



Out-of-the-Box Use Cases

An outline of use cases for Strike48's agentic security operations platform, including workflows across red team, blue team, compliance, vulnerability management, and automation.

Out-of-the-box use cases for agentic security operations

Strike48 gives security teams an agentic AI platform for executing cyber workflows out of the box. Instead of only detecting issues, Strike48 agents investigate, validate, respond, document, and improve security operations across red team, blue team, compliance, vulnerability management, and security automation use cases.

The platform reduces manual effort, lowers tooling and service costs, increases testing frequency, and improves security outcomes without requiring a full rebuild of the existing security stack.

1

Continuous Pen Testing and Red Teaming

THE PROBLEM

Traditional penetration testing is expensive, episodic, and often limited to annual or compliance-driven exercises. Organizations may receive a point-in-time report, but they rarely get continuous validation of how their environment stands up to actual attack paths.

STRIKE48 SOLUTION

Strike48 runs automated, AI-assisted penetration testing and red team execution through Pick, its offensive testing agent, and StrikeKit, its enterprise red teaming platform. Organizations run repeatable tests more frequently, across more assets, with greater visibility into findings, attack paths, and remediation priorities.

BUSINESS VALUE

Strike48 lets teams test more assets, more often, without adding budget or headcount. Teams that rely on periodic engagements gain continuous coverage between them. For holding companies or enterprises with multiple subsidiaries, Strike48 provides centralized control and visibility across distributed environments.

OUT-OF-THE-BOX OUTCOMES

- Run repeatable penetration tests across defined scopes.
- Validate attack paths and exploitability.
- Generate structured findings and remediation guidance.
- Support compliance-driven or continuous security testing programs.
- Provide a scalable alternative to one-off consulting engagements.

2

Vulnerability Exploitability Validation

THE PROBLEM

Most organizations already have vulnerability management tools, but those tools often stop at detection and prioritization. Security teams are left with long lists of vulnerabilities and limited clarity on which ones are actually exploitable in their environment.

STRIKE48 SOLUTION

Strike48 closes the gap between vulnerability detection and real-world validation. Agents assess whether vulnerabilities are exploitable, determine their impact, and prioritize remediation based on actual risk rather than theoretical severity alone.

BUSINESS VALUE

This lets security teams focus on the vulnerabilities that matter most, reduce alert fatigue, and improve remediation efficiency. It also strengthens the value of existing vulnerability management investments by adding an execution and validation layer.

OUT-OF-THE-BOX OUTCOMES

- Validate whether detected vulnerabilities are exploitable.
- Prioritize remediation based on demonstrated impact.
- Re-test after remediation to confirm closure.
- Connect vulnerability management with offensive testing.
- Support continuous validation as new vulnerabilities emerge.

3

AI-Assisted Incident Response

THE PROBLEM

Incident response is often slow, expensive, and heavily dependent on scarce human expertise. Many organizations rely on retained third-party IR services or manual internal workflows that are difficult to scale during high-pressure events.

STRIKE48 SOLUTION

Strike48 agents assist with incident triage, investigation, evidence gathering, recommended response actions, and post-incident documentation. The platform supports internal teams or is delivered as part of a managed service.

BUSINESS VALUE

Strike48 reduces response time and improves consistency during high-pressure events. It captures response logic in repeatable workflows rather than relying entirely on ad hoc human effort, so internal teams and managed service providers scale the same proven response.

OUT-OF-THE-BOX OUTCOMES

- Triage alerts and incidents.
- Gather supporting evidence across connected systems.
- Recommend response steps.
- Execute approved response workflows.
- Produce incident summaries, timelines, and documentation.
- Improve response consistency across teams.

4

Continuous Compliance and GRC Verification

THE PROBLEM

Compliance and GRC work is data-heavy, repetitive, and resource-intensive. Teams spend significant time collecting evidence, checking controls, documenting findings, and preparing for audits.

STRIKE48 SOLUTION

Strike48 agents automate or augment compliance verification by continuously checking controls, collecting evidence, identifying gaps, and producing structured outputs aligned to internal policies or external frameworks.

BUSINESS VALUE

Strike48 reduces manual administrative burden and improves audit readiness, moving organizations from periodic compliance checks to continuous control monitoring.

OUT-OF-THE-BOX OUTCOMES

- Continuously verify control alignment.
- Collect and organize compliance evidence.
- Identify control gaps or exceptions.
- Generate audit-ready summaries.
- Give GRC teams repeatable, AI-assisted workflows.
- Reduce manual review effort and analyst fatigue.

5

Agentic SOC and Blue Team Automation

THE PROBLEM

SOC teams are overwhelmed by alerts, noisy data sources, repetitive investigations, and fragmented tools. Traditional SOAR workflows can help, but they are often brittle, expensive, and limited to predefined playbooks.

STRIKE48 SOLUTION

Strike48 provides agents that investigate alerts, reason across context, execute workflows, and assist analysts with triage, enrichment, and response. Unlike static automation, Strike48 agents adapt to available context while operating within governed workflows.

BUSINESS VALUE

Security teams improve analyst productivity, reduce repetitive work, accelerate investigations, and modernize SOC operations without replacing the entire security stack.

OUT-OF-THE-BOX OUTCOMES

- Enrich and triage alerts.
- Investigate suspicious activity across tools.
- Recommend next-best actions.
- Execute approved response steps.
- Assist L1 and L2 analysts.
- Capture repeatable analyst workflows as agentic automations.

6

Purple Team Training and Continuous Security Improvement

THE PROBLEM

Red team and blue team activities are often disconnected. Offensive testing produces findings, but those lessons do not always translate into better detections, better response playbooks, or better analyst training.

STRIKE48 SOLUTION

Strike48 connects offensive and defensive workflows. Pick executes red team activity while blue team agents and human analysts detect, investigate, and respond. The output from each side improves the other.

BUSINESS VALUE

Organizations continuously test their security posture, train analysts, validate controls, and improve detections throughout the year instead of relying on isolated exercises.

OUT-OF-THE-BOX OUTCOMES

- Run controlled attack simulations.
- Train analysts against realistic scenarios.
- Validate whether existing tools detect simulated attacks.
- Improve detection logic and response workflows.
- Feed blue team learnings back into future red team testing.
- Build a continuous security improvement loop.

7

Smart Security Automation and AI Orchestration

THE PROBLEM

Most security automations are rigid. They break when systems change, lack context, and require ongoing maintenance. As environments become more complex, teams need automations that can reason over context, not just execute static rules.

STRIKE48 SOLUTION

Strike48 enables context-aware security automation. Agents monitor workflows, interpret data, identify failures, recommend fixes, and coordinate activity across integrated systems.

BUSINESS VALUE

This lets organizations modernize automation without being locked into brittle SOAR playbooks. Strike48 helps teams reduce manual intervention and automate more complex workflows reliably.

OUT-OF-THE-BOX OUTCOMES

- Build context-aware security workflows.
- Monitor integrations and workflow health.
- Detect automation failures.
- Recommend or execute corrective actions.
- Coordinate actions across security tools.
- Replace or augment legacy SOAR functionality.

8

SIEM, SOAR, and Security Data Cost Optimization

THE PROBLEM

Security teams are under pressure from rising SIEM and data ingestion costs. High-volume data sources can be too expensive to ingest fully, yet leaving them unmonitored creates security blind spots.

STRIKE48 SOLUTION

Strike48 agents query data at the source, analyze only the relevant subset, and bring back the context needed for investigation or response. This reduces the need to ingest every log into a SIEM while letting teams investigate high-value signals.

BUSINESS VALUE

Strike48 helps organizations reduce SIEM and SOAR spend and modernize their security architecture, all without losing visibility or ingesting data they do not need.

OUT-OF-THE-BOX OUTCOMES

- Query telemetry directly at the source.
- Reduce unnecessary SIEM ingestion.
- Investigate high-volume data without moving all logs.
- Support phased SIEM or SOAR cost reduction.
- Integrate with Splunk, Elastic, Cloudflare, and other existing systems.
- Preserve visibility while lowering data costs.

EXAMPLE — CLOUDFLARE LOG ANALYSIS AT SOURCE

Problem

Large Cloudflare environments can generate massive volumes of log data. Sending all of that data into a SIEM can be cost-prohibitive, but relying only on native controls may leave smaller endpoints or targeted attacks under-monitored.

Strike48 Solution

Strike48 integrates with Cloudflare and lets agents query specific endpoints, traffic patterns, or time windows directly. Instead of ingesting all Cloudflare data, Strike48 analyzes targeted subsets when needed.

Business Value

This gives organizations better visibility into high-scale environments while avoiding the cost of full log ingestion.

OUTCOMES

- Analyze targeted Cloudflare telemetry.
- Detect endpoint-specific anomalies.
- Investigate suspected attacks without full SIEM ingestion.
- Reduce noise and cost.
- Strengthen monitoring across large-scale web environments.

9

Standards-Based Security Validation and Reporting

THE PROBLEM

Organizations know they need to align with security standards such as OWASP, MITRE ATT&CK, CIS Benchmarks, or NIST CSF, but validating that alignment is usually manual and point-in-time, and hard to keep consistent from one review to the next. Teams may run periodic assessments, but they rarely have a continuous way to determine whether a specific application, machine, endpoint, API, or environment is protected against the risks those standards describe. And even when findings exist, they are often reported in technical terms that do not map cleanly to the frameworks executives, auditors, and risk teams care about.

STRIKE48 SOLUTION

Strike48 turns recognized standards into executable security assessments. Instead of treating a framework as a static checklist, agents inspect configuration, query logs, test behavior, validate controls, and produce evidence-backed findings mapped directly to the standard. Strike48 then maps those findings to the frameworks each audience uses, such as OWASP, MITRE ATT&CK, CIS Benchmarks, NIST CSF, or a customer-specific control library, so the same assessment serves engineers, security leaders, and compliance teams from a single run.

BUSINESS VALUE

This gives customers a fast, repeatable way to understand their posture against standards their teams, auditors, and executives already recognize. It also creates a clear bridge between technical findings and business-level risk reporting, so security work becomes measurable progress against the standards that govern the program.

OUT-OF-THE-BOX OUTCOMES

- Assess machines, applications, APIs, or environments against recognized security standards.
- Produce framework-mapped findings and gap analysis, showing which risks are present, mitigated, or require further validation.
- Generate technical, executive, and compliance-ready views of the same assessment.
- Track posture improvement over time by re-running assessments.
- Give auditors and boards evidence-backed posture reports.
- Convert one-time manual assessments into repeatable agentic workflows.

EXAMPLE — OWASP TOP 10 ASSESSMENT

Strike48 assesses a target machine, application, or exposed service against the OWASP Top 10 and produces a report showing which categories are relevant, which appear mitigated, and where the environment has measurable exposure that needs further testing. Customers see their exposure to widely recognized web application risks and prioritize remediation based on evidence rather than assumptions.

Security Operations at Machine Speed

Strike48 helps organizations move from static, human-heavy security operations to continuous, agentic cyber execution. The platform reduces costs, increases testing frequency, improves incident response, automates compliance, modernizes the SOC, and queries security data at the source.

Instead of replacing the existing security stack, Strike48 makes that stack more intelligent and more cost-effective to run.

Request a Demo →

Or visit strike48.com/request-demo