STRIKEREADY

USE CASES

STRIKEREADY USE CASES AT A GLANCE
POWERFUL SOLUTIONS TAILORED TO YOUR CYBERSECURITY CHALLENGES

Challenges in Cybersecurity

Fragmented tech stacks, siloed systems, and limited cross-platform integration hinder operational efficiency and increase costs. Manual workflows are error-prone, time-consuming, and labor-intensive, creating bottlenecks and blind spots. Security teams face resourcing challenges due to a scarcity of skilled professionals and high operational costs, further exacerbated by the ever-evolving threat landscape. Gaps in visibility, ineffective risk prioritization, and overwhelming intelligence sources leave organizations vulnerable to emerging threats, complicating decision making and mitigation efforts.

The StrikeReady Solution

StrikeReady modernize the cybersecurity operations by centralizing workflows within an AI-powered Security Command Center that seamlessly integrates with existing tools and automates critical processes. The platform enables SOC teams to streamline threat detection, response, and mitigation in real-time, reducing alert fatigue and optimizing efficiency. With features like enriched threat intelligence, simplified patch management, and actionable insights from the dark web, StrikeReady helps organizations stay ahead of threats while maximizing resource utilization. Its tailored solutions empower security teams to proactively defend against evolving challenges.

Here are some of the key use cases that the StrikeReady platform addresses, helping organizations streamline security operations, enhance collaboration, and accelerate threat response

CASE 1: OPERATIONALIZING THREAT INTELLIGENCE AT MACHINE SPEED

Problem Statement:

Threat Intelligence is invaluable but difficult to operationalize effectively and efficiently. The average time required to validate and act on a Threat Intelligence Report (TIR) is 4-6 hours, leading to resource drain and delayed responses. Manual processes are cumbersome, requiring security teams to repeatedly perform investigation, mitigation, and countermeasure deployment tasks, which are costly in terms of time, manpower, and money. Organizations remain vulnerable due to inefficiencies in transforming intelligence into action.

Solution Statement:

With StrikeReady, the time to validate, enrich, correlate, understand impact, and deploy fixes is reduced from 4-6 hours to just 4-6 minutes. This enables security teams to operationalize more intelligence and focus on high priority projects. By leveraging AI-powered automation, premium tools, and lightning-fast workflows, StrikeReady empowers security operations, enhancing efficiency while eliminating resource constraints. The platform delivers near real-time visibility, reduces Mean Time to Resolution (MTTR), and strengthens overall security posture.

CASE 2: AUTOMATED WORKFLOWS "OUT OF THE BOX"

Problem Statement:

Traditional SOAR (Security Orchestration, Automation, and Response) solutions come with excessive costs, complex implementation, and high failure rates. Organizations often spend $250K–$750K on licensing, $500K–$1MM+ annually on playbook development, and $330K+ on maintenance. Even after investing these resources, implementation can take 12–18 months before ROI is realized. The reliance on consultants, DevOps teams, and security professionals adds further complexity, making traditional SOAR solutions resource-intensive and prone to failure.

Solution Statement:

StrikeReady eliminates the complexities and costs of traditional SOAR solutions with automated workflows that require zero coding, zero playbooks, and zero maintenance. Deployable in just 60 minutes without professional services, StrikeReady delivers immediate value by automating security processes, reducing manual workloads, and cutting response times from hours to seconds. Organizations benefit from 90%+ process time savings, enhanced security posture, and seamless technology integration—all without the typical expenses and delays of legacy automation platforms.

CASE 3: PHISHING ALERT AUTOMATION

Problem Statement:

Organizations struggle to manage phishing alerts due to high alert volumes, inefficient manual triage, and prolonged resolution times. DIY automation attempts often fail due to lack of expertise and scalability, leading to delays, alert fatigue, and analyst burnout. On average, each phishing alert takes 30 minutes to an hour to triage, and true-positive alerts consume hours to days, making security teams less efficient in handling critical threats.

Solution Statement:

StrikeReady automates phishing alert triage, enrichment, and resolution, reducing manual workload and improving efficiency. Each alert is automatically triaged within 1 minute, enabling security teams to focus on true-positive alerts rather than wasting time on false positives.

AI-powered enrichment ensures faster, more accurate threat analysis, significantly lowering Mean Time to Resolution (MTTR) from hours to minutes. This automation improves operational efficiency, reduces costs, and enhances security teams' productivity by providing the equivalent of 2.5 full-time analysts through AI augmentation.

CASE 4: REDUCING ALERT FATIGUE WITH SOC EFFICACY

Problem Statement:

SOC teams are overwhelmed with alert overload, leading to operational inefficiencies, analyst burnout, and increased business risk. High volumes of false positives require as much effort as genuine threats, draining resources and slowing down incident response. Traditional threat-hunting processes are time-consuming, often taking up to six hours, delaying crucial security actions. The excessive workload not only reduces operational effectiveness but also increases the risk of human error, dissatisfaction, and high turnover rates among analysts.

Solution Statement:

StrikeReady transforms SOC operations with AI-driven automation, optimizing alert investigations and streamlining threat hunting. By integrating intelligent workflows, only true-positive alerts are fully enriched and actioned, reducing noise and improving accuracy. Security teams achieve over 90% process time savings with machine-speed alert triage and enrichment. Analysts benefit from advanced SOC tools and automation, drastically reducing their workload while enhancing productivity and job satisfaction. With real-time visibility and actionable insights, organizations can lower their Mean Time to Resolution (MTTR) from hours to seconds, improving security posture and overall efficiency.

CASE 5: DARK WEB RISK VISIBILITY & MITIGATION

Problem Statement:

Organizations struggle to detect and respond to critical risks originating from the dark web, leading to blind spots in risk identification and mitigation. Sensitive data exposure, such as leaked credentials, remains largely untracked, making businesses vulnerable to unauthorized access. Threat actors actively advertise stolen data and compromised access credentials, further increasing exposure risks. Many security teams rely on ad-hoc monitoring approaches, leading to delayed responses, operational inefficiencies, and over-reliance on resource-intensive manual processes.

Solution Statement:

StrikeReady enhances risk visibility and mitigation with AI-powered workflows that provide deep insights into dark web threats while streamlining remediation. Its Credential Monitoring capability tracks leaked credentials in real time, issuing actionable alerts for internal and external exposures. Threat Actor Insights empower security teams to detect and analyze dark web activity involving their organization, proactively addressing potential breaches. Continuous Dark Web Monitoring automates intelligence gathering, eliminating reliance on manual processes and providing seamless, ongoing threat visibility. With StrikeReady, organizations achieve 95% faster risk mitigation, drastically reduce operational inefficiencies, and safeguard critical assets against emerging cyber threats.

CASE 6: SECURITY CONTROL VALIDATION (SCV)

Problem Statement:

Organizations struggle to answer a fundamental question—"Are we vulnerable?"—with clarity and speed. Manual testing processes are time-consuming, often taking hours or even days, delaying crucial security insights and decision-making. Traditional security tools lack adaptability, making it difficult to keep up with evolving threats, and misconfigured defenses create gaps that leave organizations exposed. Without a fast and reliable way to validate security controls, businesses risk being unprepared for emerging attacks, leading to potential breaches, operational disruptions, and financial losses.

Solution Statement:

StrikeReady's AI-driven Security Control Validation (SCV) delivers instant security validation with automation, providing clear, actionable insights in minutes instead of days. The platform ensures continuous adaptation to emerging threats, validating security configurations and eliminating misconfigurations that could leave vulnerabilities unchecked. By automating security validation, StrikeReady reduces Mean Time to Resolution (MTTR) by 96%, enhances red team capabilities, and removes the need for costly Breach and Attack Simulation (BAS) tools, saving organizations $100K–$300K annually. StrikeReady's pre-built threat simulations, automated testing, and real-time monitoring enable security teams to proactively defend their environments with confidence, ensuring faster insights, stronger defenses, and complete security posture validation.

CASE 7: VULNERABILITY MANAGEMENT UNIFIED

Problem Statement:

Organizations struggle with fragmented vulnerability management due to disconnected network, endpoint, and cloud scanners, leading to inefficient tracking and prioritization of patches. Compatibility issues disable security modules, creating blind spots that increase risk exposure. The lack of centralized visibility and automation results in delayed remediation, making it easier for vulnerabilities to be missed or exploited.

Solution Statement:

StrikeReady provides a centralized dashboard that consolidates data from all vulnerability tools, offering a single-pane view for comprehensive risk assessment. Automation at scale correlates vulnerabilities with software versions and prioritizes remediation efforts. Integrated patch management tracks progress, ensuring compliance and accountability. With real-time alerts, security teams can swiftly detect, prioritize, and mitigate threats, significantly reducing breach risks and improving security posture.

CASE 8: INVESTIGATION PLATFORM – EMPOWERING ANALYSTS, ENHANCING INSIGHTS

Problem Statement:

Security analysts face significant challenges when investigating alerts due to fragmented data sources, manual processes, and increasing fatigue. Analysts must constantly switch between IT systems, business platforms, and threat intelligence sources to gather relevant context, leading to inefficiencies and delays. The repetitive nature of manual correlation and low-priority alerts contributes to high analyst burnout, making it difficult to focus on real threats.

Additionally, manual data collection slows down response times, increasing the risk of missed true positives and delayed incident resolution.

Solution Statement:

The StrikeReady Investigation Platform revolutionizes alert handling by automating data retrieval, enrichment, and correlation to streamline investigations. It consolidates data from multiple tools into a single interface, eliminating tab overload and reducing manual toggling. Analysts can seamlessly switch between IT, business, and threat intelligence sources, enhancing decision-making efficiency. The platform leverages automation to accelerate investigations, ensuring relevant insights are surfaced instantly, reducing analyst fatigue while improving accuracy and response speed. By integrating AI-driven workflows, StrikeReady empowers analysts to detect, analyze, and respond to threats with unprecedented efficiency.

CASE 9: CASE MANAGEMENT AND COLLABORATION

Problem Statement:

Security teams struggle with fragmented workflows, where alerts, documentation, and actions are scattered across multiple systems, leading to inefficiencies and delays. Poor communication tools hinder collaboration, escalating resolution times and reducing response effectiveness. Manual documentation of incident investigations is time-consuming and prone to errors, impacting compliance and transparency. Additionally, teams lack structured insights from past incidents, preventing them from improving future responses. These inefficiencies prolong threat resolution and expose organizations to security risks and compliance failures.

Solution Statement:

StrikeReady transforms incident case management by consolidating alerts into unified case views, eliminating fragmented investigations. The platform enables seamless collaboration by integrating communication tools like Slack, text, and email, allowing analysts to comment, share files, delegate tasks, and escalate cases effortlessly. Analysts can take proactive actions, such as blocking domains or quarantining systems, directly within the platform, while real-time updates are synced across extenal ticketing and management systems. StrikeReady also automates timeline documentation, ensuring complete transparency and compliance with audit-ready records. Actionable post-incident insights help teams refine workflows and improve future responses, ultimately reducing Mean Time to Resolution (MTTR) and enhancing overall security posture.

Ready to Modernize and Automate Your SOC?

Schedule a Demo Today at

info@strikeready.com or visit
www.strikeready.com

Learn More

Schedule Demo