CrowdStrike White Paper

CROWDSTRIKE

LOG MORE TO IMPROVE VISIBILITY AND ENHANCE SECURITY

Improve threat hunting with long-term storage of log data for security telemetry

LIMITING LOG DATA STORAGE CREATES BLIND SPOTS

As the amount of system log data grows exponentially, security teams and threat hunters routinely must limit how much they can collect and how long they can store it because of the performance limitations and costs associated with traditional log management tools.

These legacy tools, which often use storage-intensive indexes to improve log searches, are unable to ingest and analyze massive amounts of data, causing them to falter at scale. And because the size of these indexes is often larger than the data that is most relevant to incident investigators, organizations can incur excessive licensing and infrastructure costs if their security teams attempt to ingest all of this data for future searches and investigations.

Unfortunately, when an organization limits data collection, its security team has limited visibility into incidents occurring (or that have already occurred) in the IT infrastructure. Adversaries exploiting these visibility gaps can enter an organization's network and hide for months instead of days or hours — long enough to do significant damage as their cyberattack goes undetected.

MORE DATA MEANS MORE CONTEXT TO RESPOND TO AN EVER-EVOLVING THREAT LANDSCAPE

To fully investigate and uncover stealthy attacks, security teams must have access to not only an immense amount of historical, context-rich data but also a scalable, extensible log management solution capable of leveraging it to provide a behavioral review of users, processes and connectivity — revealing the trails left behind by the adversary.

For example, a supply chain attack like **SUNBURST** requires security teams to have a long-term view of prior events to identify potential indicators of compromise (IOCs). In such attacks, an adversary can remain dormant for six or more months waiting for a user to inadvertently surrender their credentials, enabling the adversary to move laterally and quietly within an infrastructure. Likewise, when a seemingly trusted and signed binary has been corrupted at the source, the ability to review event history is required to reconcile when and how an adversary started their attack. This ability is even more crucial in responding to vulnerabilities like **Log4Shell**, where organizations had to quickly sweep their entire cyber environment for detection and remediation. With limited data and visibility, many security teams struggled to patch and respond swiftly, putting their organizations at risk of a breach.

LEGACY LOGGING TOOLS HINDER MODERN INCIDENT RESPONSE

Security teams typically use security information and event management (SIEM) or log management tools when responding to incidents. However, these legacy approaches cannot handle the more complex, dynamic and ever-growing scope of log data required for modern incident response.

In the quest for threat context, incident responders must often take on some of the heavy lifting that comes with the "data gravity" of a comprehensive logging solution, which comes in the form of diverse data sets and extensible query capabilities with pre-built functions that allow you to ingest up to a petabyte of data.

Given licensing costs and limitations in capacity or performance, security teams are usually forced to reduce their log intake because their legacy platform is unable to ingest massive amounts of historical data and query it effectively to find new insights. As a result, they are forced to compromise by accepting blind spots in their strategy. And because there is no effective way to predict which data will be needed in an investigation, this forced reduction in historical data can create serious challenges when investigating a security incident or performance issue.

There is an alternative that helps threat hunters and incident responders maximize the available data and use the resulting historical view to power better investigations. A scalable log management platform can collect and provide immediate access to all valuable information collected in system logs. With this data at your disposal, you get extensive historic information to track up to 365 days of behavior (for users, processes and networks) while limiting the time required to move between tools or wait for a query to complete.

STORING LONG-TERM LOG DATA ENHANCES THREAT IDENTIFICATION

As attacks evolve and the amount of data accelerates, security and IT teams must embrace a "federated intelligence" strategy — where large amounts of intelligence can be efficiently and affordably stored — if they are to gain the threat context and historical visibility they need to more easily and quickly detect and understand potential threats. This additional retention of data also provides visibility into long-term trending and baseline activities and behaviors, allowing investigators to better understand and more accurately identify potentially malicious activity during investigations.

Through the storage of long-term security data, threat hunters can seamlessly sift through and analyze vast and diverse data sets via queries to detect long-term trends and uncover elusive or hidden threats in their distributed environments. To store and manage all of your security data effectively, without heavy resource or cost requirements, you must implement solutions that unify your dispersed data sets and enable your team to act with speed. Through the enhanced scale and additional threat insight provided by long-term security data retention, you can analyze multiple log sources and narrow the scope of a detection to match to a given adversary, empowering you to stop breaches faster.

UNIFYING DATA SETS ACCELERATES INVESTIGATION, HUNTING AND RESPONSE

Developing a comprehensive security practice involves deploying a number of different solutions and employing a team of security professionals to manage them. These solutions include firewalls, network analytics, cloud security, identity protection, email security, Windows event monitoring and others that provide telemetry that can feed a scalable, extensible logging solution. Because these solutions deliver valuable data and unique insights from different areas of the environment, unifying these sources for true end-to-end visibility and control is critical, but it remains a daunting challenge for IT and security teams. As security teams are typically overworked and under-resourced, organizations need solutions that help reduce mundane activities by unifying threat data, automating processes and filtering out the noise so teams can focus instead on higher skill activities and critical threats.

The introduction of **extended detection and response (XDR)** helps organizations overcome this challenge by seamlessly collecting disparate threat data from previously siloed security tools across the technology stack for easier and faster investigation, threat hunting and response capabilities. By unifying and storing XDR data via a scalable logging solution, security teams get deep, contextual and faster analytics on massive amounts of security telemetry for comprehensive visibility of their entire environment. Fast and flexible ingestion and effective correlation of threat data from any log, application or feed helps teams remove friction across their disparate data sets to improve productivity and gain actionable insights for real-time protection. By storing and managing this XDR data for longer with expanded data

retention, security teams have access to more unified, richer data to enhance their search capabilities and end-to-end visibility of their environments. This additional context and speed enables organizations to see potential threats faster for improved threat hunting and troubleshooting at scale.

GAIN THREAT CONTEXT WITH A SCALABLE LOG MANAGEMENT SOLUTION

The ability to collect, parse and interrogate multiple log sources enables threat hunters to create high-fidelity findings. In the same way law enforcement uses information like phone logs, social media and financial records to build a case, log management solutions allow threat hunters to delve into deeper context and build more powerful investigations.

As organizations respond to the rise of big data and ongoing digital transformations, one thing remains elusive: the tenets of "big context." The inability to make data tactile has been, at times, the bane of the threat hunter and incident responder.

The answer to a more complex, diverse and dynamic data environment is in the data itself. A modern log management platform can effectively capture more information (both from a cost and a performance standpoint), but it requires complete and enriched security data collected across the organization's technology stack to provide context and actionable insights surrounding potential threats. This unified security data allows you to cross-reference findings, detections and other intelligence with data originating from firewall logs, network telemetry (NDR or NETFLOW) and other log sources. By correlating high-quality security data across endpoints, workloads, identities and more, hunters get higher fidelity findings and more granular context for smarter investigations.

The quality of security data you store and use in a log management platform is the key to the success of your hunting and investigations as it provides necessary insights for identifying and remediating threats. For a complete picture of threats or malicious activity occurring in your environment, your security data should include unified and enriched sources from across the organization as part of security detections, enabling defenders to more narrowly define the scope of detections to exactly match adversary techniques and actions for fewer false positives. The addition of enriched security telemetry from a source like the CrowdStrike Security Cloud, one of the world's largest unified, threat-centric data fabrics, provides an anchor data source that, in addition to providing high-context endpoint findings, can be leveraged with other telemetry and log data to provide unparalleled threat context across the distributed environment.

INTRODUCING FALCON LONG TERM REPOSITORY

To make use of all of your data, you need a feature-rich query language and index-free searches to enable threat hunters and investigators to quickly find answers hidden in the data. You should be able to run complex searches to gain insights using regular expressions and multiple joins to generate new insights from the data. This should also allow you to get alerts and visualize streaming data in real time and at scale. These capabilities are all available through CrowdStrike Falcon Long Term Repository (LTR), powered by Humio.

Falcon LTR feeds CrowdStrike Falcon® platform security data across endpoints, workloads and identities into the Humio log management solution via CrowdStrike Falcon Data Replicator (FDR). Falcon data is continuously ingested and enriched by the CrowdStrike Security Cloud as it correlates trillions of security events per day with indicators of attack (IOAs) to provide teams with contextualized telemetry on more than 400 event types. This rich set of Falcon data contains detailed information about user IDs, processes, hashes, detections, network connectivity and more.

This data is also correlated by CrowdStrike Asset Graph, which dynamically monitors and tracks the relationships among all assets such as devices, users, accounts, applications, cloud workloads and operations technology (OT), along with the rich context necessary for proper security hygiene and proactive security posture management. When combined with other incumbent data sources through Falcon LTR, you can instantly search and cross-reference your security and device telemetry with other threat resources for unparalleled threat analytics and hunting. Combine this with Humio Marketplace applications written specifically for Falcon LTR and you can move beyond simply appending more logs and actually scale them with other solutions.

To expand the historical view of incidents, Falcon LTR allows you to store and manage your Falcon data for a year or more, enabling teams to gain visibility and threat context across your growing attack surface. Longer data retention, combined with enriched security telemetry powered by the CrowdStrike Security Cloud and CrowdStrike Asset Graph, gives your security team enhanced threat insights to gain visibility over attack paths to detect and respond faster. With longer retention, contextual analytics and lightning-fast search results at any scale, you can meet your unique compliance and security needs.

Falcon LTR offers security teams per-endpoint pricing, which provides a simpler and more predictable licensing model that allows teams to collect all security data without having to choose or predict which events might be needed in an investigation. Responders are enabled to ingest and query all of the endpoint, workload and identity data at your disposal, providing a more complete and accurate picture of incidents and potential threats in your environment.

APPENDING VS. SCALING

In a traditional, more restrictive pricing model for log management software, adding logs and data to a log management platform does little more than add to the weight of the existing data gravity dilemma. Humio's FDR Marketplace package, which accompanies Falcon security data, goes further, as the incoming data is scaled by the accompanying saved queries, dashboards and threat hunting workflows.

Threat hunters and incident responders do not necessarily need more data — they need better and more diverse data. Falcon LTR puts a rich data source at their fingertips and provides a way to add data from CrowdStrike — the industry's leader in endpoint security — into existing threat hunting processes. While the endpoint data from Falcon LTR itself is valuable, the added context that security teams can derive from combining this data source with other log management data sources increases the value even more.

ENABLING THE THREAT HUNTER

A log management solution's key data sources are typically Windows Sysmon events, authentication logs, intrusion detection/network telemetry and, if you're fortunate, threat intelligence. Threat hunters mash up these events to deliver high-context findings that can be distilled into actionable intelligence. Even with all of this data, it is common for a responder to pivot to a tool to get endpoint metrics — or even look directly at the endpoint itself, which is often one of thousands.

While CrowdStrike Falcon Insight™ endpoint detection and response (EDR) has previously been available for ingest into log management solutions via FDR, many log management licensing models made it difficult and expensive to use. Per-endpoint pricing allows teams to leverage the solution without the worry of unpredictable ingest costs or limits.

To further this endpoint data and support your threat hunters' visibility and control over the entire environment, Falcon LTR unifies your disparate data and operationalizes it to enhance your XDR capabilities. With industry-leading endpoint protection at the core of your data combined with additional data sources including network, email, cloud, web, IoT/OT and more, you can synthesize multi-domain telemetry to provide your security team with one unified, threat-centric command console. With consolidated, multi-platform telemetry in Falcon LTR, you get dramatically enhanced threat correlation for more speed when detecting and responding, fortifying your protection against sophisticated attacks.

In cybersecurity, there is still uncertainty about automation and how to take action against an IP, a user's credentials or a workstation. Falcon LTR offers the ability to thread key endpoint, workload and identity findings into the threat hunting framework, which functions in parallel with existing investments in SIEM, SOAR and other technologies. With this approach, investigators gain the ability to correlate data from Falcon with existing logs, effectively removing layers until you feel that the action you are taking — such as disabling an account, blocking an IP or initiating containment of a system — is warranted. The breadth of intelligence available to a threat hunter increases by orders of magnitude when Falcon data is added to the intelligence that you are using to make decisions.

What if incident response teams and threat hunters could collect logs without being forced to abandon key data due to strict licensing models, storage restrictions or performance impacts? When logs are left on the "editing floor," you lose visibility and allow costs and external limitations to dictate your surveillance strategy. With a predictable licensing model, free from licensing, performance and storage constraints, Falcon LTR customers gain access to data that has often been underutilized because of these restrictions.

CONCLUSION

Falcon LTR, powered by the Humio log management platform, provides advanced threat hunting and threat analytics at unprecedented scale with extended data retention for a year or longer. The technology gives threat hunters and investigators access to enriched and contextualized Falcon security telemetry across endpoints, workloads and identities to deliver timely and actionable insights. Once the data is available, lightning fast historic searches and sub-second live searches help you find threats quickly. With flexible licensing and advanced techniques to minimize storage and computing resources, Falcon LTR provides a cost-effective way to empower threat hunters and investigators to eliminate blind spots and uncover incidents across the IT infrastructure.

WANT TO LEARN MORE?

Learn more about Falcon LTR: **www.crowdstrike.com/falcon-ltr**

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** | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

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