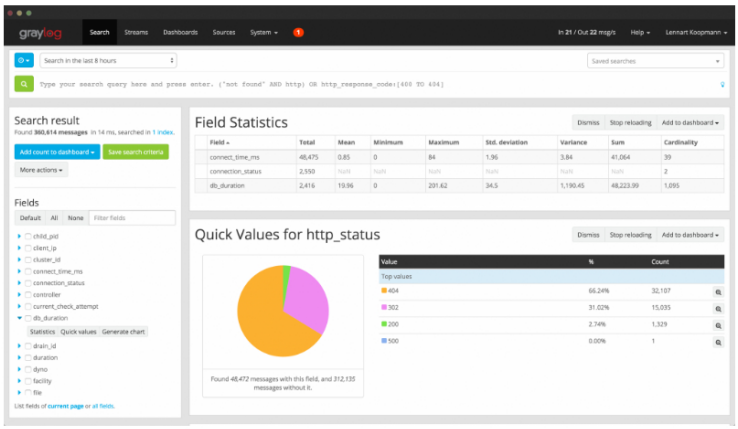
SIEM Platforms

This lessons is designed to provide you with an insight into the different SIEM platforms on the market. We will explore the different platforms, their capabilities, strengths and weaknesses. We will also introduce you to the platform we will be using in this course to teach SIEM skills, Splunk.

GRAYLOG

https://www.graylog.org/

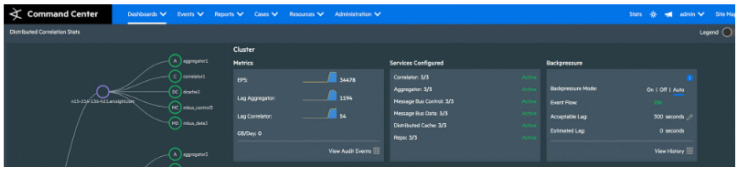
Graylog offers two different SIEM products, Graylog Open Source which is 100% free, and their paid-for product, Graylog Enterprise. If you want to download and play around with Graylog Open Source you can download it here. Graylog Enterprise has a free limit and can be used by small organizations that process less than 5 GB worth of events per day. Below is a screenshot of a search page within Graylog, giving you an idea of how the platform looks.

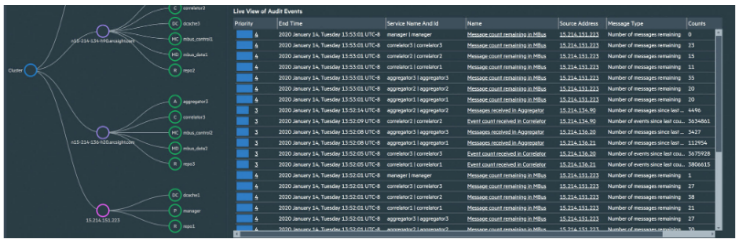


ARCSIGHT

https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview

ArcSight (with their SIEM ArchSight, also referred to as ArcSight Enterprise Security Management, or ESM) states that it can help SOCs to build out a layered analytics approach by integrating with a wide range of commercial security tools, and offers Security Automation and Response (SOAR) workflows to provide an automated response to security events, leaving analysts to focus on more important investigations. Powerful real-time correlation within ArcSight claims to be the fastest way to detect threats from large datasets.





QRADAR

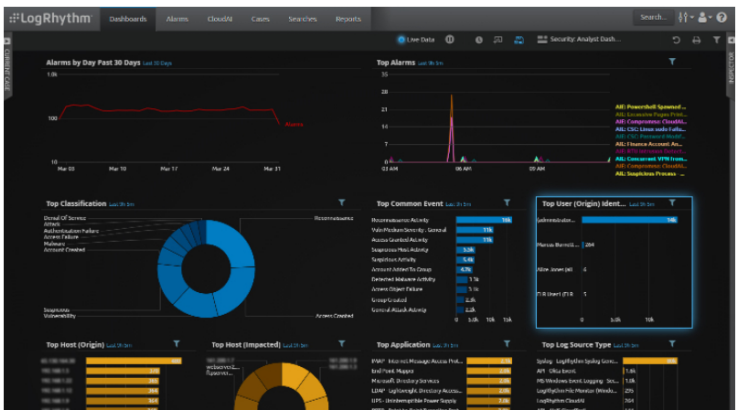
https://www.ibm.com/uk-en/security/security-intelligence/qradar

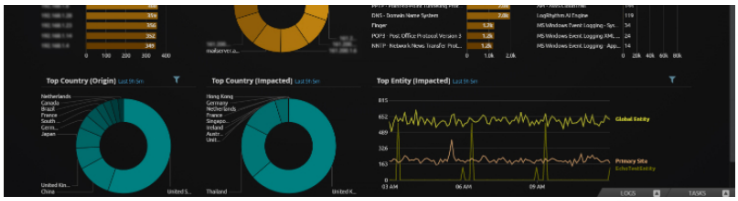
In addition to basic SIEM capabilities, QRadar SIEM also offers the ability to import data from threat intelligence feeds. When purchasing QRadar, clients can also opt-in to subscribe to the paid-for IBM Security X-Force Threat Intelligence, which identifies malicious indicators, which can be used to provide investigation enrichment, or for immediate alerting. Additional modules exist for QRadar that can assist security teams with incident response, risk management, and vulnerability management.

LOGRHYTHM

https://logrhythm.com

LogRyhthm boasts some pretty impressive features, such as machine learning, Security Automation and Response (SOAR), End-Used Behavioural Analytics (UEBA), and Network Detection and Response (NDR) to give unmatched environment visibility and response capabilities, directly from the SIEM platform. LogRhythm also states that *"you'll easily baseline your security operations program and track your gains — so you can easily report your successes to your board"*, which does indeed sound like a useful and efficient way to generate metrics and prove to executives that we really do protect the business, every single day.

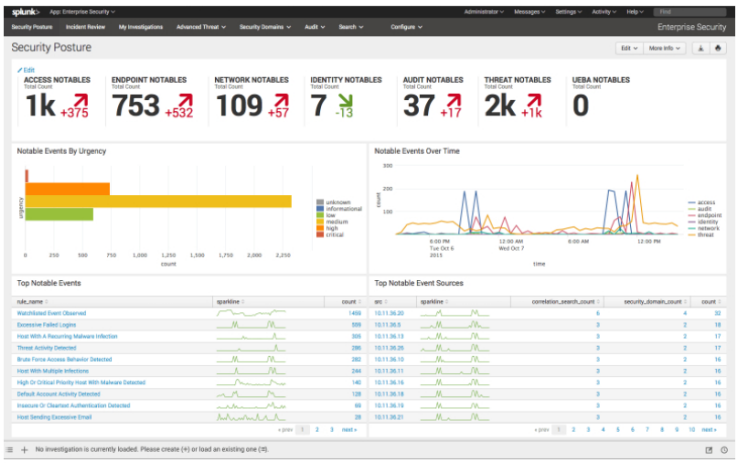




SPLUNK

https://www.splunk.com/en_us/platform.html

Splunk is one of the most popular SIEM platforms in the industry. SIEM administrators can download and add "Apps" that provide additional functionality to Splunk, such as analytics, dashboards, improved searching, and data manipulation. Imported data can be searched using custom-written search queries, which can also be used to generate alerts, and create visual dashboards.



Previous Topic | Mark Complete | Next Topic

Back to Lesson