Category	Main Type	Sub-Type / Components	Features / Functions	Purpose / Goal	Example Tools / Systems	Metrics / Evidence
Detection Control	**Event Triggers**	Rule-based, Behavior-based, Anomaly-based, Signature-based	Manual or automated firing of detection rules	Verify rule activation & coverage	Sigma, Falco, Suricata, Zeek	Detection coverage %, rule execution logs
Threat Simulation	**Synthetic Attack Generator**	Atomic Red Team, MITRE ATT&CK TTP injector, Fuzzer	Simulate attacker behavior to test alerts	Validate detection fidelity	Atomic Red Team, Infection Monkey, Caldera	TTP coverage matrix, detection delta
SIEM Integration	**Log Collection & Correlation**	Syslog, OTEL, FluentBit, ELK, Splunk, Loki	Aggregate detection logs from multiple sources	Ensure all sources feed into SOC	ELK stack, Grafana Loki	Log ingestion rate, alert forwarding rate
Security Telemetry	**Endpoint & Network Sensors**	Agent-based (OSQuery), Network taps, Kernel probes	Observe all runtime layers (syscalls, APIs, network)	Validate visibility completeness	OSQuery, eBPF, Falco, OpenTelemetry	% event types observed, missing signal map
Alert Pipeline	**Alert Routing & Enrichment**	Enrich, deduplicate, correlate alerts	Add context (user, asset, severity, MITRE tag)	Produce actionable alerts	ElastAlert, Prometheus Alertmanager	MTTA (Mean Time to Alert), enrichment success rate
Detection Testing	**Regression & Validation Tests**	Unit, Integration, System, Red vs Blue tests	Validate detection logic after code/policy changes	Prevent silent alert failures	pytest, cargo-test, k6, GoTest	% rules firing after update, false-negative rate
Detection Coverage Mapping	**MITRE ATT&CK Mapping**	Enterprise, Cloud, Container, Blockchain matrix	Map detections to ATT&CK techniques	Measure completeness of coverage	ATT&CK Navigator, Sigma2ATT&CK	% TTP coverage, duplicate rules

Category	Main Type	Sub-Type / Components	Features / Functions	Purpose / Goal	Example Tools / Systems	Metrics / Evidence
Response Simulation	**Alert Response Triggers**	Runbooks, SOAR playbooks, automated response	Trigger the whole detection-to-response chain	Validate SOC readiness	Cortex XSOAR, Shuffle, StackStorm	End-to-end response success rate
Metrics Collection	**Detection Efficacy Metrics**	Precision, Recall, Latency, Noise ratio	Evaluate detection quality	Reduce false positives & misses	Prometheus, Grafana, ELK metrics	FPR, FNR, latency ms, event volume
Forensics & Replay	**Event Replay & Audit**	Replay historic logs to re-test new rules	Ensure new rules detect past attacks	Elastic Replay, Zeek, Loki	# retroactive detections, replay fidelity	
CI/CD Integration	**Security Gates & Hooks**	"Detection smoke tests" in CI	Auto-trigger detections per deployment	Guarantee continuous readiness	GitHub Actions, OPA, Kyverno	CI gate pass/fail, alert webhook trigger
Detection Inventory	**Ruleset Cataloging**	Inventory of all active detections	Centralize and version detection logic	Prevent rule drift & duplication	GitOps repo, YAML rulesets	Ruleset version, drift delta
AI/ML-Enhanced Detection	**Anomaly Models**	Statistical, ML, LSTM, Transformer models	Generate synthetic anomalies to trigger ML alerts	Test model adaptability	PyOD, Grafana Mimir, Loki ML	Model retraining success, drift %
Blockchain & Smart-Contract Detection	**On-chain Triggers**	Reentrancy, price manipulation, governance events	Simulate malicious transactions to trigger monitors	Ensure DeFi/Web3 SOC coverage	Forta, Tenderly, EigenLayer Watchers	# triggered alerts per contract event
User Behavior Analytics (UBA)	**Identity-based Detection**	Credential misuse, privilege escalation	Simulate abnormal login or token use	Verify IAM anomaly alerts	UEBA engine, OpenSearch Dashboards	% user anomalies caught
Deception / Honeypot	**Trap Triggers**	Fake APIs, wallets, nodes	Trigger decoy events	Test lateral movement detections	Canarytokens, HoneyDB	# traps triggered, attacker dwell time

Category	Main Type	Sub-Type / Components	Features / Functions	Purpose / Goal	Example Tools / Systems	Metrics / Evidence
Testing Automation	**Chaos / Fault Injection**	Drop logs, corrupt telemetry, delay events	Verify alert pipeline resilience	Ensure fault-tolerant detection flow	Chaos Mesh, Gremlin	% alerts lost during fault test
Audit & Evidence	**Compliance Verification**	SOC2, ISO, NIST control mapping	Prove detection system operational	Satisfy governance & audit	OPA, Evidence.dev	Audit report, detection attestation