

Category	Subcategory	Name	Short Description	Link
SOAR/Automation		TheHive	Open-source incident response platform	https://thehive-project.org/
SOAR/Automation		Cortex	Automation engine for DFIR	https://thehive-project.org/cortex/
SOAR/Automation		Shuffle SOAR	Open-source SOAR automation platform	https://shuffler.io
SOAR/Automation		StackStorm	Event-driven automation platform	https://stackstorm.com
SIEM		Wazuh	Open-source SIEM & XDR	https://wazuh.com
SIEM		Elastic Security	SIEM based on Elastic Stack	https://www.elastic.co/security
SIEM		Graylog Open	Log management & SIEM	https://www.graylog.org/products/open
SIEM		OpenSearch Security Analytics	Open-source SIEM module	https://opensearch.org
MDR/SOC		Security Onion	SOC platform for monitoring and analytics	https://securityonionsolutions.com/software
MDR/SOC		RockNSM	Network security monitoring	https://rocknsm.io
MDR/SOC		MozDef	Mozilla's incident management system	https://github.com/mozilla/MozDef
Identity		FreeIPA	Integrated identity and authentication system	https://www.freeipa.org
Identity		Keycloak	Open-source SSO & identity management	https://www.keycloak.org
Identity		AuthLibre	Identity & auth library	https://github.com/authlib/authlib
Access Management		Authelia	2FA and SSO reverse proxy	https://www.authelia.com
Access Management		LemonLDAP::NG	WebSSO & access management	https://lemonldap-ng.org
Access Management		OpenAM	Community IAM platform	https://github.com/OpenRock/OpenAM
DFIR		Velociraptor	Endpoint DFIR & live forensics	https://www.velocidex.com
DFIR		GRR Rapid Response	Remote live forensics platform	https://github.com/google/grr
DFIR		CyberChef	Digital forensics & data transformation tool	https://gchq.github.io/CyberChef
Endpoint Security		OSQuery	Endpoint visibility & telemetry	https://osquery.io
Endpoint Security		Falco	Runtime security detection	https://falco.org
Endpoint Security		OpenEDR	Open-source endpoint detection	https://github.com/ComodoSecurity/openedr
Endpoint Security		ClamAV	Open-source antivirus engine	https://www.clamav.net
Asset Management		NetBox	Infrastructure resource modeling	https://netbox.dev
Asset Management		Snipe-IT	IT asset management system	https://snipeitapp.com
Asset Management		OCS Inventory	Inventory & asset discovery	https://ocsinventory-ng.org
Asset Management		GLPI	ITSM & asset management	https://glpi-project.org
Network Security	VPN	WireGuard	Modern secure VPN protocol	https://www.wireguard.com
Network Security	VPN	OpenVPN	Open-source VPN platform	https://openvpn.net/community
Network Security	VPN	StrongSwan	IPsec-based VPN platform	https://www.strongswan.org
Network Security	VPN	SoftEther	Multi-protocol VPN	https://www.softether.org
Network Security	Firewalls	OPNsense	Open-source firewall & routing	https://opnsense.org
Network Security	Firewalls	pfsense	Firewall & routing platform	https://www.pfsense.org
Network Security	Firewalls	IPFire	Hardened firewall distribution	https://www.ipfire.org
Network Security	Firewalls	VyOS	Router & firewall OS	https://vyos.io
AppSec	SAST/DAST	OWASP ZAP	Web security scanner	https://www.zaproxy.org
AppSec	SAST/DAST	Semgrep	Static analysis tool	https://semgrep.dev
AppSec	SAST/DAST	Bandit	Python security scanner	https://bandit.readthedocs.io
AppSec	SAST/DAST	Brakeman	Rails security scanner	https://brakemanscanner.org

AppSec	SAST/DAST	Gosec	Go static analysis scanner	https://github.com/securego/gosec
Supply Chain		Sigstore	Signing & supply chain integrity	https://www.sigstore.dev
Supply Chain		Cosign	Container signing	https://github.com/sigstore/cosign
Supply Chain		Trivy	Vulnerability & SBOM scanner	https://trivy.dev
Supply Chain		Syft	SBOM generator	https://github.com/anchore/syft
Supply Chain		Grype	Vulnerability scanner	https://github.com/anchore/grype
Supply Chain		Dependency-Track	SBOM & supply chain risk	https://dependencytrack.org
Supply Chain		OpenSSF Scorecards	Repo security scoring	https://github.com/ossf/scorecard
Supply Chain		in-toto	Supply chain integrity framework	https://in-toto.io
Cloud Security		kube-bench	CIS benchmark auditing	https://github.com/aquasecurity/kube-bench
Cloud Security		kube-hunter	Kubernetes penetration testing	https://github.com/aquasecurity/kube-hunter
Cloud Security		Falco	Runtime threat detection	https://falco.org
Cloud Security		Cloud Custodian	Cloud governance & security	https://cloudcustodian.io
Email Security		Rspamd	Spam filtering engine	https://rspamd.com
Email Security		SpamAssassin	Spam detection	https://spamassassin.apache.org
Email Security		OpenDMARC	DMARC validation	https://github.com/trusteddomainproject/OpenDMARC
Email Security		OpenDKIM	DKIM signing/verification	https://www.opendkim.org
Encryption		Cryptomator	Client-side encryption	https://cryptomator.org
Encryption		VeraCrypt	Disk encryption	https://www.veracrypt.fr
Compliance		OpenGRC	Governance & compliance toolkit	https://github.com/strongdm/open-grc
Compliance		ArcherySec	Vulnerability & compliance tool	https://archerysec.io
Compliance		OpenControl	Open security compliance	https://opencontrol.dev
Vulnerability Management		OpenVAS	Vulnerability scanning	https://www.openvas.org
Vulnerability Management		Nmap	Network scanner	https://nmap.org
Vulnerability Management		Nuclei	Template-based scanning	https://nuclei.projectdiscovery.io
Vulnerability Management		Nikto	Web vulnerability scanner	https://cirt.net/Nikto2