CROWDSTRIKE

White Paper

The Essential SOAR Playbook: Practical Use Cases for Modern Security Teams

Table of Contents

Executive Summary

Security teams are drowning in alerts, complexity, and manual processes that can't keep pace with modern threats. Security orchestration, automation, and response (SOAR) has become a critical capability to help teams scale their response, reduce fatigue, and eliminate inefficiencies. This white paper explores how CrowdStrike Falcon® Fusion SOAR — the backbone of Charlotte Agentic SOAR and natively built into the CrowdStrike Falcon® platform — helps security teams automate repetitive tasks, accelerate investigations with agentic capabilities, and reduce time to respond across the entire incident life cycle.

Speed:

Reduce response times from hours to minutes through automated workflows and AI-assisted investigation and response

Consistency:

Ensure standardized response procedures through repeatable playbooks and unified platform integration

Scale:

Enable teams to handle increasing alert volumes without proportional staffing increases by automating routine tasks

Agentic:

Empower every analyst with AI agents and adaptive, agentic workflows that orchestrate them together

The white paper demonstrates these benefits through five real-world use cases that highlight the power of Falcon Fusion SOAR:

- Automated malware triage and containment
- Compromised account remediation
- Exposure management
- Phishing response orchestration
- AI-powered indicator of compromise (IOC) investigations

Each use case illustrates how Falcon Fusion SOAR's native platform integration, combined with advanced AI capabilities and access to rich telemetry, enables security teams to build sophisticated response workflows without complex coding or fragile integrations. The result is a more responsive, resilient, and efficient security operation that can meet today's threat challenges at machine speed.

From Overwhelmed to Empowered: The Critical Role of SOAR in Modern Security

Security operations centers (SOCs) are under intense pressure to keep pace with the growing scale and complexity of cyber threats. Analysts face a relentless wave of alerts, and security teams struggle with talent shortages and rising expectations to respond faster, reduce risk, and show measurable outcomes. Traditional tools often operate in isolation, requiring manual handoffs and human stitching to coordinate response — and slowing everything down. This is where SOAR becomes essential, offering the automation and orchestration needed to streamline and scale operations.

By connecting and automating actions across the SOC — from threat intelligence and IT service management (ITSM) to cloud, identity, and email security — SOAR platforms reduce manual overhead and drive consistent, measurable response. When SOAR is natively integrated into a unified security platform and leverages AI-powered capabilities, its power multiplies: Playbooks can act on trusted telemetry, identity context, and threat intelligence in real time without relying on external APIs or fragile connectors. The result is a faster, smarter, and more resilient SOC where detection and response work in concert as a continuous, orchestrated loop.

A native capability of the Falcon platform, Falcon Fusion SOAR delivers security orchestration and automation without the complexity of traditional solutions. Security teams can harness the platform's industry-leading threat intelligence, real-time telemetry, and rich identity context to transform manual security workflows into powerful automated responses. This native integration enables SOC teams to build and deploy sophisticated response workflows at the speed of threats while maintaining the simplicity of a unified platform. With Falcon Fusion SOAR, detection flows naturally into workflow automation, and every action is backed by the full power of the Falcon platform.

But Falcon Fusion SOAR goes further. It's the orchestration backbone of Charlotte Agentic SOAR — where automation meets intelligence. It integrates with CrowdStrike® Charlotte AI™ and Charlotte AI AgentWorks, uniting reasoning, adaptability, and action within the Falcon platform for advanced agentic use cases. Together, powered by CrowdStrike Enterprise Graph®, they deliver intelligence, context, and automation in one unified platform — creating a faster, smarter SOC ready to outpace any threat.

Figure 1. Falcon Next-Gen SIEM unifies detection, investigation, and native SOAR capabilities in one AI-native platform.

Transforming Security Operations: The Power of AI-Driven SOAR

Think It. Type It. Automate It: The Fast Track to Smart Workflow Automation

Advanced SOAR platforms, like Falcon Fusion SOAR, eliminate the need for deep scripting expertise by offering an intuitive, no-code automation engine. Analysts can quickly build, modify, and deploy workflows using a drag-and-drop interface or through natural language prompts, thanks to an integrated natural language processing (NLP) agent. The Workflow Generation Agent interprets human-readable instructions — such as "investigate failed logins and notify the user's manager" — and translates them into structured automation steps, dramatically lowering the barrier to entry. This combination of visual and language-driven design empowers analysts of all skill levels to contribute to automation development, accelerating time-to-value and fostering collaboration across the SOC.

SOAR playbooks define response logic through configurable triggers, conditions, and actions, automating everything from data enrichment to user containment and threat eradication. Whether it's accelerating phishing triage or automating ransomware response, the automation engine ensures repeatable processes, reduces human error, and enables rapid scaling across the SOC.

Agentic workflows take this one step further. By embedding AI decision-making, memory, and adaptability into automated playbooks, security teams can build agent-like automations that operate autonomously within defined guardrails. These agentic workflows can assess evolving conditions, adjust their behavior in real time, and escalate or suppress actions based on contextual analysis, such as the severity of a threat, the identity of an impacted user, or the presence of similar incidents in the past. This approach reduces the burden on analysts while enabling more intelligent, situation-aware responses at machine speed.

From Siloed Tools to Seamless Action: Orchestrate Across the Stack with One Platform

A SOAR platform is only as powerful as the ecosystem it can orchestrate. The real value of automation comes from the ability to unify your entire security and IT stack, enabling tools to work in concert rather than in silos. With deep, out-of-the-box integrations across product categories and security domains, advanced SOAR solutions make it easy to build workflows that span your existing infrastructure.

As a native capability of the Falcon platform, Falcon Fusion SOAR seamlessly integrates with CrowdStrike Falcon® Next-Gen SIEM and across CrowdStrike modules. It additionally offers more than 2,500 third-party actions readily available through the unified content library. By connecting workflows across threat intelligence, cloud platforms, firewalls, ITSM systems, identity providers, and more, SOAR platforms empower teams to automate complex, multi-step response actions that would otherwise require manual intervention across disparate tools.

These integrations allow playbooks to orchestrate cross-functional tasks, such as gathering telemetry from endpoint detection and response (EDR), opening a ticket in a service desk tool, updating a firewall rule, or sending notifications via collaboration platforms. This seamless toolchain interoperability reduces silos and empowers SOCs to act decisively and holistically.

Figure 2. Tap into a rich ecosystem of integrations, across security and IT, that extend and enhance investigation and response.

Investigate, Collaborate, and Close: Dynamic Case Management Built for Speed

Modern security operations demand more than ticketing and documentation — they require smart, adaptive systems that can keep up with the volume and complexity of today's threats. Seamlessly integrated case management brings intelligence and automation to every phase of incident response, transforming how SOCs manage, investigate, and resolve threats. By serving as a central hub for managing investigations, documenting actions taken, and enabling team collaboration, case management helps optimize your SOC and improve operational maturity.

Rather than manually stitching together related alerts or combing through raw data, analysts can rely on AI to create incident visualizations, auto-correlate events, enrich cases with contextual intelligence, and recommend next steps based on historical responses and threat models. Built-in natural language summarization — powered by AI — distills multi-source evidence into concise incident narratives, reducing cognitive load, improving handoffs between shifts or teams, and streamlining compliance and post-incident reviews. Falcon Fusion SOAR's native integration with case management, combined with the advanced capabilities of CrowdStrike Charlotte AI, automates these complex workflows while providing intelligent decision support and adaptive response recommendations, significantly accelerating incident resolution times.

Falcon Fusion SOAR also streamlines collaboration through shared timelines, automated evidence collection, and context-rich notifications. Meanwhile, dashboards and metrics surface trends in alert fatigue, playbook effectiveness, and team performance, giving SOC leaders the insights they need to continuously refine operations.

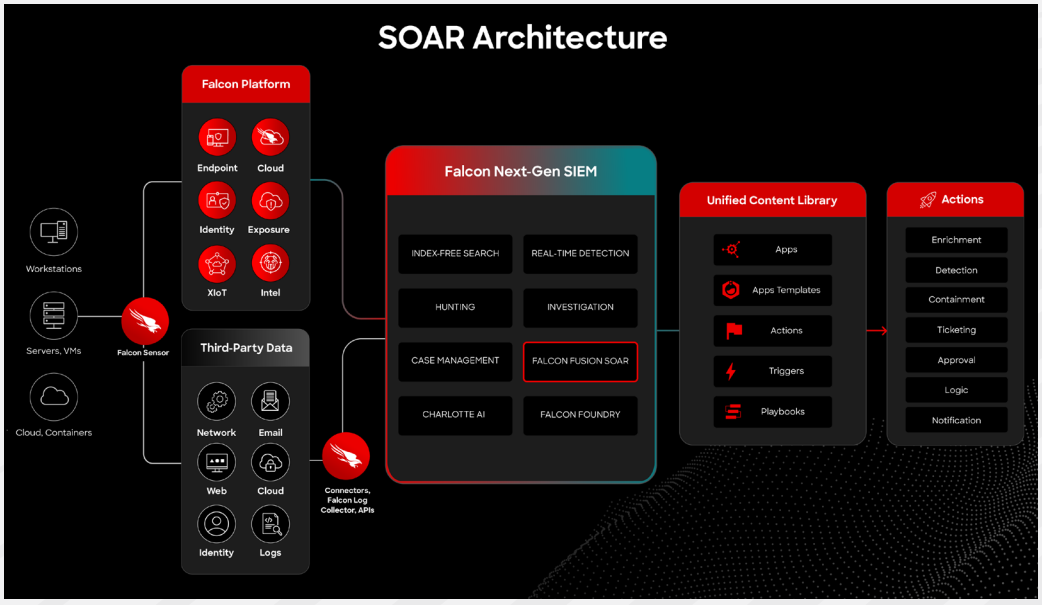

Figure 3. Falcon Fusion SOAR brings together Falcon-native data, third-party tools, and a powerful content and workflow library in one unified platform.

From Theory to Practice: Five Essential SOAR Use Cases for the Modern SOC

1. Automating Malware Triage and Response with Falcon Fusion SOAR

In the face of advanced malware threats and the rapid pace of modern attack campaigns, security teams are overwhelmed by high volumes of alerts, many of which require timely investigation to reduce adversary dwell time. While EDR solutions offer rich telemetry and visibility into malware-related activity, the manual correlation of indicators, cross-tool analysis, and response execution can be both time-consuming and error-prone.

Falcon Fusion SOAR transforms this fragmented process into a unified, automated workflow, reducing investigation time, improving consistency, and enabling scalable incident response.

Trigger: Action from Machine Learning Detections

The malware triage playbook in Falcon Fusion SOAR is automatically triggered when a high-severity detection is received — especially one flagged by machine learning-based models in the Falcon platform. This trigger acts as the catalyst for a structured response pipeline, enabling the SOAR platform to instantly spring into action without requiring manual intervention.

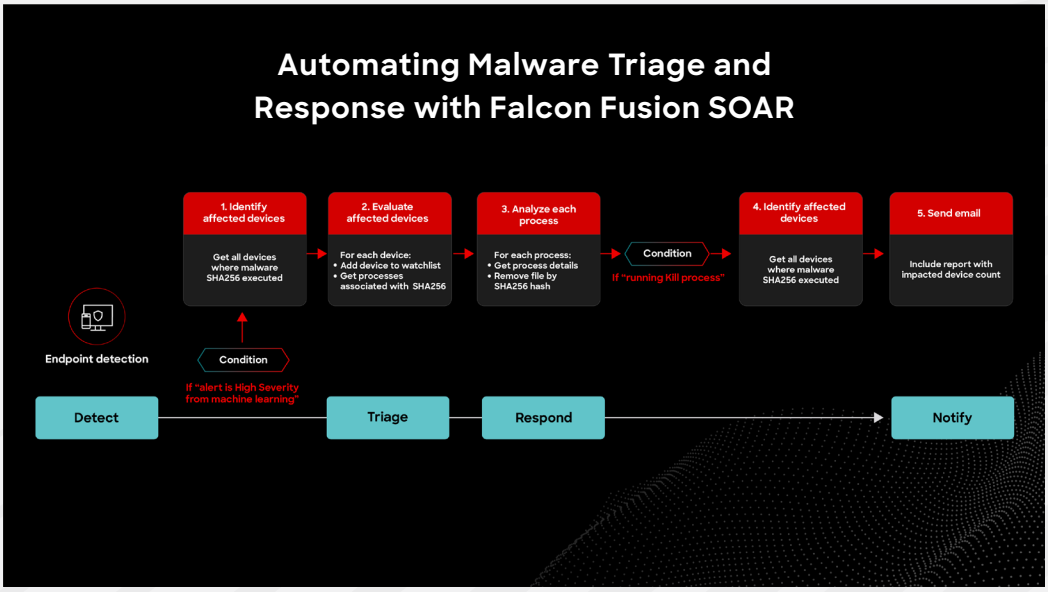

Figure 4. Malware triage kicks off automatically when high-severity detections are triggered in the Falcon platform, initiating an immediate SOAR response.

Step 1: Identifying Affected Devices

Once a malicious file (identified by its SHA256 hash) is flagged, Falcon Fusion SOAR initiates a query to enumerate all devices across the environment where the file has executed. This broad search ensures visibility into the scope of impact and creates a foundation for a comprehensive response.

Step 2: Per-Device Remediation Logic

For each device identified, Falcon Fusion SOAR executes a repeatable sequence of actions:

- Add the device to a watchlist to monitor for further suspicious behavior or reinfection attempts
- Retrieve all processes associated with the known malware hash for in-depth investigation

This per-device logic ensures tailored remediation while maintaining scalability across multiple endpoints.

Steps 3 and 4: Process-Level Containment and Cleanup

Each process tied to the malicious SHA256 hash is inspected in detail. If the process is still running:

- Falcon Fusion SOAR kills the active process, immediately halting malicious activity
- The system then removes the malware file from disk, ensuring no opportunity for reinfection

This step reflects Falcon Fusion SOAR's strength in precise surgical response, leveraging real-time endpoint telemetry and action APIs.

Step 5: Analyst Notification and Reporting

Upon completion of the remediation steps, Falcon Fusion SOAR automatically generates a summary report detailing:

- The number of impacted devices
- Remediation actions taken per host
- IOCs observed

This report is sent via automated email to designated stakeholders, ensuring transparency and documentation without additional manual effort.

Outcome: Reduced Dwell Time and Analyst Burden

The Falcon platform leverages real-time endpoint data, and Falcon Fusion SOAR's malware workflow enables rapid containment, surgical remediation, and full-loop automation. The analyst remains in the loop only when needed — such as for escalation decisions or long-tail investigation — while the platform handles high-confidence automation with speed and precision.

This approach can help reduce response times from hours to minutes and empower security teams to scale their operations without increasing headcount, especially in the face of increasingly sophisticated malware campaigns.

2. Automating Compromised Account Remediation with Falcon Fusion SOAR

As organizations face an increasing wave of credential-based attacks — fueled by password reuse, phishing campaigns, and leaked credentials on the dark web — security teams must act swiftly to detect and remediate compromised accounts before adversaries exploit them further. Manual workflows often lag behind the pace of these threats, leaving gaps in response coverage and increasing the likelihood of account misuse or lateral movement.

Falcon Fusion SOAR enables automated, scheduled detection and mitigation of compromised credentials using real-time identity signals from CrowdStrike Falcon® Identity Threat Protection, ensuring continuous defense and minimal operational overhead.

Trigger: Scheduled Daily Scan for Weak or Compromised Passwords

The compromised account workflow is triggered automatically on a daily schedule, leveraging Falcon Identity Threat Protection to query for human user accounts exhibiting specific identity risk factors, such as:

- WEAK_PASSWORD (including matches in breach corpuses)
- Credentials found in compromised password databases
- Accounts flagged due to risk-based heuristics

This proactive schedule eliminates the need for manual review or third-party feed ingestion while ensuring that identity hygiene checks are run at regular intervals.

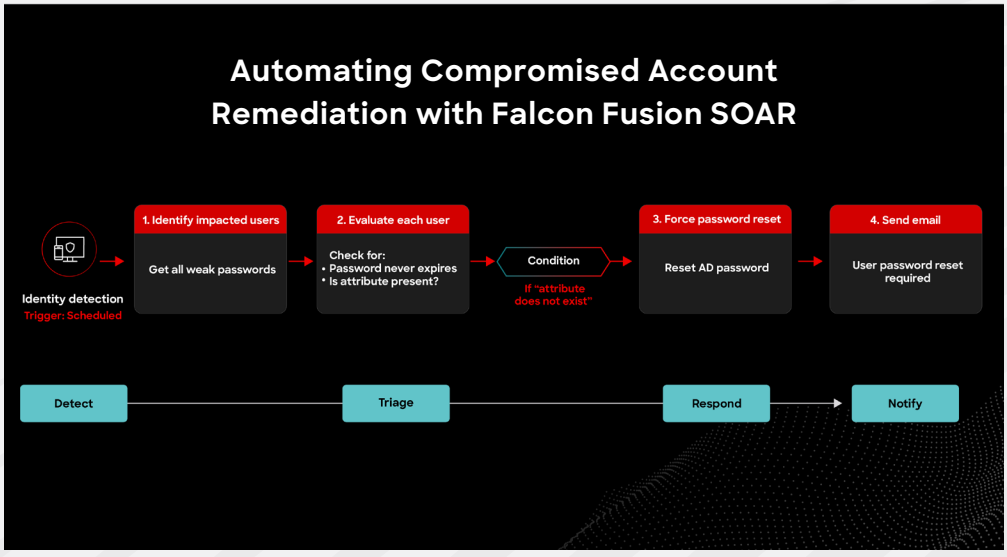

Figure 5. Falcon Fusion SOAR can perform a daily automated scan for compromised credentials, powered by real-time identity risk insights from Falcon Identity Threat Protection.

Step 1: Identify At-Risk Users

The workflow begins by querying all users who meet the predefined criteria (e.g., weak or leaked passwords). This step isolates compromised or vulnerable accounts that require immediate remediation, establishing the initial scope for downstream automation.

Step 2: Concurrent Remediation for Each User

For every user identified:

- User context is enriched, retrieving detailed identity attributes, including domain, privileges, and account properties
- The workflow checks whether the user has the "Password Never Expires" flag set; if this exemption is not present, the workflow proceeds to remediate

This check ensures that privileged or service accounts are treated cautiously while enabling full remediation for standard users.

Step 3: Reset Passwords via Active Directory

Once validated, Falcon Fusion SOAR triggers a password reset request for the user's Active Directory account. The reset ensures that credentials linked to breach data are rendered useless, effectively cutting off adversary access.

This step is executed concurrently across all affected users, minimizing time to remediation without overloading IT or identity and access management (IAM) teams.

Step 4: Notify Users Automatically

If a user has a valid email address on file, Falcon Fusion SOAR sends a customized email notification, explaining the security finding and instructing them on the next steps:

- The email informs the user that their password was found in a breach
- The notification guides them to change their password at the next login
- The email's tone is informative and proactive, helping maintain trust while enforcing security policies

This automatic notification closes the loop without requiring help desk intervention, ensuring transparency and awareness.

Outcome: Zero-Touch Identity Hygiene at Scale

This Falcon Fusion SOAR workflow provides a zero-touch remediation loop for compromised accounts, combining detection, validation, and response in a seamless sequence. By automating password resets and user communications, the workflow dramatically reduces the window of opportunity for credential abuse while eliminating manual overhead for security and IT teams.

Security teams can schedule this playbook to run daily or on demand, ensuring that identity protection is a continuous process, not a reactive task. In the broader SOAR ecosystem, this capability complements phishing, multifactor authentication (MFA) abuse, and lateral movement detection use cases, giving analysts a powerful toolkit to combat account compromise across the enterprise.

3. Automating Exposure Management with Falcon Fusion SOAR

Modern enterprises face mounting pressure to maintain secure, up-to-date software across thousands of devices. Yet tracking application usage and remediating outdated or vulnerable versions remains a challenge for security and IT teams alike. Gaps in visibility or manual handoffs can leave exposures unaddressed — until attackers exploit them.

In conjunction with CrowdStrike Falcon® Exposure Management, Falcon Fusion SOAR empowers security teams to detect outdated applications in real time, automate remediation workflows through ITSM systems like ServiceNow, and open a parallel investigation path for the SOC through Falcon Next-Gen SIEM.

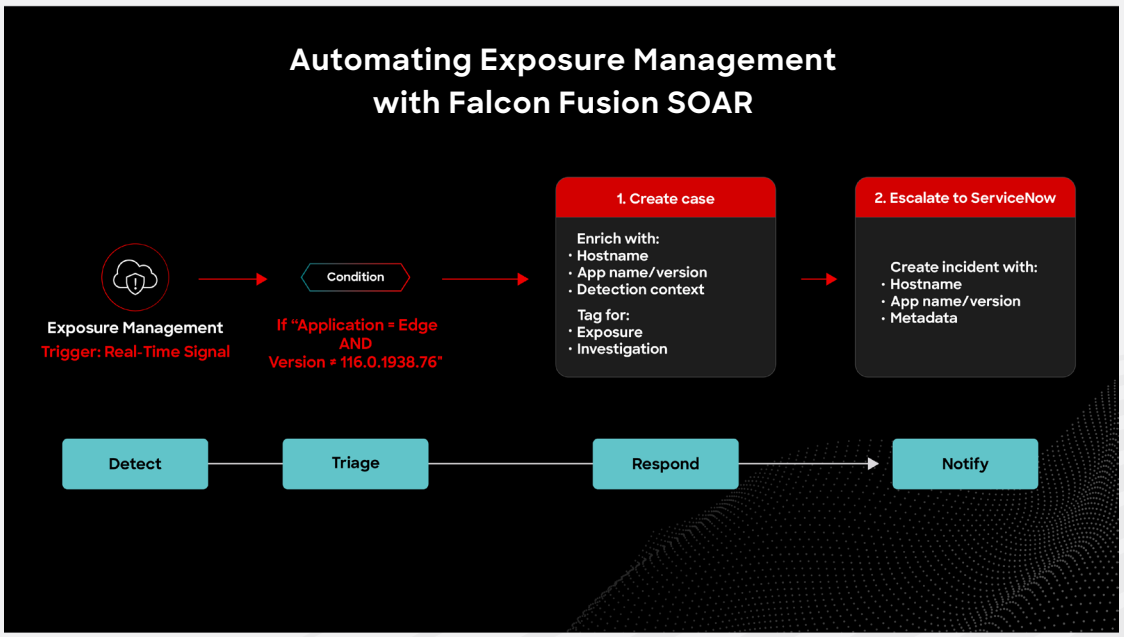

Figure 6. Falcon Fusion SOAR and Falcon Exposure Management work together to identify outdated apps in real time and automate investigation and remediation with ITSM platforms.

Trigger: Real-Time Application Usage Signal

This exposure management workflow is initiated by a live signal from Falcon Exposure Management, which continuously monitors application activity across endpoints. In this case, it specifically looks for the use of Microsoft Edge running any version other than 116.0.1938.76, the approved secure baseline.

This immediate detection ensures no delay between exposure identification and response orchestration.

Step 1: Evaluate Exposure Condition

Falcon Fusion SOAR evaluates the following criteria:

- Application name is `Edge`
- Application version is not `116.0.1938.76`

This condition targets known vulnerable or noncompliant instances, triggering downstream automation only when there's meaningful risk to help minimize alert fatigue and false positives.

Step 2: Create a ServiceNow Incident for IT Remediation

Upon a match, Falcon Fusion SOAR:

- Creates a ServiceNow ticket that is pre-populated with application name, version, hostname, and metadata
- Assigns the incident to the relevant IT remediation group
- Categorizes the case under "software" for clear triage and reporting

This seamless integration helps ensure that the IT team can rapidly and consistently address outdated application usage.

Step 3: Create a Case in Falcon Next-Gen SIEM for SOC Visibility

Simultaneously, Falcon Fusion SOAR creates a case in Falcon Next-Gen SIEM to:

- Enable SOC analysts to track exposure-related trends across the environment
- Associate this case with any correlated detections or risky behaviors
- Enrich the case with metadata such as host details, application version, and identity context

This step ensures exposures are not treated as isolated hygiene issues but as potential precursors to compromise, empowering analysts to investigate broader attack paths or misconfigurations contributing to the issue.

Outcome: End-to-End Exposure Response and Cross-Team Coordination

This enhanced workflow unifies exposure detection, IT remediation, and SOC investigation into a single automated loop:

- Falcon Exposure Management detects the risk in real time
- Falcon Fusion SOAR drives remediation through ServiceNow
- Falcon Next-Gen SIEM tracks the incident from a threat detection and investigation perspective

The result is faster time to mitigation, complete auditability, and a feedback loop for improving detection fidelity and response efficiency.

By automating exposure management across security and IT operations, organizations can move from passive visibility to actionable intelligence and response, reducing risk and improving resilience across the software estate.

4. Automating Phishing Response with Falcon Fusion SOAR

Phishing continues to be a primary threat vector for credential harvesting, malware delivery, and initial access in targeted attacks. Security teams often rely on user-reported emails to detect these campaigns, but manual triage, containment, and remediation of phishing attempts can be inconsistent and time-consuming — especially at scale.

Falcon Fusion SOAR operationalizes phishing response through an automated workflow that integrates user identity, malware analysis, and endpoint telemetry. This ensures that phishing threats are swiftly analyzed, contained, and remediated with minimal analyst intervention.

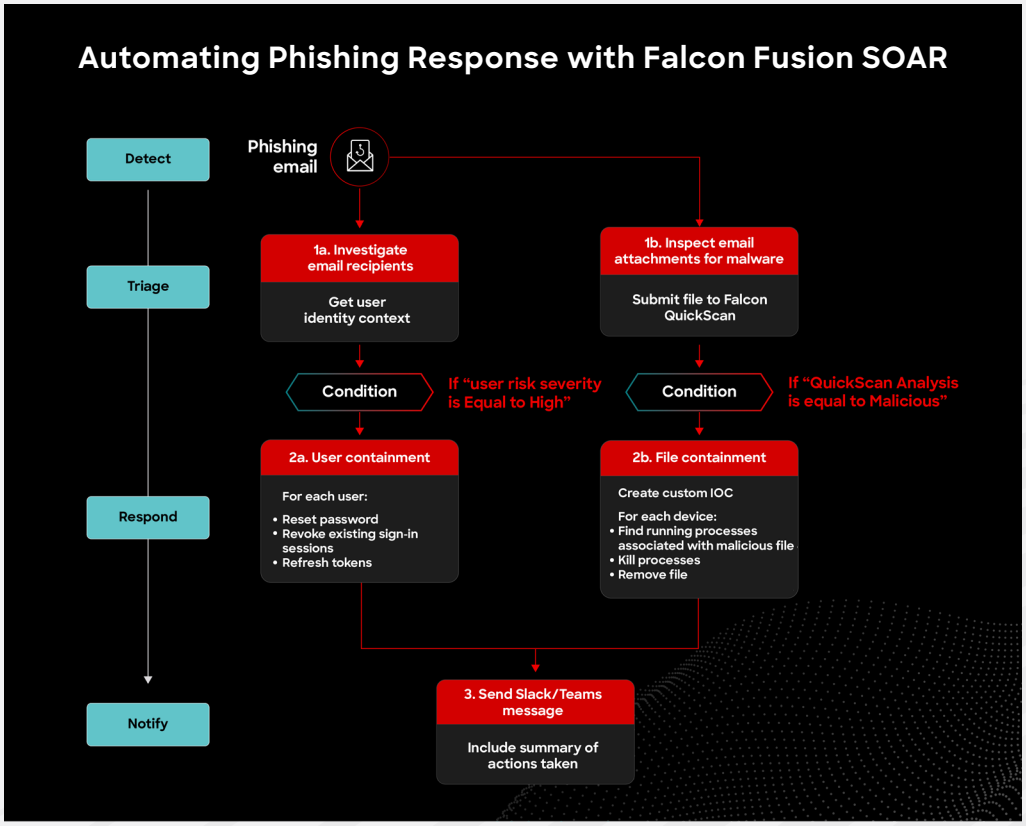

Figure 7. Falcon Fusion SOAR streamlines phishing response at scale through workflow automation that unifies identity, malware analysis, and endpoint insights for rapid remediation.

Trigger: User-Reported Phishing Email

The phishing workflow is initiated when a user reports a suspicious email through integrated reporting mechanisms (e.g., Outlook add-in, phishing mailbox). This report automatically triggers a Falcon Fusion SOAR playbook, kicking off parallel analysis threads focused on both users and attachments.

Step 1a: Loop Through Email Recipients and Evaluate Risk

Falcon Fusion SOAR begins by looping through all recipients of the reported email. For each user:

- The system retrieves user identity context from Falcon Identity Threat Protection
- A risk severity score is evaluated for each recipient based on behavioral indicators and account posture

If a user's risk severity is classified as High, the workflow proceeds to automated containment.

Step 2a: User Containment Based on Identity Risk

For each high-risk user, Falcon Fusion SOAR executes the following containment actions:

- Password reset to prevent continued credential use
- Revocation of existing sign-in sessions and refresh tokens to disrupt any active adversary access

These actions are executed immediately and without manual approval for users who meet the containment criteria.

This identity-based decision tree ensures surgical response while avoiding unnecessary disruption for low-risk users.

Step 1b: Analyze Email Attachments via CrowdStrike QuickScan Pro

Simultaneously, Falcon Fusion SOAR loops through all file attachments in the phishing email and:

- Submits each file to CrowdStrike® QuickScan Pro for lightweight malware analysis
- Evaluates returned verdicts for threat classification

If an attachment is identified as malicious, the workflow proceeds to file-level containment.

Step 2b: File Containment via Custom IOCs

Upon detection of a malicious file, a custom IOC is created to track the malicious hash. And for each endpoint where the file is observed:

- Falcon Fusion SOAR identifies any running processes associated with the file
- The system terminates active processes
- The malicious file is removed from disk, ensuring thorough cleanup

This automated response leverages real-time telemetry and the Falcon API to eliminate the threat before it spreads laterally.

Step 3: Notify Stakeholders of Action Taken

Once all user and file containment steps are completed, Falcon Fusion SOAR sends out automated notifications:

- A structured summary of the incident and remediation actions is sent via Slack, Teams, or email
- Recipients include SOC analysts, affected users, and other relevant stakeholders

These updates maintain transparency and provide documentation for compliance and reporting

Outcome: Coordinated Phishing Defense Across Identity and Endpoint

By orchestrating parallel analysis across user identity and file behavior, this phishing response workflow delivers comprehensive visibility and control:

- High-risk users are isolated before compromised credentials can be weaponized
- Malicious attachments are neutralized before they execute payloads
- SOC teams gain real-time visibility without the burden of manual triage

Falcon Fusion SOAR transforms phishing response from reactive, manual effort into a structured, repeatable, and auditable process, enabling defense at machine speed across both human and endpoint attack surfaces.

This orchestration is achieved through Falcon Next-Gen SIEM, which unifies native telemetry with third-party data — including email gateways, threat intelligence platforms, and sandbox results — into a correlated, real-time view of phishing activity. By integrating data across the security ecosystem, Falcon Fusion SOAR enables precise, coordinated response at scale.

The result is a fully connected workflow that converts fragmented phishing signals into actionable intelligence, accelerating time to containment and reducing operational burden on security teams.

5. Automating IOC Investigations with Falcon Fusion SOAR, LLM-Powered Analysis, and External Intelligence Integration

With adversaries increasingly leveraging dynamic infrastructure like fast-flux IPs and ephemeral command-and-control (C2) domains, IOC triage can no longer rely solely on internal telemetry. Modern security teams need the ability to fuse real-time event data with external intelligence sources and machine-assisted triage, all without breaking analyst workflows.

To address this, Falcon Fusion SOAR — in combination with Falcon Next-Gen SIEM and Advanced Event Search — automates the entire IOC investigation life cycle, from data collection and large language model (LLM) enrichment to dynamically updating lookup tables for future detections.

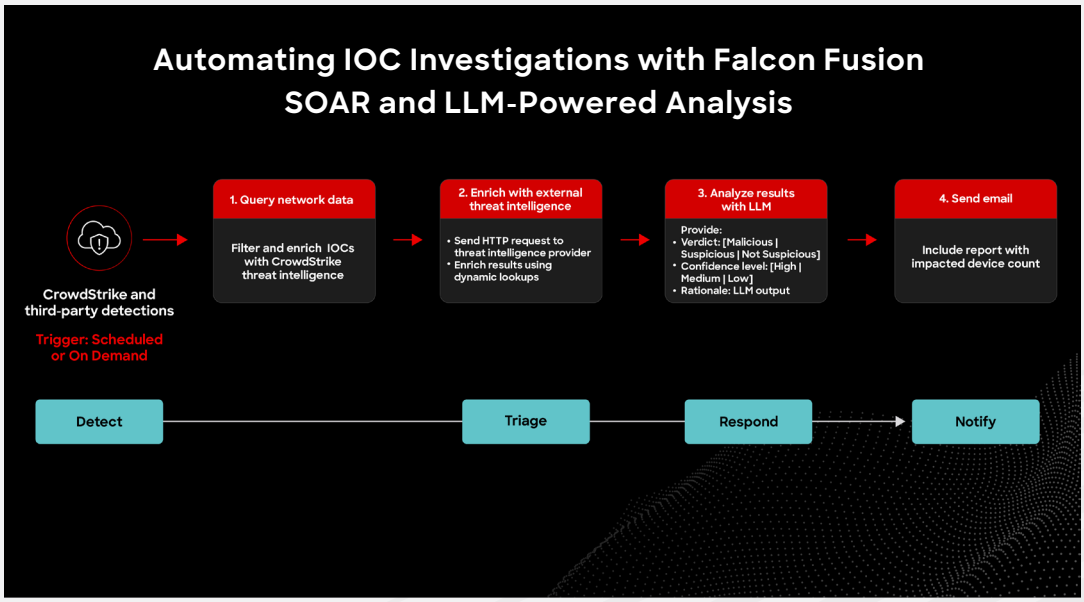

Figure 8. Falcon Fusion SOAR streamlines IOC investigation with automated data collection, LLM-based enrichment, and dynamic updates to lookup tables for future detections.

Trigger: On-Demand IOC Investigation

This workflow is triggered manually by an analyst or via automated playbooks. The input is a destination IP address of interest, which is often tied to:

- Falcon detections
- Threat intelligence reports
- Suspicious activity in user or network behavior

This flexibility enables IOC sweeps, rapid triage, and threat hunting — all on demand.

Note: This same investigation flow could also be triggered automatically — for example, to iterate over all IOCs associated with a Falcon Next-Gen SIEM case and perform reputation lookups and contextual triage at scale.

Step 1: Query Events Using Advanced Event Search

Falcon Fusion SOAR runs a query in Advanced Event Search over the last 24 hours of telemetry, targeting events from key vendors (e.g., Palo Alto Networks, Fortinet, Corelight). It filters for any traffic involving the input IP and annotates it with:

- Vendor rule names
- IOC metadata (e.g., labels, confidence level of IOC maliciousness)
- Destination details (domain, NAT IP, port)

This gives analysts a strong foundation for evaluating the IP's behavior in the environment.

Step 2: Enrich with External Threat Intelligence

In parallel, the workflow makes an HTTP API request to a third-party threat intelligence provider (e.g., AbuseIPDB, VirusTotal, AlienVault OTX) to:

- Query reputation for the destination IP
- Retrieve labels, tags, risk scores, or categories

This external lookup data is parsed and formatted into CSV or JSON and then written as a lookup file in the Falcon Next-Gen SIEM environment using Falcon Fusion SOAR's built-in actions:

- `Get lookup file metadata` → check if file exists
- `Overwrite lookup file` → publish enriched results

This ensures that the IP's reputation is now available for future detection queries, anomaly correlation, and other workflows.

> *Example:* The IP `192.0.2.100` is observed with suspicious outbound connections. External lookup identifies it as associated with the "Cobalt Strike C2" tag. This data is stored in a file like `ioc_external_enrichment.csv` and immediately usable in future Advanced Event Search queries via `match(file="ioc_external_enrichment.csv", ...)`.

Step 3: Generate Summary with LLM-Powered Analysis

The original Advanced Event Search results are then passed to a LLM — configured via the latest version of Claude — along with a structured prompt instructing it to:

- Analyze the event context
- Cross-reference with IOC tags
- Provide a verdict: Malicious, Suspicious, or Not Suspicious
- Output a confidence score and rationale

This delivers a clear, actionable summary to the SOC in seconds.

Step 4: Notify Analysts

Finally, Falcon Fusion SOAR sends an automated email to the designated analyst or team:

- Subject: Suspicious IOCs Detected
- Body: Includes destination IP, verdict, confidence level, and LLM-generated rationale
- Attachment/link: Advanced Event Search results and (optionally) the external enrichment file

This ensures triage results are captured, distributed, and available for incident response, escalation, or tagging in Falcon.

Outcome: Falcon Fusion SOAR-Driven, AI-Enhanced IOC Triage with Continuous Intelligence

This enhanced workflow delivers an end-to-end IOC investigation framework combining:

- Advanced Event Search for deep contextual telemetry
- External threat enrichment for risk-informed decision-making
- LLM analysis for fast, explainable triage
- Dynamic lookup publishing to Falcon Next-Gen SIEM for future detection and correlation

This enables analysts to investigate and enrich indicators in real time, leverage third-party threat intelligence automatically, and create reusable intelligence artifacts for future workflows.

By integrating external threat data and publishing enriched lookups automatically, Falcon Fusion SOAR becomes a bridge between tactical response and long-term threat detection strategy.

Falcon Fusion SOAR: Security at Lightning Speed

Falcon Fusion SOAR revolutionizes security operations by eliminating the complexity and manual workflows that typically slow down security teams. Through an intuitive approach that combines natural language workflow automation, dynamic case management, and breakthrough AI capabilities, teams can transform complex security processes into automated responses within minutes.

Customers are already realizing measurable business impact with Falcon Fusion SOAR. For example, a global manufacturer and home improvement products company achieved $62,000 in effort savings by automating activities across its 11 business units using Falcon Fusion SOAR and CrowdStrike Falcon® Flight Control, a Falcon platform feature that enables a robust multi-tenancy architecture, allowing an environment to be logically segmented.[1] This reduction in manual effort not only freed up analysts to focus on higher-value security tasks but streamlined collaboration across business units, proving the platform's ability to deliver both security and operational ROI at scale.

Beyond efficiency gains, customers consistently highlight Falcon Fusion SOAR's ease of use, seamless integration with the Falcon platform, and ability to unify workflows across the SOC. They call out Falcon Fusion SOAR as "a game changer" for reducing manual tasks, minimizing management overhead, and blending naturally into existing security operations.[2]

"We're super excited about Falcon Fusion. It's intuitive, and having that type of automation within the Falcon platform is huge for us. There's a lot of custom ad hoc rules that we leverage, and having that SOAR capability to automate any of those steps is valuable."

— Nathan Kelly, Senior Information Security Engineer, TaylorMade Golf

As a native component of the Falcon platform, enhanced by state-of-the-art AI agents and Charlotte AI, Falcon Fusion SOAR enables teams to analyze incidents and orchestrate actions across their entire security stack with unprecedented speed and precision. The result? Teams operate at lightning speed, responding to threats faster and more confidently while reclaiming valuable time for strategic initiatives.

Are you ready to start your workflow automation journey with Falcon Fusion SOAR? Contact our team today to unleash the power of AI and automation.

[1] Internal ROI study, customer since 2019, above value realization conducted in 2024, anonymized attribution only
[2] CrowdStrike internal customer research surveys, anonymized attribution only

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/