graylog

A+ SECURITY WITH GRAYLOG

Category:
Security Information & Event Management (SIEM)

Industry:
Education

Looking For:
Flexibility, Cost-effectiveness

Size:
250 Employees

K-12 Schools and school districts are increasingly relying on technology, with Chromebooks replacing physical books and online learning taking place both inside and outside the classroom. They are adding hardware and other devices to overloaded and under-resourced IT infrastructure at a rapid pace to support the burgeoning needs of the district ranging from administration to the classroom. Adding to the burden is a lack of preparedness for security breaches that can accompany rapid expansion.

"Bottom line: we're still in the learning business, we're not in the technology business," she [AJ Phillips] said. "But my goodness, technology can make us or break us."

Source: ***EdTech Focus on K-12***

EXAMPLE SITUATION

- K-12 school district with 1,900+ students
- The district relies on a robust technology infrastructure consisting of domain controllers, file storage servers, switches, high-density access points, etc.
- Plan to add Cloud-based storage in the upcoming year
- Detecting, containing, and mitigating security issues and the resulting impact is challenging with the different entry points from within and outside of the district
- Balancing budget management with requested technologies, desired student outcomes, and curricular demands presents a challenge
- Demonstrating the need for technology that supports the district initiatives is key to gaining support from school board members who often know very little about the technology presented to them
- The school board must track and report on the progress and outcomes of these investments, ensuring that taxpayer dollars are spent wisely
- Uses Cloud Apps like Infinite Classroom, Schoology, and Google Classroom to communicate with parents and students, report grades, provide learning materials, and manage assignments
- The District offers an entirely online High School

GRAYLOG IN ACTION

One of the main concerns in the district is cyber security and data privacy. Graylog Enterprise is the solution of choice for education and other non profit organizations that need a fast and cost-effective way to collect and analyze log data for use in detecting and investigating security incidents.

SECURE YOUR SYSTEMS WITH REAL-TIME ANSWERS

One of the main concerns in the district is cyber security and data privacy. Graylog Enterprise is the solution of choice for education and other non profit organizations that need a fast and cost-effective way to collect and analyze log data for use in detecting and investigating security incidents.

Luckily Graylog makes threat hunting ridiculously fast, which is vital when faced with a system breach.

For example, the entire school district was recently upgraded with Meraki Cloud Based high density access points. Also, all switches were upgraded with Cisco branded edge switches. During the summer of 2019, file storage and domain controllers were all virtualized into a cluster environment which allows for stability, and provides redundancy to help guard against data loss or loss of access. Any one of these devices can be compromised if they were not configured properly. Unfortunately, this was the case with access points, which were not configured and properly locked down.

Virtual learning is a high profile environment, so the IT team set up a Dashboard to monitor it 24x7 Dashboard included es. The number of current connections is one of the things they were monitoring. When the call came in that students were denied access upon logon. The IT admin checked the Dashboard and noticed a number of authentication errors with the domain controller.

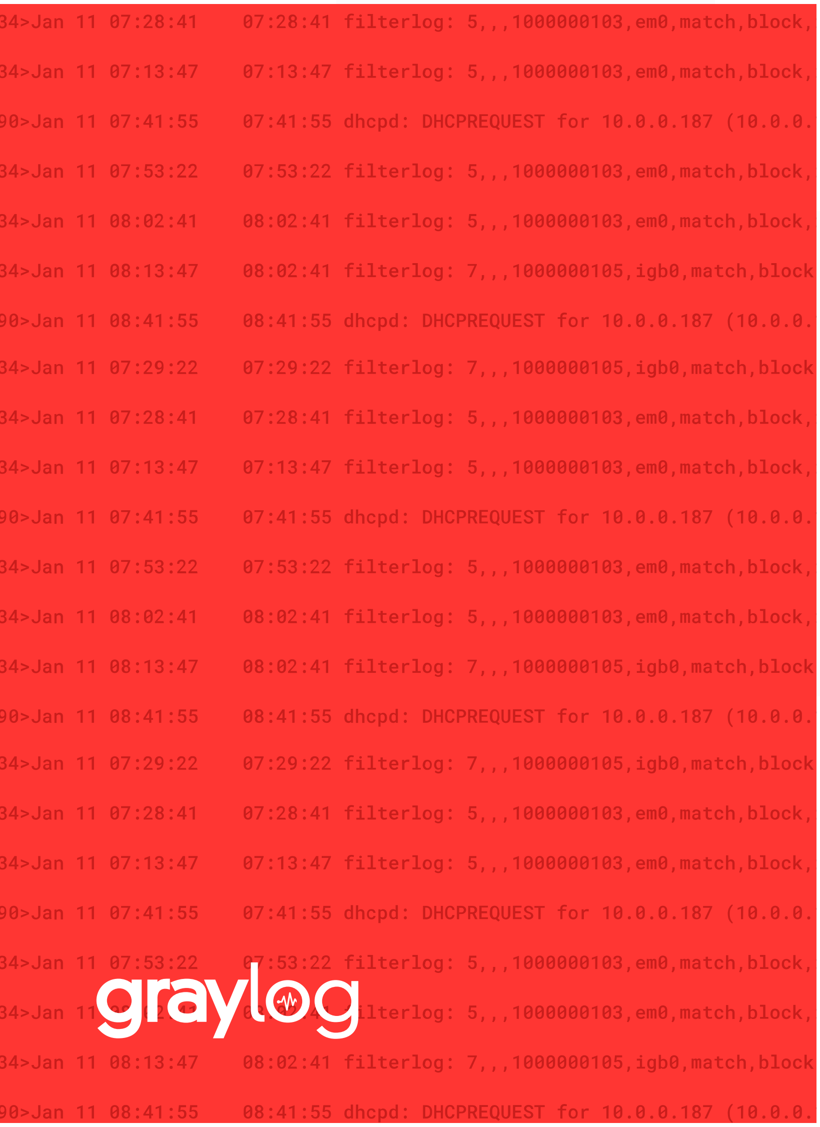
Graylog Enterprise’s parameterization, search workflow, and access controls made it easy to gather more details on the root of the problem. Starting from the domain controller widget on the Dashboard, the admin was able to quickly drill into the data and trace the issue to the wireless access points and identify the misconfigured device and resolve the issue.

MAINTAINING SECURITY WITH CORRELATION ALERTS

To keep the school district’s systems secure from future attacks, the admin created a network health monitoring dashboard to track the telltale metrics on a daily basis along with a correlation alert to trigger for any detected configuration changes or logins that appear to be from unknown locations or locations outside of the typical school district.

SUMMARY

When it comes to making decisions about technology—or any other expenditures, for that matter—it's important for school board members to be in a good position to explain it to the public and encourage a larger community conversation about it. Graylog's proven threat-hunting capabilities and its power to address operations challenges, the school board came to understand the site-wide power of Graylog's enterprise edition to optimize log management on a holistic level.



```
34>Jan 11 07:28:41    07:28:41 filterlog: 5,,,1000000103,em0,match,block,
34>Jan 11 07:13:47    07:13:47 filterlog: 5,,,1000000103,em0,match,block,
90>Jan 11 07:41:55    07:41:55 dhcpd: DHCPREQUEST for 10.0.0.187 (10.0.0.
34>Jan 11 07:53:22    07:53:22 filterlog: 5,,,1000000103,em0,match,block,
34>Jan 11 08:02:41    08:02:41 filterlog: 5,,,1000000103,em0,match,block,
34>Jan 11 08:13:47    08:02:41 filterlog: 7,,,1000000105,igb0,match,block
90>Jan 11 08:41:55    08:41:55 dhcpd: DHCPREQUEST for 10.0.0.187 (10.0.0.
34>Jan 11 07:29:22    07:29:22 filterlog: 7,,,1000000105,igb0,match,block
34>Jan 11 07:28:41    07:28:41 filterlog: 5,,,1000000103,em0,match,block,
34>Jan 11 07:13:47    07:13:47 filterlog: 5,,,1000000103,em0,match,block,
90>Jan 11 07:41:55    07:41:55 dhcpd: DHCPREQUEST for 10.0.0.187 (10.0.0.
34>Jan 11 07:53:22    07:53:22 filterlog: 5,,,1000000103,em0,match,block,
34>Jan 11 08:02:41    08:02:41 filterlog: 5,,,1000000103,em0,match,block,
34>Jan 11 08:13:47    08:02:41 filterlog: 7,,,1000000105,igb0,match,block
90>Jan 11 08:41:55    08:41:55 dhcpd: DHCPREQUEST for 10.0.0.187 (10.0.0.
34>Jan 11 07:29:22    07:29:22 filterlog: 7,,,1000000105,igb0,match,block
34>Jan 11 07:28:41    07:28:41 filterlog: 5,,,1000000103,em0,match,block,
34>Jan 11 07:13:47    07:13:47 filterlog: 5,,,1000000103,em0,match,block,
90>Jan 11 07:41:55    07:41:55 dhcpd: DHCPREQUEST for 10.0.0.187 (10.0.0.
34>Jan 11 07:53:22    07:53:22 filterlog: 5,,,1000000103,em0,match,block,
34>Jan 11 08:02:41    08:02:41 filterlog: 5,,,1000000103,em0,match,block,
34>Jan 11 08:13:47    08:02:41 filterlog: 7,,,1000000105,igb0,match,block
90>Jan 11 08:41:55    08:41:55 dhcpd: DHCPREQUEST for 10.0.0.187 (10.0.0.
```

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