Glossary of Terms

Preliminary Post Incident Review (PIR): Content Configuration Update Impacting the Falcon Sensor and the Windows Operating System (BSOD)

	General	Technical
Channel Files	Channel files are like instruction manuals for sensors. They tell the sensors how to work, including the allow/blocklist. These files are saved on the host computer and updated dynamically, such as when administrators make changes in their Falcon sensor/policy configuration or detection logic is updated.	Dynamic configuration files utilized by the sensor. They contain configuration information, such as whitelisting details, and are transmitted to a given Falcon sensor (or sensors) within an environment.
Content Configuration Updated	CrowdStrike's process that updates policy and detection settings.	CrowdStrike Falcon's backend process that updates the policy settings and detection content that affects how the Falcon Sensor operates.
Content Configuration System	Manages the creation and distribution of channel files.	Manages the creation and distribution of channel files. The Content Configuration System is part of the Falcon platform in the cloud.
Content Interpreter	A component of the Falcon sensor that reads and interprets Rapid Response Content from a channel file.	A component of the Falcon sensor that reads and interprets Rapid Response Content from a channel file, which enables the Sensor Detection Engine to observe, detect or prevent malicious activity, depending on the customer's policy configuration
Content Validator	Performs validation checks on content before it is deployed.	Part of the content configuration system that performs validation checks on content before it is deployed.
Template Types	Pre-made forms that help experts quickly respond to threats. These forms are written in code.	A sensor capability that pre-defines a set of fields for Rapid Response Content to leverage for new telemetry and detections.
Template Type Stress Testing	Process that CrowdStrike performs to test the template types under various conditions to enable reliability and performance.	Testing the template types under various conditions to enable reliability and performance. Tests are executed in a staging environment that consists of a variety of operating systems and workloads.
Template Instance	Instructions for the Falcon sensor to observe, detect, or prevent a specific behavior.	A series of instructions for the Falcon sensor to recognize a single specific behavior to observe, detect, or prevent.
Rapid Response Content	This is a special kind of update that quickly improves the security system on your computer. It helps the system recognize and stop new types of threats without needing to change the main program. A quick update that keeps your protection up-to-date and ready to handle the latest dangers.	A set of Template Instances providing the Falcon Sensor with dynamic detection logic updates to respond quickly to new threats.
Sensor Content	A wide range of capabilities for the sensor to detect threats, including AI and ML models. Sensor content is part of a sensor release and not dynamically updated from the cloud.	A wide range of capabilities for the sensor to detect threats, including on-sensor AI and ML models. Sensor content is part of a sensor release, and not dynamically updated from the cloud.
Named Pipes	Named pipes allow different software programs to communicate with each other on the same computer.	A method for inter-process communication that allows separate processes to communicate with each other. This is referred to as InterProcessCommunication (IPC).

InterProcessCommunication (IPC) Template Type	A template type used to detect threats involving interprocess communication.	A template type used to detect threats involving interprocess communication, such as Named Pipes.
IPC Template Instance	A specific configuration created from an InterProcess Communication Template Type. It tells the sensor which behaviors to observe, detect, or stop.	A specific configuration derived from the IPC Template Type that maps to particular behaviors for the sensor to observe, detect, or prevent. For example, deploying an IPC Template Instance to detect unauthorized use of named pipes for malware lateral movement within a network.
Sensor Detection Engine	Component of the Falcon sensor is responsible for detecting and preventing malicious activity.	The component of the Falcon sensor responsible for detecting and preventing malicious activity. Used to observe, detect or prevent malicious activity, depending on the customer's policy configuration.
Additional Terms		
Behavioral Heuristics	Techniques used to detect threats based on behavior patterns rather than static signatures.	Techniques used to detect threats based on behavior patterns rather than static signatures, such as detecting process injection or credential scanning.
Fault Injection	A testing method where intentional errors are introduced into a system to see how it responds and to identify weaknesses, helping to make the system more robust and reliable.	A testing technique where intentional errors are introduced to validate the robustness and error-handling capabilities of a system. For instance, in a distributed database system, fault injection might involve simulating network partitions, where certain nodes become temporarily unreachable.
Canary Deployments	A software distribution strategy where updates are first rolled out to a small group of users to test for issues before a wider release.	A deployment strategy that incrementally releases new software changes to a small subset of users to validate functionality and detect issues before a full-scale rollout.
Fuzzing	A testing technique where random or unexpected data is input into a software program to find bugs or vulnerabilities, helping to make the software more secure and reliable.	A testing methodology that inputs random, malformed, or unexpected data into a program to uncover security vulnerabilities, bugs, and edge cases that could lead to system crashes or unexpected behavior.
Adversary Response	The actions or reactions taken to counter or defend against someone or something trying to cause harm or disruption, such as in cybersecurity.	Involves detecting, analyzing, and mitigating threats through advanced threat intelligence, forensic analysis, and immediate incident response to contain and eradicate attacks.
Behavioral Pattern-Matching	A method of identifying common behaviors or trends by comparing them to known patterns, helping to predict or recognize specific actions or events.	An advanced technique that identifies and correlates specific behaviors within a dataset by comparing them to known patterns, using machine learning algorithms and statistical models to detect anomalies and predict specific actions or events.
Exception Handling	A way for software to manage and fix unexpected problems or errors, enabling the program to continue to run smoothly without crashing.	A programming concept used to manage and respond to runtime errors in a controlled manner, involving three main components: a "try block" to run code that might fail, a "catch block" to handle specific errors if they occur, and a "finally block" to run cleanup code.
Out-of-Bounds Memory Read	A programming error where a program reads memory it is not supposed to.	A programming error that occurs when a program accesses memory beyond allocated boundaries.
Dogfooding	Process by which a company uses its own products to test and improve them.	Process by which a company uses its own products or services internally to test and validate their quality, functionality, and user experience.