

CYBERSECURITY AS A SERVICE

Blue Teaming as a Service

KEY SERVICES

Comprehensive Cybersecurity Defense
for Enterprise Resilience



ENTERPRISE SECURITY

What is Blue Teaming as a Service?

A managed defensive capability that protects assets, detects threats, and coordinates rapid response — continuously.

CONTINUOUS

Monitoring and proactive detection across the enterprise.

SCALABLE

Flexible service delivery aligned to risk and growth.

INTEGRATED

Embedded into client technology, processes, and teams.

DEFEND

Resilience by design

Core Blue Team Workflow

A closed-loop operating cycle engineered for speed, evidence, and continuous improvement.



Every incident strengthens the next detection.

Security Monitoring

Always-on visibility across enterprise telemetry.

SIEM correlation

Comprehensive log collection and analysis

Real-time alert monitoring

Rapid threat detection with contextual prioritization

24 / 7 SECURITY OPERATIONS

Threat Detection & Response

01

Behavioral detection

Identify suspicious activity and anomalous behavior.

02

Incident investigation

Establish scope, root cause, and affected assets.

03

Alert triage

Prioritize signals by risk, confidence, and impact.

04

Containment

Limit exposure and coordinate remediation actions.

05

Response coordination

Manage the incident lifecycle end to end.

EDR / XDR Services

01

Endpoint monitoring

Continuously observe endpoint activity and telemetry.

02

Malware detection

Apply advanced heuristics to malicious artifacts.

03

Behavior analysis

Detect anomalous processes and execution chains.

04

Endpoint isolation

Contain compromised hosts with decisive action.

05

Threat hunting

Expose stealthy actors across correlated data.

Threat Hunting

01

Beyond alerts

Proactively test hypotheses across the environment.

02

IOC-based hunting

Search for known malicious indicators and traces.

03

Behavioral hunting

Find unknown tactics through anomalous behavior.

04

MITRE ATT&CK

Structure hunts around adversary techniques.

05

Persistent threats

Reveal hidden and advanced actor activity.

Vulnerability Management

01

Asset scanning

Regularly assess the enterprise attack surface.

02

Risk prioritization

Rank findings by exploitability and business impact.

03

Patch monitoring

Track timely fixes across affected systems.

04

Misconfiguration detection

Identify insecure settings and control gaps.

05

Verification

Track remediation through validated closure.

Digital Forensics

01

Endpoint analysis

Trace intrusion paths and attacker activity.

02

Memory analysis

Detect in-memory threats and volatile artifacts.

03

Disk & log evidence

Gather durable evidence across data sources.

04

Timeline reconstruction

Rebuild the sequence of attack events.

05

Evidence preservation

Maintain secure collection and chain of custody.

Threat Intelligence

01

IOC monitoring

Track emerging indicators across the threat landscape.

02

Reputation tracking

Assess IP, domain, and hash risk signals.

03

Feed integration

Combine multiple sources into actionable context.

04

Campaign tracking

Connect activity to evolving adversary campaigns.

05

Actor intelligence

Add attribution, intent, and risk context.

Network Security

01

Traffic monitoring

Identify anomalous patterns in network flows.

02

IDS / IPS validation

Investigate and validate prevention alerts.

03

Firewall monitoring

Review configurations, changes, and events.

04

DNS security

Detect malicious resolution and domain behavior.

05

Anomaly detection

Alert on deviations from expected baselines.

Email Security

01

Phishing defense

Detect and prevent deceptive email threats.

02

Attachment analysis

Examine suspicious files and payloads.

03

URL analysis

Block harmful destinations before impact.

04

Threat investigations

Trace campaigns, senders, and affected users.

05

BEC monitoring

Detect impersonation and financial fraud patterns.

Cloud Security

Native visibility and coordinated defense for dynamic cloud environments.



■ Activity & telemetry

Monitor cloud events across services.

■ IAM monitoring

Detect risky identity and access behavior.

■ Misconfigurations

Expose insecure cloud control settings.

■ Native detection

Use cloud-native signals to identify threats.

■ Incident response

Coordinate containment across cloud teams.

Identity & Access Monitoring

01

Login analytics

Monitor sign-ins for anomalous behavior.

02

Privileged accounts

Alert on sensitive access and account activity.

03

Brute-force detection

Identify repeated authentication attacks.

04

Impossible travel

Expose geographically inconsistent sessions.

05

Compromise response

Investigate and contain account takeover.

Security Automation & Compliance

AUTOMATION

Move at machine speed.

- SOAR integration
- Automated enrichment & investigation
- Automated containment actions
- Response playbook execution

COMPLIANCE

Prove control effectiveness.

- Security policy monitoring
- Audit log management
- Compliance reporting & assessments
- Evidence collection for audits

Incident Response & Reporting

INCIDENT LIFECYCLE

**Classify → Contain →
Eradicate → Recover**

Prioritized action, operational recovery support, and post-incident lessons learned.

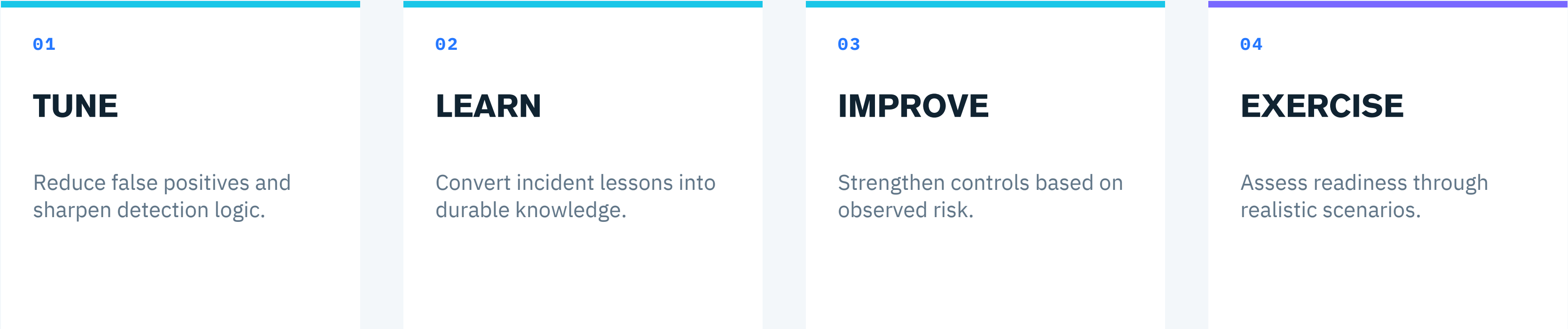
SECURITY VISIBILITY

**Dashboards that turn evidence
into decisions**

SOC dashboards • incident reports • risk scores •
attack timelines • executive KPIs

Continuous Security Improvement & Readiness

Defense is a living system — every signal, incident, and exercise advances the posture.



An evolving defense posture for an evolving threat landscape.

One Platform. Full-Spectrum Defense.

BLUE TEAMING

The critical defensive pillar connecting people, telemetry, intelligence, and response.

PROTECT → DETECT → RESPOND → RECOVER

- RED TEAMING
- MALWARE ANALYSIS
- THREAT INTELLIGENCE
- SOC / SIEM
- INCIDENT RESPONSE

Partner with us for comprehensive, managed cybersecurity defense.