graylog

GRAYLOG KEEPS YOU SECURE

Category:
Security/SIEM

Industry:
Manufacturing/automotive

Looking For:
Real-time answers

Size:
5,000+ employees

Security breaches at companies of any size are more common than you might think. Companies with more than one office are at a higher risk of experiencing security breaches because of the distributed architecture. The key is finding them fast, stopping them, securing against them, and monitoring for any recurrences. Graylog Enterprise xxx

"... breaches that affect hundreds of millions or even billions of people are far too common. About 3.5 billion people saw their personal data stolen in the top two of 15 biggest breaches of this century alone."

Source: CSO Online

EXAMPLE SITUATION

- A manufacturing startup with seven branch offices (3 in the United States, 1 in Canada, 1 in the United Kingdom) in rapid growth mode discovers a system breach.
- The security breach's vector of entry, time of engagement, compromised assets, and technical ramifications are not clear.
- Resolving the breach requires swift, extensive, and accurate log analysis.
- There is no deployed solution to collect, monitor, or analyze log data in a central location.
- The distributed company architecture makes it harder to aggregate and analyze such data, much less normalize and correlate it across sites and IT components.

GRAYLOG IN ACTION

Graylog Enterprise is the solution of choice for companies that need to detect, respond, and hunt, fast when presented with a system breach.

SECURE YOUR SYSTEMS WITH REAL-TIME ANSWERS

A system breach is a common scenario that companies in every industry face. To resolve and prevent them, the IT team needs to know when it happened and what assets were likely compromised, and the person in charge wants to know the business and technical consequences of the breach.

Responding at the speed of business requires real-time answers and that is what you get with Graylog.

By aggregating all IT assets and logs into a single repository, offering different ways to view results and drill deeper for answers, Graylog makes threat hunting ridiculously fast, which is vital when faced with a system breach.

EXPLORE YOUR DATA WITH LOG AGGREGATOR

The threat hunt begins at the breach detection point but to get the real-time answers needed to stop a breach, you need to look at the data across your entire IT infrastructure. With seven branch offices and no idea of the entry point or severity of the breach, the fastest way to isolate the problem is by working with aggregated data. It is easier to parse and analyze – you can reduce the number of data points in a meaningful way and obtain the answer you need from them. Without aggregation, the raw amount of data makes log management an overly cumbersome process.

Graylog's platform uses a comprehensive procession algorithm to parse logs and search through virtually unlimited data. Solid centralized management assists all members of a team to scour through all relevant queries by defining permissions and roles.

DEEPER ANALYSIS WITH SEARCH WORKFLOW

Incident investigation requires a deeper log analysis to gather more details on the root of the problem. This becomes more important when in an IT Infrastructure with multiple globally distributed hosts as in the example above with seven countries (3 in the United States, 1 in Canada, 1 in the United Kingdom). For example:

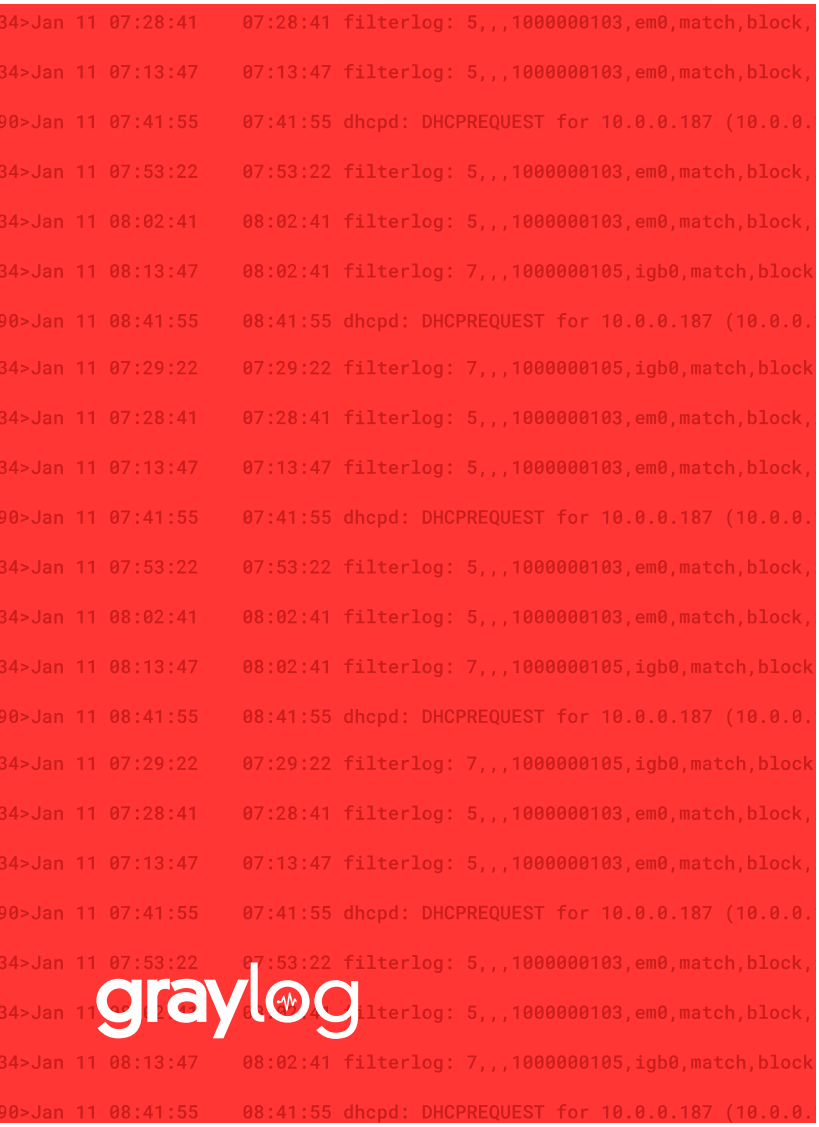
- If a data breach is detected at a particular host in Canada due to its excess CPU utilization, the next step is to run queries looking for similar utilization on all hosts at all sites in the other six countries.
- By drilling-down into the charts produced by the search workflow, the analysis revealed that the problem is limited to that particular host.
- A deeper log analysis uncovers information that is critical to resolving the breach such as the day the utilization increased, particular events of the day, and any associated compromises, then run similar queries and analyses on the other hosts to confirm the problem is isolated to the one in Canada.

Graylog Enterprise's parameterization, search workflow, and access controls make it easy for the experts to investigate a system breach across any type of IT infrastructure in any location, pinpoint the problem, and resolve it fast.

To keep your systems secure from future attacks, you can create a Dashboard to track the telltale metrics on a daily basis, and you can set up Alerts to let you know the instant a problem arises. Finally Graylog makes it easy to generate audit reports spanning all sites demonstrating the origin, scope, and impact of the breach as well as the steps involved in resolving it.

SUMMARY

A security breach requires the fastest and most comprehensive resolution possible. Graylog offers the most flexible and comprehensive approach to detecting, responding, and hunting immediate security breaches fast using . It offers a real-time solution needed to shut down any similar future breaches, address compliance issues fully, and satisfy executive requirements.



graylog

ABOUT GRAYLOG

Graylog is a centralized log management platform for companies seeking seamless data collection and normalization from any data source, faster analysis, and greater affordability. Purpose-built for modern log analytics, Graylog removes complexity from IT operations, data exploration, error tracing, and threat hunting so you can quickly and easily find meaning in data and take action faster. Our customers enjoy increased productivity, improved performance, secure systems, and an empowered team.

www.graylog.com
sales@graylog.com

1301 Fannin St, Ste. 2140
Houston, TX 77002