splunk>

CASE STUDY

Maastricht University Saves Weeks of Manpower and Delivers Improved Services

Maastricht University

Executive summary

Maastricht University (UM) is a public university in Maastricht, the Netherlands and one of the top 100 universities worldwide, according to the Times Higher Education World University rankings. Having to manage nearly 400 different IT systems per day made it challenging for UM to investigate security incidents such as phishing or ransomware attacks. UM needed a product that could handle gigabytes of machine-generated data per day. Since deploying Splunk Enterprise, UM has seen benefits including:

- Improved security through anomaly detection
- Increased visibility into IT operations
- Improved user experience from reduced blacklisting

Why Splunk

Phishing campaigns would typically penetrate at least one account successfully out of UM's 50,000 email users, and then proceed to send spam and new phishing mails using UM resources. Slow troubleshooting when this occurred resulted in UM mail servers getting blacklisted as the team was unable to tackle the problem in a proactive fashion. In order to speed up the troubleshooting process, UM tried a number of different solutions, including centralizing the log data, using a number of open source products and experimenting with building its own solution. However, the volumes of data coming from disparate sources slowed everything down and made searching difficult.

UM was recommended Splunk Enterprise by partner SMT, and it is now used by the sysadmins in the UM server management, workplace and networking teams to monitor system health and search and investigate security incidents. UM is sending all the data from its numerous applications—including VPN, web servers, firewall logs and VNS logs—into Splunk Enterprise. UM runs two Splunk indexers with a single search head sitting on top. The initial indexer was used by the security team; when other UM teams learned what Splunk software was delivering from a security perspective, they also wanted access.

Industry

- Higher education

Splunk Use Cases

- Application delivery
- Security
- IT operations

Challenges

- Difficulties investigating when an attack had taken place due to numerous different IT systems
- Slow troubleshooting for phishing mails
- Needed a product that could handle gigabytes of machine-generated data per day
- Multiple man hours spent dealing with phishing attacks and blacklisting by email providers

Business Impact

- Weeks of manpower saved by more proactive security approach, enabling immediate identification and resolution of issues
- Better service delivered to the university's staff and students
- Stronger security through the ability to baseline normal and spot the anomalies that could indicate a threat
- Greater visibility into IT system health, resulting in a smoother, automated update process

Data Sources

- Application data
- VPN logs
- Web server data
- Firewall logs

Splunk Products

- Splunk Enterprise

Improved security by identifying anomalies

Splunk software makes it easy for the UM team to spot when something unusual happens because they now have a better understanding of what "normal" looks like across the environment. This enables the university to investigate any suspicious activities in student and staff accounts. Examples of how this works in practice include monitoring important groups in Active Directory so that if an account is added to the domain admins group, it triggers an email alert; monitoring access to important or sensitive mailboxes for any unauthorized access; and monitoring for abnormally large volumes of mail to one inbox, which could indicate abuse.

Increased visibility into IT operations

With Splunk Enterprise, UM is able to gain a better insight into the state of its IT environment. For example, when Windows XP came to the end of its support, using Splunk software enabled the university to get a view of the number of Windows XP machines in the network and correlate them to their owners. In addition, UM moved from manually updating its Windows environment to using the Windows software update service. The team now has visibility into the patching status, with pie charts showing the progress of updates in real time, and can identify if there are patches missing. This wasn't possible before the Splunk deployment.

Delivering better service to UM's users

Successful phishing attacks resulting in regular blacklisting of UM's servers by email providers meant that the university's staff and students would sometimes have trouble sending mails to external mail services like Hotmail or Yahoo! for days at a time. Splunk Enterprise has allowed UM to spot patterns and determine the attributes of a phishing attack, even if it's an unknown threat. These attributes trigger an alert so that the team can deal with the attack quickly and efficiently. Not only does the new approach to phishing attacks mean that blacklisting rarely occurs, the team is also able to react proactively to other common issues such as users getting locked out of their accounts. Whenever this happened previously, it was an extremely time consuming process for the team to identify the root cause and solve the problem. Splunk Enterprise has made that not only possible, but easy.

"Splunk Enterprise has helped us tackle phishing attacks so we are no longer blacklisted by email providers. Not only can we now deliver an uninterrupted service to our users, but we've saved weeks of manpower."

System Administrator
Maastricht University

The insights that UM gets from Splunk software have enabled the sysadmin team to provide improved service for users, while saving a huge amount of time. UM's sysadmins used to spend countless man hours dealing with phishing attacks and the subsequent blacklisting by email providers, as well as investigating and resolving user issues. The ability to address issues proactively has saved weeks in manpower, freeing up the sysadmin team's time to be more productive elsewhere.