Falcon Fusion Accelerates Orchestrated and Automated Response Time

MITRE adversary scenarios demonstrate Falcon Fusion's powerful SOAR capabilities

April 28, 2022

Janani Nagarajan Endpoint & Cloud Security

- CrowdStrike Falcon Fusion automates and accelerates incident response by orchestrating sandbox detonations to automatically analyze related malware samples and enrich the results with industry-leading threat insights
- Falcon Fusion enables analysts to build real-time active response and notification capabilities with customized triggers based on detection and incident disposition
- The CrowdStrike Falcon® platform leverages critical context, visibility and response capabilities when defending against persistent adversaries with unified endpoint, workload and identity protection

In the recent MITRE Engenuity ATT&CK Enterprise Evaluation —— which emulated today's two most sophisticated Russian-based adversaries, WIZARD SPIDER and VOODOO BEAR (Sandworm Team) —— CrowdStrike Falcon achieved 100% automated prevention across all of the evaluation steps. This not only demonstrates the power of the Falcon platform to stop breaches, but also provides a clear demonstration of the dynamic nature of Falcon Fusion, delivering the automated workflows customers require to stop today's most sophisticated threats.

Natively integrated into the Falcon platform, Falcon Fusion is a unified and extensible security orchestration, automation and response (SOAR) framework. In the MITRE Engenuity ATT&CK Enterprise Evaluation, Falcon Fusion enabled multiple autonomous workflows —— including using indicators of attack (IOAs) as triggers for additional malware analysis or updating the identity watchlist based on compromised credentials —— to essentially stop the attackers cold.

Falcon Fusion is able to leverage the power of Falcon Identity Protection, Falcon X™ threat intelligence with comprehensive IOAs, and machine learning (ML) to enable security operations center (SOC) teams to make faster and better decisions with the right insights and tools by reducing time to hunt through data and autonomously responding to sophisticated threats.

Using Falcon Fusion Against Credential-based Attacks

In the Initial Access step during the VOODOO BEAR emulation scenario (step 11.A.1), stolen access credentials were used to initiate the attack. Using Falcon Fusion workflows, the stolen credentials were added to an identity watchlist along with the device, blocking the use of that credential for the attacker to leverage again. In a real-world configuration, Falcon Fusion could have been used to trigger a multifactor authentication (MFA) challenge if those credentials were used in any subsequent attacks.

Falcon Fusion, in conjunction with Falcon Identity Protection capabilities, was able to automatically alert on the use of compromised credentials for the monitored accounts and auto-classify the accounts as a valuable target, enabling additional security controls based on risk levels and behaviors during an ongoing attack.

Figure 1. A Falcon Fusion workflow adding a user with noted stolen credentials, based on detection using lateral movement tactics, to the Falcon Identity Protection watchlist, which in turn can enforce MFA action based on repeated usage

Throughout Round 4 of the MITRE Engenuity ATT&CK Enterprise Evaluation, Falcon Fusion increased the time-to-value in driving automated workflows based on custom IOA detections. In real-world scenarios, Falcon Fusion dramatically reduces alert fatigue and frees up resources so analysts can focus on other critical and strategic tasks. This integrated approach provides analysts with a powerful cloud-delivered platform to defend against future attacks, as demonstrated throughout the evaluation.

Using Falcon Fusion for Custom IOA Monitoring and Falcon X Malware Analysis

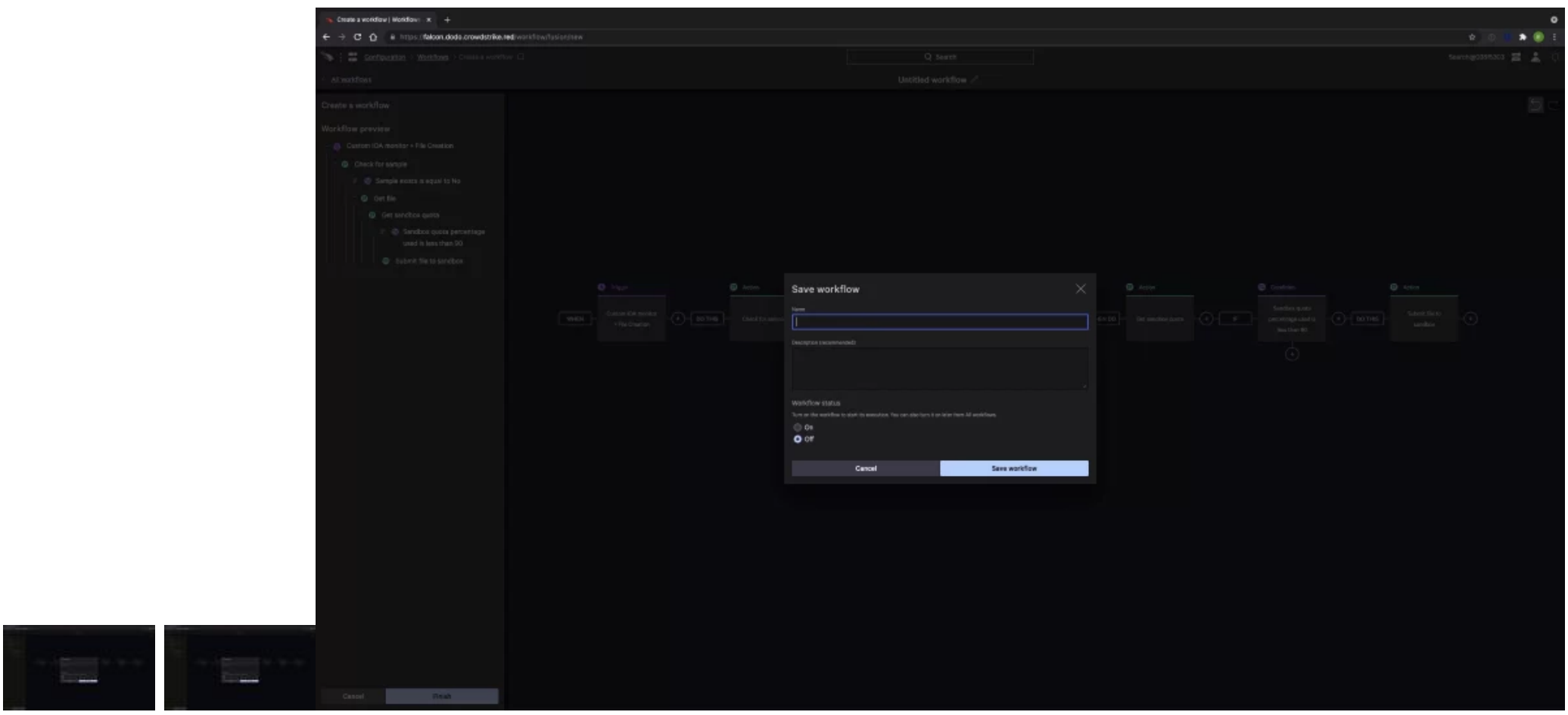
The WIZARD SPIDER Initial Compromise emulation scenario (substep 1.A.2) showcased a potential workflow that involved immediately sending files to the CrowdStrike Falcon X malware sandbox for detonation if dropped via remote desktop sessions. In real-world scenarios, the Falcon platform sends all suspicious files to the Falcon X automated sandbox, driven by CrowdStrike Falcon Prevent™ next-generation antivirus security policies. For custom IOAs based on different file types (e.g., documents, PE .exe files, PE DLL files, or scripts), Falcon Fusion helps drive the Falcon X sandbox detonation automatically using the IOAs as trigger, ensuring further analysis occurs as part of a layered defense approach without any manual intervention.

Figure 2. A Falcon Fusion workflow retrieving an auto-submit file, which triggers the submission of behavioral detections to the Falcon X sandbox for further analysis

Detonating binaries in the Falcon X sandbox uncovers the behavior of suspicious files and extracts more information than is possible on the endpoint. This provides analysts with optimized threat intelligence and context allowing them to identify indicators of compromise (IOCs) and hunt for secondary payloads, making it difficult for adversaries to bypass detections by changing the initial dropper component.

Scenario: Falcon Fusion workflows for Custom IOA monitors allow indicators to be generated to the cloud without generating detections that will show up in the Falcon detections UI.

- Custom IOA monitors can be created for Domain name, Network connection, File creation, Process execution or all four items and used as a trigger. In this example, File creation —— when a file writes a process to disk —— was chosen as the workflow trigger.
- For the first action, the following can be chosen under the Intelligence category: Check for sample, Get sandbox quota, Submit SHA256 to sandbox or Submit URL to sandbox. In this example, Check for sample was chosen to check —— using the condition "sample exists = false" —— that a sample hasn't already been uploaded from an endpoint to the cloud.
- A Falcon Real Time Response (RTR) script can be used to get the target file name that was written to disk. Custom RTR scripts can be used with Falcon Fusion to directly access distributed systems and run a variety of commands to investigate, conduct forensic analysis or completely remediate remote systems.
- The "Submit file to sandbox" sequential action was chosen, with Windows 7 64-bit selected as the setting needed for sandbox analysis and Tor enabled. Post-detonation, the link to the sandbox report will become available for additional investigation and new workflow creation from the Falcon dashboard.
- Post-remediation actions —— such as running checks on the system to ensure it is clean; issuing automated notifications via collaboration channels like email, Slack or Microsoft Teams; and updating ticket status on IT management systems like ServiceNow or Jira —— can be performed to ensure full-cycle incident response.



6:33

Falcon Fusion demo

Modernize Your SOC and IT Operations

Falcon Fusion's native integration with the Falcon platform makes it unique among SOAR frameworks. Running in a software-as-a-service (SaaS) environment and requiring no custom integrations to be developed and available at no additional cost, Falcon Fusion delivers high performance and immediate time-to-value.

The native integration of Falcon Fusion within the Falcon platform allows you to collect contextually enriched data and automate security operations, threat intelligence and incident response to mitigate cyber threats and vulnerabilities —— all through the same console. In addition to its power, Falcon Fusion's automation is easy to use and can simplify complex security workflows, optimizing SOC performance.

Start your free Falcon platform trial now and realize the benefits of the Falcon Fusion SOAR framework. Access Falcon Fusion from your Falcon console to see how you can simplify your SOC and IT workstreams, while achieving speed and precision against sophisticated adversaries.

Additional Resources

- Read CrowdStrike CTO Mike Sentonas's blog that showcases how independent testing proves that CrowdStrike Falcon platform continues to lead the industry in stopping ransomware, destructive malware adversaries and breaches.
- Learn more about the Falcon Fusion integrated cloud-scale framework.
- Get technical details about Falcon Fusion by viewing the data sheet.
- Learn how the powerful CrowdStrike Falcon platform provides comprehensive protection across your organization, workers and data, wherever they are located.
- Get a full-featured free trial of CrowdStrike Falcon Prevent™ and see for yourself how true next-gen AV performs against today's most sophisticated threats.

- Tweet
- Share

Related Content