



# CYRAVEX SECURITY

OFFENSIVE INSIGHT. DEFENSIVE STRENGTH.

SAMPLE DELIVERABLE / MANAGED SECURITY POSTURE

## Managed Security Posture Report

Illustrative client-facing monthly report demonstrating CyraVex Security posture reporting, vulnerability prioritization, detection engineering, and operational guidance.

CLASSIFICATION

**PUBLIC SAMPLE**

No real client data

SERVICE MODEL

**MANAGED SECURITY**

Scoped support • not 24/7 MDR

VERSION

**1.0**

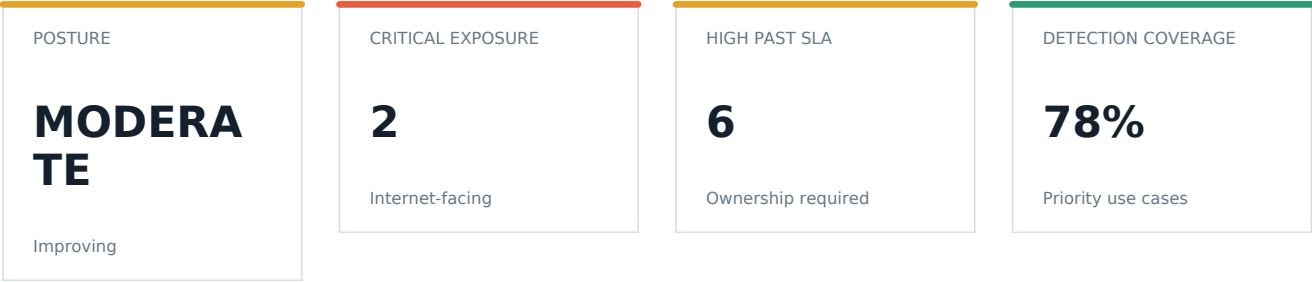
September 2026

Fictional environment and metrics only. No real client systems or telemetry were used.

01 / EXECUTIVE SUMMARY

# Risk is concentrated in exposure aging and detection gaps

The illustrative environment has strong endpoint visibility and improving cloud controls, but two critical internet-facing exposures, aging high-risk vulnerabilities, and uneven data-exfiltration coverage require management attention.



EXECUTIVE MESSAGE

The environment does not need more security tooling first. It needs disciplined remediation ownership, tighter external exposure control, and higher-quality detections around cloud privilege abuse and data movement.

- Contain the two critical internet-facing exposures immediately.
- Reduce the backlog of high-risk vulnerabilities older than 30 days.
- Improve data-exfiltration and cloud-privilege detection coverage before expanding lower-value rules.
- Use named owners, due dates, and risk-acceptance review dates for every material exception.

02 / SERVICE CONTEXT

# Defined managed-security support, not implied 24/7 MDR

This illustrative report represents a scoped managed-security support engagement. It demonstrates the type of posture reporting, vulnerability prioritization, detection engineering, and operational guidance Cyravex can provide.

INCLUDED IN THIS MODEL

Monthly vulnerability review, exposure prioritization, remediation tracking, detection engineering support, alert-quality review, posture reporting, and a scheduled risk discussion.

NOT IMPLIED BY THIS REPORT

24/7 SOC staffing, guaranteed response SLAs, continuous incident command, unlimited investigations, continuous threat hunting, or formal compliance attestation.

OPERATING PRINCIPLE

Measure security outcomes, not tool activity. Every metric should connect to a risk decision, accountable owner, remediation action, or validated control.

03 / DATA & METHODOLOGY

# How the posture view is assembled

Production reporting should use verified source data and documented calculation logic. This sample uses fictional metrics solely to demonstrate report structure and client communication quality.

| SOURCE                 | PURPOSE                                             | CADENCE      | QUALITY CHECK               |
|------------------------|-----------------------------------------------------|--------------|-----------------------------|
| Vulnerability platform | Asset findings, severity, age, exposure state       | Daily/Weekly | Reconcile owner + timestamp |
| EDR / endpoint         | Coverage, policy state, high-risk endpoint gaps     | Daily        | Reconcile owner + timestamp |
| SIEM / log platform    | Log-source health, use-case coverage, alert quality | Continuous   | Reconcile owner + timestamp |
| Cloud platforms        | Configuration, IAM, public exposure, audit logs     | Daily/Weekly | Reconcile owner + timestamp |
| Identity provider      | MFA, privileged access, risky sign-ins              | Daily        | Reconcile owner + timestamp |
| Ticketing / exceptions | Owners, due dates, acceptance, remediation evidence | Weekly       | Reconcile owner + timestamp |

- Normalize asset identity before counting coverage or vulnerability age.
- Separate newly discovered findings from reopened or accepted items.
- Validate data freshness before executive reporting.
- Document metric definitions so trends are comparable month to month.

# Monthly posture at a glance

| DOMAIN                    | SCORE                  | STATUS       |
|---------------------------|------------------------|--------------|
| External attack surface   | <div><div></div></div> | Needs action |
| Vulnerability remediation | <div><div></div></div> | Needs action |
| Endpoint coverage         | <div><div></div></div> | Strong       |
| Cloud configuration       | <div><div></div></div> | Improving    |
| Detection engineering     | <div><div></div></div> | Improving    |
| Identity controls         | <div><div></div></div> | Good         |

IMPROVING

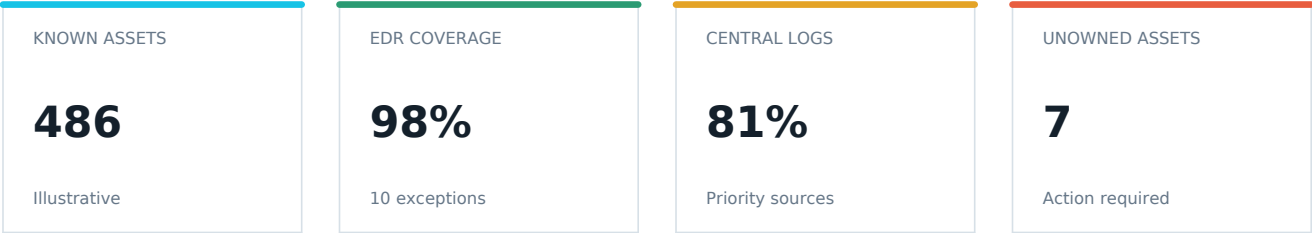
Endpoint coverage and cloud-baseline remediation improved during the illustrative period. Identity MFA adoption also increased.

PRIMARY RISK

Remediation aging remains the main operational weakness; material findings can persist even when discovery and monitoring are strong.

05 / ASSET & TELEMETRY

# Visibility is strong, but critical gaps must be explicit



|                                                                                                                                                                                        |                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div><b>COVERAGE STRENGTHS</b></div> <div>Workstations, privileged endpoints, major cloud accounts, identity events, and internet-facing application logs have broad visibility.</div> | <div><b>COVERAGE GAPS</b></div> <div>Several legacy servers, one acquired SaaS integration, and selected database audit logs are not yet consistently centralized or assigned to an accountable owner.</div> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- Assign an owner to every unowned asset before discussing control maturity.
- Prioritize telemetry by investigation value and business risk, not by log volume.
- Track EDR/log exceptions separately with expiry and compensating controls.

## 06 / EXTERNAL ATTACK SURFACE

# Internet-facing exposure requires tighter change discipline

| AREA                      | COUNT | CURRENT RISK                   | OWNER              |
|---------------------------|-------|--------------------------------|--------------------|
| Public applications       | 18    | 2 high-risk observations       | Product / Platform |
| Administrative interfaces | 4     | 1 critical restriction gap     | Infrastructure     |
| VPN / remote access       | 3     | 1 high-risk outdated component | IT                 |
| Cloud public endpoints    | 11    | 2 policy exceptions            | Cloud              |
| Domains / DNS             | 27    | No critical issue              | IT / Product       |

## EXPOSURE CONTROL

Require explicit owner, business purpose, authentication expectation, logging, and review date for every administrative or sensitive internet-facing service.

- Restrict administrative interfaces by VPN, identity-aware proxy, allowlist, or equivalent control.
- Continuously identify newly exposed services and compare against approved inventory.
- Retire stale DNS records and unsupported services.
- Verify public cloud endpoints do not bypass intended application controls.

07 / VULNERABILITY EXPOSURE

# Highest-priority remediation queue

|                                                      |          |             |
|------------------------------------------------------|----------|-------------|
| V-01                                                 | CRITICAL | Open        |
| Internet-facing remote-code execution exposure       |          |             |
| Owner: Infrastructure   Target: 48 hours             |          |             |
| V-02                                                 | CRITICAL | Open        |
| Public admin interface with weak access restrictions |          |             |
| Owner: Platform   Target: 48 hours                   |          |             |
| V-03                                                 | HIGH     | In progress |
| Outdated VPN component with known exploit path       |          |             |
| Owner: IT   Target: 7 days                           |          |             |
| V-04                                                 | HIGH     | Open        |
| Privileged endpoint missing current EDR policy       |          |             |
| Owner: IT/SecOps   Target: 7 days                    |          |             |
| V-05                                                 | HIGH     | In progress |
| Cloud storage policy allows broad internal access    |          |             |
| Owner: Cloud   Target: 14 days                       |          |             |
| V-06                                                 | HIGH     | Open        |
| Legacy TLS endpoint remains externally reachable     |          |             |
| Owner: Infrastructure   Target: 14 days              |          |             |

PRIORITIZATION MODEL

Prioritize exploitability, internet exposure, asset importance, privilege required, available compensating controls, and business impact. Severity alone is not enough.

08 / REMEDIATION AGING

# Aging risk is an ownership and escalation problem

| AGE        | CRITICAL | HIGH | MEDIUM | LOW |
|------------|----------|------|--------|-----|
| 0-7 days   | 1        | 4    | 7      | 11  |
| 8-30 days  | 1        | 5    | 12     | 18  |
| 31-60 days | 0        | 4    | 16     | 21  |
| 61+ days   | 0        | 2    | 9      | 14  |

HIGH >30D

6

Escalate

REOPENED

3

Track separately

ACCEPTED RISK

5

Review dates

MTTR HIGH

24d

Illustrative

- Escalate high findings older than 30 days to the accountable manager.
- Require documented risk acceptance when remediation cannot meet target.
- Track reopened findings separately from new discovery.
- Measure time-to-remediate by severity and business owner, not only overall average.

# Core controls are strong but lifecycle gaps remain

| DOMAIN                    | SCORE                  | STATUS  |
|---------------------------|------------------------|---------|
| Privileged MFA            | <div><div></div></div> | Strong  |
| Workforce MFA             | <div><div></div></div> | Improve |
| EDR coverage              | <div><div></div></div> | Strong  |
| Privileged EDR policy     | <div><div></div></div> | Improve |
| Dormant-account review    | <div><div></div></div> | Improve |
| Service-account ownership | <div><div></div></div> | Gap     |

PRIORITY IDENTITY ACTION

Complete service-account ownership, privilege review, and dormant-account remediation. These gaps can undermine otherwise strong MFA coverage.

ENDPOINT ACTION

Close EDR policy exceptions on privileged systems first; track policy drift and sensor health separately from simple installation coverage.

## 10 / CLOUD POSTURE

# Misconfiguration risk is concentrated in access and logging

| DOMAIN             | RISK   | OBSERVATION                                     | OWNER          |
|--------------------|--------|-------------------------------------------------|----------------|
| IAM / privilege    | Medium | 3 broad roles need review                       | Cloud          |
| Public storage     | Medium | 2 approved exceptions; 1 needs expiry           | Cloud / Data   |
| Audit logging      | High   | One production account missing full data events | Cloud / SecOps |
| Network exposure   | Low    | No unrestricted management ports                | Infrastructure |
| Secrets management | Medium | Legacy app still uses long-lived secret         | Platform       |

**CLOUD PRIORITY**

Restore complete audit visibility before expanding cloud detection logic. Detections cannot be reliable when source telemetry is incomplete.

- Reduce broad roles and bind access to business function.
- Replace long-lived credentials with managed identities or short-lived tokens where possible.
- Review public-storage exceptions and expiry dates monthly.
- Continuously test that high-value cloud audit sources remain enabled.

11 / DETECTION ENGINEERING

# Coverage is broad, but several business-relevant use cases need work

| DOMAIN                    | SCORE                  | STATUS  |
|---------------------------|------------------------|---------|
| Identity compromise       | <div><div></div></div> | Strong  |
| Endpoint malware          | <div><div></div></div> | Strong  |
| Cloud privilege abuse     | <div><div></div></div> | Improve |
| Data exfiltration         | <div><div></div></div> | Gap     |
| Web application abuse     | <div><div></div></div> | Improve |
| Suspicious admin behavior | <div><div></div></div> | Good    |

HIGHEST-VALUE GAP

Data-exfiltration monitoring lacks consistent coverage across cloud storage, bulk export, and unusual transfer patterns.

ENGINEERING RULE

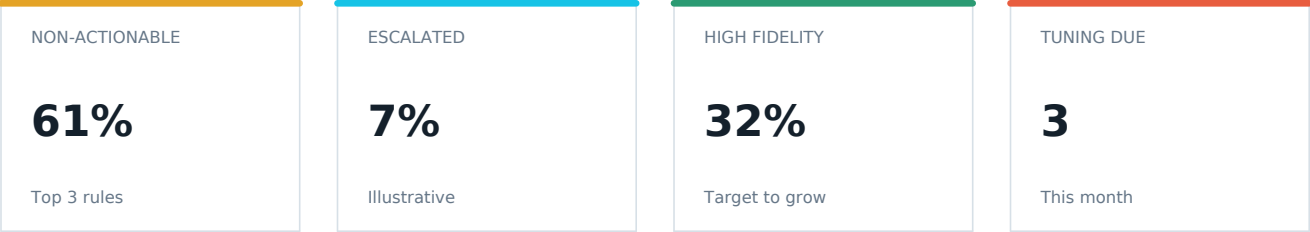
Tune and validate existing high-value detections before rapidly expanding rule count. Useful signal matters more than total detection volume.

- Map detections to priority attack scenarios and critical assets.
- Define required telemetry before declaring a use case covered.
- Test detections with controlled simulations and known-bad scenarios.
- Track detection owner, version, last validation date, and known blind spots.

12 / ALERT QUALITY

# Operational load is driven by a small number of noisy detections

| DETECTION          | SHARE | WHY NOISY                  | ACTION                             |
|--------------------|-------|----------------------------|------------------------------------|
| Impossible travel  | 28%   | Mostly VPN / mobile shifts | Tune with device + network context |
| Automation login   | 19%   | Known service workflows    | Use service-account context        |
| Cloud admin change | 14%   | Approved IaC deployments   | Enrich with deployment metadata    |
| Other detections   | 39%   | Mixed                      | Review individually                |



TUNING PRINCIPLE

Suppress only with documented rationale, bounded conditions, an owner, and a review date. Broad suppression can convert alert fatigue into silent control failure.

13 / SECURITY EVENTS

# Illustrative operational themes from the period

| EVENT THEME                                | STATUS        | OUTCOME / GAP                            | OWNER         |
|--------------------------------------------|---------------|------------------------------------------|---------------|
| Credential stuffing against customer login | Contained     | Rate limits and MFA reduced impact       | Product       |
| Suspicious privileged PowerShell           | Investigated  | Benign admin task; rule tuning required  | IT/SecOps     |
| Cloud access-key anomaly                   | Contained     | Key rotated; IAM review initiated        | Cloud         |
| Potential data-export spike                | Investigating | Telemetry incomplete on one storage path | Data / SecOps |

OPERATIONAL LESSON

Two events were contained quickly because identity and endpoint context were available in one investigation path.

VISIBILITY LESSON

The data-export investigation took longer because one storage source lacked complete audit telemetry. Logging gaps directly affect response quality.

## 14 / EXCEPTIONS &amp; RISK

# Temporary exceptions need expiry, ownership, and compensating controls

| ID    | RISK   | EXCEPTION / REASON                               | COMPENSATING CONTROL           |
|-------|--------|--------------------------------------------------|--------------------------------|
| EX-01 | High   | Legacy TLS service - Migration blocked by vendor | Network allowlist + monitoring |
| EX-02 | Medium | Broad cloud role - Automation refactor pending   | MFA + alerting + owner review  |
| EX-03 | Medium | Public storage share - External partner workflow | Signed URLs + expiry           |

- EX-01: review/expiry 30 Sep 2026
- EX-02: review/expiry 15 Oct 2026
- EX-03: review/expiry 20 Sep 2026

**RISK-ACCEPTANCE RULE**

Accepted risk is not closed risk. Record approver, rationale, compensating controls, review/expiry date, and trigger for re-evaluation.

15 / METRICS & TREND

# Use a small scorecard that supports decisions

| METRIC                      | PRIOR PERIOD | CURRENT | TREND     |
|-----------------------------|--------------|---------|-----------|
| Critical/high past SLA      | 9            | 6       | Improving |
| Internet-facing critical    | 3            | 2       | Improving |
| EDR coverage                | 96%          | 98%     | Improving |
| Priority detection coverage | 72%          | 78%     | Improving |
| Non-actionable alert share  | 68%          | 61%     | Improving |
| Open exceptions             | 4            | 5       | Watch     |

EXECUTIVE REPORTING RULE

Pair every metric with a direction, target, owner, and interpretation. A number without context is not a security decision.

16 / 30-DAY ACTION PLAN

# Prioritized actions for the next operating cycle

| PRIORITY | OWNER          | ACTION                                 | TARGET   |
|----------|----------------|----------------------------------------|----------|
| P1       | Infrastructure | Patch or isolate V-01                  | 48 hours |
| P1       | Platform       | Restrict public admin surface V-02     | 48 hours |
| P2       | IT/SecOps      | Close high findings older than 30 days | 2 weeks  |
| P2       | SecOps         | Tune top three noisy detections        | 2 weeks  |
| P2       | Cloud          | Restore complete audit telemetry       | 2 weeks  |
| P2       | SecOps/Data    | Increase data-exfiltration coverage    | 30 days  |
| P3       | Security Lead  | Run exception review with owners       | 30 days  |

MANAGEMENT CHECKPOINT

At the next monthly review, every P1/P2 item should have either verified completion evidence or an approved exception with compensating controls and a new review date.

17 / 90-DAY IMPROVEMENT

# Move from visibility to repeatable control validation

| WINDOW     | OUTCOME                         | KEY ACTIONS                                                                                                      | EVIDENCE                    |
|------------|---------------------------------|------------------------------------------------------------------------------------------------------------------|-----------------------------|
| 0-30 days  | Contain material exposure       | Close critical external findings, restore missing telemetry, tune noisy alerts, enforce exception review.        | Owner + ticket + validation |
| 31-60 days | Strengthen operating discipline | Formalize remediation SLAs, service-account ownership, detection validation, cloud access reviews.               | Owner + ticket + validation |
| 61-90 days | Measure control effectiveness   | Validate priority detections, test response workflows, review trend targets, retire stale exceptions and assets. | Owner + ticket + validation |

TARGET STATE

A mature monthly cycle should show verified telemetry coverage, risk-based vulnerability aging, tested priority detections, documented exceptions, and clear executive decisions.

18 / GOVERNANCE & ESCALATION

# A practical operating cadence

| CADENCE    | FORUM                   | PURPOSE                                                                               | OUTPUT                      |
|------------|-------------------------|---------------------------------------------------------------------------------------|-----------------------------|
| Weekly     | Security operations     | Critical exposure, incidents, high-risk backlog, urgent telemetry gaps                | Decision + owner + due date |
| Monthly    | Security posture review | Trends, exceptions, detection quality, ownership, next actions                        | Decision + owner + due date |
| Quarterly  | Leadership / steering   | Top risks, control effectiveness, investment decisions, recurring blockers            | Decision + owner + due date |
| On trigger | Critical escalation     | Material incident, exploitable public exposure, control failure, accepted-risk breach | Decision + owner + due date |

CLIENT RESPONSIBILITIES

Provide authorized access to agreed telemetry, maintain asset ownership, assign remediation owners, and approve risk decisions.

CYRAVEX RESPONSIBILITIES

Analyze agreed data, prioritize material risk, document recommendations, support detection/tuning work, and report within contracted scope.

# Severity, SLA, and evidence conventions

| SEVERITY | INTERPRETATION                                                | ACTION                          | NOTE              |
|----------|---------------------------------------------------------------|---------------------------------|-------------------|
| Critical | Active/exploitable material risk with severe impact potential | Immediate escalation            | Illustrative only |
| High     | Significant risk requiring prompt remediation                 | Named owner + short due date    | Illustrative only |
| Medium   | Meaningful weakness with limited conditions or impact         | Planned remediation             | Illustrative only |
| Low      | Hardening or limited-impact weakness                          | Backlog / risk-based scheduling | Illustrative only |

- Production severity should combine technical severity with asset criticality, exposure, exploitability, and control context.
- Evidence should reference source, timestamp, asset identity, and validation status.
- Accepted risk should remain visible until expiry or closure.
- Metrics in this sample are fictional and must never be represented as real client data.

## DATA HANDLING

Collect only necessary telemetry and evidence, apply least-privilege access, define retention, and avoid placing client secrets into unapproved public AI services.

## 20 / CONCLUSION

# Operational security improves when visibility becomes accountable action

The illustrative posture is not defined by the number of tools deployed. Sustainable improvement comes from controlling external exposure, remediating material risk on time, validating detections, maintaining useful telemetry, and escalating unresolved risk to accountable decision-makers.

**CYRAVEX SECURITY**

Managed Security support can combine vulnerability management, detection engineering, security operations support, and posture reporting within a clearly defined scope. It does not imply 24/7 SOC or MDR coverage unless separately operationalized and contracted.

**Discuss Managed Security Support | [cyravex.com](https://cyravex.com)**