDoS, protocol exploits, traffic analysis	Stateful firewalls, IDS/IPS, DDoS protection, traffic filtering, anomaly detection	Suricata, Snort, pfSense, OPNsense, Zeek, nftables
Network Interfaces	ARP spoofing, MAC flooding, promiscuous mode, packet sniffing, NIC firmware attacks	802.1X, port security, MAC filtering, private VLANs, encrypted tunnels	FreeRADIUS, wpa_supplicant, WireGuard, IPsec, MACsec
Hypervisor	VM escape, hyperjacking, hypervisor vulnerabilities, DoS attacks	Hypervisor hardening, VM isolation, resource limits, security updates	KVM w/ SELinux, Xen, ESXi, Hyper-V, Proxmox VE
Virtual Networks	VLAN hopping, VM-to-VM attacks, vSwitch compromise, traffic interception	Virtual firewall, vSwitch security, network isolation, encrypted vNICs	Open vSwitch, VMware NSX, Linux bridge w/ ebtables
Virtual Storage	Snapshot attacks, VM disk theft, storage covert channels, data remanence	Virtual disk encryption, secure deletion, snapshot encryption, access controls	LUKS for VMs, dm-crypt, VMware encryption, Ceph encryption
Storage Encryption	Data theft, physical disk theft, forensic analysis, cold boot attacks	Full disk encryption, file-level encryption, key management, secure boot integration	LUKS, dm-crypt, ZFS encryption, BitLocker, VeraCrypt
Storage Controllers & Firmware	Firmware backdoors, controller compromise, DMA attacks, malicious firmware updates	Firmware verification, signed updates, controller isolation, firmware TPM integration	UEFI Secure Boot for storage, fwupd, vendor-specific tools
HARDWARE			
Cold Boot Attacks	DRAM remanence, memory freezing, encryption key extraction from RAM	Memory encryption, RAM scrambling, fast memory clearing on shutdown	AMD SME/SEV, Intel TME, memory overwriting tools
HW-assisted Virtualization	VM escape via hardware, nested virtualization attacks, hypercall exploitation	Intel VT-d, AMD-Vi, IOMMU configuration, hardware isolation	Intel VT-x/VT-d, AMD-V/AMD-Vi, ARM virtualization extensions
Trusted Boot / Attestation	Boot process tampering, bootkit installation, measured boot bypass	TPM-based measured boot, remote attestation, boot integrity checking	TPM 2.0, tpm2-tools, Keylime, safeboot, IMA/EVM
BIOS / UEFI	Firmware rootkits, UEFI bootkits, persistent malware, firmware modification	UEFI Secure Boot, firmware updates, write protection, firmware scanning	CHIPSEC, UEFITool, fwupd, flashrom
Secure Boot	Bootloader compromise, unsigned boot components, key compromise	Cryptographic boot verification, key management, signed bootloaders	UEFI Secure Boot, shim, MOK, sbsigntools
Trusted Platform Module	TPM reset attacks, weak PCR policies, physical TPM attacks, bus sniffing	Proper PCR usage, encrypted TPM communication, fTPM security	TPM 2.0 chips, tpm2-tools, clevis, systemd-cryptenroll

Trusted Execution Env	TEE vulnerabilities, side-channel attacks on SGX, TrustZone exploits, voltage glitching, key extraction via power/voltage analysis	TEE isolation, secure enclave design, attestation, side-channel mitigations, voltage regulation	Intel SGX, AMD SEV-SNP, ARM TrustZone, OP-TEE
Peripheral / NIC Firmware	Malicious peripheral firmware, DMA attacks, BadUSB, Thunderbolt attacks	Firmware verification, IOMMU, USB port controls, peripheral attestation	fwupd, USBGuard, Thunderbolt security levels, Intel VT-d
Rogue / HW Implants	Hardware trojans, malicious chips, supply chain hardware modification	Hardware verification, supply chain security, tamper-evident seals, hardware audits	X-ray inspection, hardware security modules, trusted suppliers
Side-Channel Attacks	Spectre, Meltdown, timing attacks, cache attacks, power analysis (DPA/CPA), voltage fluctuation attacks, EM emanation, acoustic cryptanalysis	Microcode updates, kernel page table isolation, constant-time crypto, voltage regulation, EM shielding, power supply filtering	Linux mitigations (KPTI, retpoline), Intel/AMD microcode, TEMPEST shielding, power line filters
CPU / Microcode	CPU vulnerabilities, microcode bugs, speculative execution exploits	Microcode updates, CPU feature controls, vulnerability mitigations	intel-microcode, amd64-microcode, kernel boot parameters
Physical Access	Direct hardware access, console access, boot device manipulation, component theft	Physical security controls, locked racks, tamper detection, full disk encryption	Chassis intrusion detection, cable locks, security cages, tamper-evident tape
Remote / OOB Management	IPMI vulnerabilities, BMC exploits, iLO/iDRAC attacks, default credentials	OOB network isolation, credential management, firmware updates, disable unused features	ipmitool, Redfish, network segmentation, credential rotation
CROSS-CUTTING			
Logging / Monitoring / SIEM	Log tampering, log flooding, blind spots, insufficient logging, log injection	Centralized logging, log integrity, real-time monitoring, correlation rules, retention	ELK Stack, Graylog, Wazuh, OSSEC, Splunk, Prometheus, Grafana
Encryption in Transit	MITM attacks, protocol downgrade, weak ciphers, certificate spoofing, traffic interception	TLS 1.3, certificate pinning, HSTS, strong cipher suites, mutual TLS	OpenSSL, Let's Encrypt, certbot, nginx/Apache TLS, WireGuard, mTLS
Vulnerability Management	Unpatched vulnerabilities, zero-days, misconfigurations, exposed services	Regular scanning, vulnerability assessment, prioritization, remediation tracking	OpenVAS, Nessus, Trivy, Nuclei, Rapid7, Qualys
Patch Management	Exploitation of known vulnerabilities, outdated software, missing security updates	Automated patching, testing procedures, rollback plans, patch compliance monitoring	Ansible, SaltStack, Puppet, unattended-upgrades, WSUS, Spacewalk
Configuration Management	Misconfigurations, configuration drift, insecure defaults, unauthorized changes	Infrastructure as Code, baseline hardening, configuration validation, drift detection	Ansible, Terraform, Chef, Puppet, CIS Benchmarks, OpenSCAP
Incident Response	Delayed detection, inadequate response, evidence destruction, lack of playbooks	IR plan, playbooks, forensics tools, communication plan, tabletop exercises	TheHive, Velociraptor, GRR, SOAR platforms, forensics suites
Threat Intelligence	Unknown threats, outdated intelligence, false positives, intelligence gaps	Threat feeds, IOC integration, threat hunting, ISAC participation, CTI platforms	MISP, OpenCTI, AlienVault OTX, abuse.ch feeds, VirusTotal
Security Testing & Audits	Undiscovered vulnerabilities, compliance gaps, security control failures	Penetration testing, red team exercises, security audits, code review, compliance checks	Metasploit, Cobalt Strike, Burp Suite Pro, Nuclei, audit frameworks
Backup & Disaster Recovery	Ransomware, data destruction, backup corruption, recovery failures	3-2-1 backup rule, immutable backups, air-gapped backups, recovery testing	Restic, Borg, Bacula, Veeam, ZFS snapshots, rsnapshot
Change Management	Unauthorized changes, malicious modifications, change-related outages	Change approval process, security review, change tracking, rollback capability	GitLab/GitHub workflows, JIRA, ServiceNow, peer review processes
Compliance & Governance	Regulatory violations, audit failures, policy violations, documentation gaps	Policy enforcement, compliance frameworks, regular audits, GRC platforms	OpenSCAP, compliance-as-code, InSpec, ISO 27001, NIST CSF, CIS Controls
Risk Management	Unidentified risks, inadequate risk treatment, resource misallocation	Risk assessment, risk register, threat modeling, risk-based prioritization	FAIR, OCTAVE, risk matrices, threat modeling tools (STRIDE, PASTA)

by Martin Holovsky @ Defensive.Network