Cribl

EBOOK

Security and ITOps: Better Together

THE CHALLENGE

To effectively respond to the growing number and complexity of security threats, organizations need to consume unprecedented amounts of data – overwhelming current monitoring and response capabilities.

THE SOLUTION

Cribl LogStream simplifies data management, enhances threat hunting, and improves the ability to recover from attacks.

THE BENEFITS

- Reduce event noise, so relevant signals stand out
- Enrich logs in flight via reverse IP lookups and more
- Improve data quality for enhanced threat hunting
- Speed up incident response with LogStream's Replay feature

EBOOK

Security and ITOps: Better Together

Introduction: Security operations teams are dealing with unprecedented challenges with more data, complexity, and security threats.

When it comes to security today, perhaps the number one issue organizations are facing is the exponential growth of security threats, including the complexity and potential to inflict major damage. Security architects and Security Operations (SecOps) teams are scrambling to respond as enterprises continue to diversify IT infrastructures. Security telemetry is the foundation for monitoring and responding to security threats, but the growth of telemetry is overwhelming current monitoring and response capabilities. As a result, the ability to consume exponentially larger volumes of security data is becoming a critical dependency for successful security monitoring.

Consequently, we predict three types of companies will soon emerge:

1. *Organizations who collect the ever-multiplying volume of data and store it in a tool such as Splunk or Elastic, ultimately paying what can add up to millions of dollars to do so.*
2. *Companies who decide not to log security data to save money and accept the risk of compromise due to missed security events.*
3. *Organizations who take control of their data plane, collect useful data efficiently, and leverage their tools to get the best possible result.*

If you work in SecOps, you probably know that security teams are concerned about being able to consume the right data, data quality in general, and being able to manage the data to get the best possible results. This is the unique value that LogStream offers: control of your data plane.

ANY SECOPS ANALYST CAN USE LOGSTREAM'S EASY UI TO QUICKLY WRITE RULES THAT MANAGE DATA AND REMOVE NOISE, ENRICH DATA WITH THREAT INTELLIGENCE, AND ROUTE IT TO THEIR ANALYTICS TOOL OF CHOICE.

Typical approach to data management compromises the ability to detect, recover from, and prevent future cybersecurity attacks.

SecOps teams are tasked with overseeing analytics tools that help detect and prevent attacks, plus enable recovery. But effectively and efficiently consuming all data, including cloud data (often originating from multiple clouds) just isn't easy, introducing a myriad of compatibility and integration challenges.

Security analysts need to be able to reduce security data signal to noise ratio to get the best results from large, diverse datasets. However, a considerable amount of security data (nearly half in some cases) is not necessarily useful. As a result, being able to extract the right information in real time is a significant technical challenge largely due to sheer volume. For example, the vast majority of DNS data is not useful data; but how do you effectively reduce the noise in order to detect the important signal contained in the DNS data source?

This is where Cribl LogStream comes in.

SecOps teams need the ability to easily route data to any tool without being limited to a vendor's ecosystem. Any SecOps analyst can use LogStream's easy UI to quickly write rules that manage data and remove noise, enrich data with threat intelligence, and route it to their analytics tool of choice. For example, a SecOps team can easily bring a UEBA tool from Exabeam or Securonix into a Splunk environment without the integration challenges that would normally discourage this change. With LogStream in front of data, if the need to bring in another tool arises, it's a simple matter of writing a few lines of code and sending a stream of data to the tool in question to begin extracting value.

LogStream provides a simplified, rich user experience which makes solving hard problems much easier, as well as the flexibility to be able to control, redact, route, and enrich data.

Use cases: How LogStream simplifies data management, enhances threat hunting, and improves the ability to recover from attacks.

DATA MANAGEMENT

SecOps teams need to be able to consume application logs, security data, infrastructure data, and cloud data; what adds up to be potentially hundreds of different data types and often unmanageable complexity. While there are solutions such as custom integrations available, they can take six months to a year to use when starting from scratch, often because of usability limitations and the additional engineering time to buy your own solution. Each new custom integration creates an unsustainable workload for your engineering team.

Not to mention, most vendors charge by the amount of data they manage. It's no secret that such vendors don't have an incentive to enable customers to easily reduce the amount of data being consumed. Therefore, data management in and of itself is an uphill battle due to time constraints.

Cribl changes this dynamic entirely. For example, it's common for Cribl customers to reduce data ingestion by 25-45%. The default tools that come with LogStream make it easy to achieve data reduction and provide a starting point for SecOps teams to reduce data ingestion even further as they enrich their understanding and uncover opportunities for trimming.

In an ideal world, SecOps teams enable engineers and analysts to spend time on security, not managing data. Liberating engineering time and resources can be reoriented to objectives that matter.

LOGSTREAM SITS BETWEEN DATA SOURCES AND DESTINATIONS. THIS GIVES ENGINEERS AND ANALYSTS THE ABILITY TO EFFECTIVELY MONITOR ALL DATA WORKFLOWS, IMPROVING DATA GOVERNANCE.

1. **Managing Complexity with a Rich User Experience**

   LogStream's user experience makes managing regular expressions, visualizing data flow, and integration easier.

   In using Splunk HF or Logstash, for instance, building regular expressions cannot be easily tested and require awkward workarounds to validate. The user experience in LogStream gives you the ability to test your code with capture data in the UI so you know it's going to work, significantly reducing the time it takes to manage data, often by 50% or more. You'll know your code will work before you push to production.

2. **Managing the Data Plane**

   Enterprises have many data sources. LogStream is situated between data sources and destinations. This gives engineers and analysts the ability to monitor data and ensure nothing is missing or broken and ensure all data workflows are working as expected, which improves data governance.

3. **Data Enrichment**

   Many data logs are essentially incomplete, making enrichment an essential function of management.

   Consider firewalls, for example. The SecOps team has considerable data that's IP-based, but IPs aren't as useful as they could be. Therefore, it's necessary enrich incoming data in flight by conducting a reverse lookup to determine the fully qualified domain name and add the information to the event (which otherwise requires expensive search time processes on the backend). Using LogStream, it's easy to write code to conduct reverse IP lookups on behalf of engineers and add it to an event automatically.

   It's also possible to take lists of IOCs or threat deeds and automate the lookup process to allow for comparisons. Once again, in the case with firewalls, a large stream of data is flowing. Automating the lookup process allows operators to compare source and destination IPs with threat deeds to identify dangerous communications. For example, if LogStream sees a match, it adds metadata to the end of the event which reads "threat=true", eliminating the need to manually look up IOCs and expediting the normal workflow. Ultimately, this provides better data to the SIEM and saves an enormous amount of overhead on the back end in terms of having to run searches after the fact.

   Reducing event noise allows relevant signals to stand out. Further, data management licensing needs are typically reduced, and the rate of data growth slows. Security, in effect, becomes more effective with data.

4. **Ease of Use** *(and freeing SecOps to focus on more valuable activities)*

   A typical SecOps admin is tasked with writing code to manage data and integrate tools, but when LogStream is brought into the mix, an admin can work in a rich UI that makes every step of the development process dramatically easier from capturing sample data, to building complex regex and creating workflows to manage data. The time needed to build custom integrations will drop dramatically using LogStream.

INCIDENT RESPONSE TEAMS CAN USE LOGSTREAM REPLAY TO GO INTO THE OBJECT STORE, PULL THE FULL FIDELITY COPY OF A LOG, FIND THE EXACT DATA IN QUESTION, AND ANALYZE IT USING THE TOOL OF CHOICE.

Not to mention, LogStream can use databases such as the GeoIP database from MaxMind to do lookups of IP addresses and identify where they're coming from, which provides context. For instance, consider a SecOps team tasked with keeping a close lookout for any kind of interactions from China or Russia. From an operational standpoint, this becomes important when having an outage, for example. When using GeoIP information, it's easy to cluster the source of an outage in a particular region to gain better context.

5. Onboarding

Today, there are endless data sources in many different formats due to the rise of cloud, PaaS, etc. The typical SecOps team must dedicate significant time to write custom scripts, create a scheduling process, and write code to monitor data collection.

LogStream offers many ways to collect and receive data with prepackaged options, as well as the ability to extend and create inputs using the REST collector. With a small amount of code, users can schedule LogStream to reach out to another tool to pull data with an API. Collecting data is no longer an extensive custom development effort.

THREAT HUNTING

Data enrichment in LogStream enables the ability to hunt down threats more effectively thanks to the improved quality of data. LogStream's ability to enrich data as it is ingested empowers the threat team to find issues faster and with more accuracy. This capability puts less stress on the log analytics platform as well. LogStream has few limits on how it can use data to enrich events to power a more effective threat hunting operation.

INCIDENT RESPONSE

LogStream Replay also helps with recovery if a security attack takes place, allowing the SecOps team to understand what happened in greater detail. It's of course possible that data is incomplete, however, using Replay, the SecOps team can exhaust all possibilities. Otherwise, it would be necessary to
do a restore from tape, which is very slow or pay the cost of logging all data.

Incident response teams can use LogStream Replay to go into the object store, pull the full fidelity copy of a log, find the exact data in question, and analyze it using the tool of choice. Simply put, SecOps teams don't need such data practically 99.9% of the time. Being able to park a full fidelity copy in an object store allows for data on demand at the cost of the object store – not Splunk, for instance, which results in enormous cost savings.

By being able to control the data plane, incident response analysts can go into Replay, click a few buttons, and restore data rather than opening a ticket with the backup team and waiting for a response to restore data.

TO PRESENT THE BEST BUSINESS JUSTIFICATION FOR CRIBL LOGSTREAM, BE SURE TO TURN YOUR TECHNICAL REQUIREMENTS INTO CRITICAL-TO-FUND BUSINESS JUSTIFICATIONS, LIKE ANALYTICS PLATFORM COST SAVINGS AND DATA GOVERNANCE.

Conclusion: Key best practices for your budget request.

We understand the undertaking of presenting leadership with clear, concise business justifications for spending money on a new solution – or in this case, Cribl LogStream. You need to turn your technical requirements into justifications your business will recognize as critical enough to fund. Don't worry, we've done the work for you.

Below you'll find detailed examples you can use for your budget request:

- *Analytics platform cost savings*
  Enables engineering to precisely alter or drop the right data quickly using a rich user experience. Can reduce Splunk license utilization by 25% allowing greater data diversity within Splunk for the same cost.

- *Lower storage costs by leveraging low cost object storage*
  Enables sending raw data to lower cost storage, i.e. AWS S3 and then replaying data on demand into the analytics platform if access to data is required. Manage 12 months retention requirements in your object store instead of using your expensive storage for Elastic or Splunk. Can reduce storage costs by 25% depending on your use case.

- *Free up engineering time*
  LogStream's rich user experience streamlines and automates common BAU data management work. Average a 50% reduction in BAU admin work and use that time towards higher business value work.

- *Flexible Data Management*
  Supports numerous data sources and destinations such as Splunk S2S, HEC, Beats, and syslog. Flexible options for dropping, masking and transforming data using a rich user interface. Data independence that puts the customer in control of which tool receives your data.

- *Data Governance/Visibility*
  Gives governance and engineering teams complete visibility into the data flow and enables the ability to instantly drop, mask, tag or reroute data on-demand. Enable proactive data governance.

- *Unlimited Scale*
  LogStream can provide value with minimal systems resources and scale to thousands of cores as required. Its distributed deployment model can manage workers across the globe, on-prem or in the cloud.

ABOUT CRIBL

Cribl is a company built to solve customer data challenges and enable customer choice. Our solutions deliver innovative and customizable controls to route security and observability data where it has the most value. We call this an observability pipeline, and it helps slash costs, improve performance, and get the right data, to the right destinations, in the right formats, at the right time. Join the dozens of early adopters, including market leaders such as TransUnion and Autodesk, to take control and shape your data. Founded in 2017, Cribl is headquartered in San Francisco, CA. For more information, visit **www.cribl.io** or our **LinkedIn**, **Twitter**, or **Slack** community.