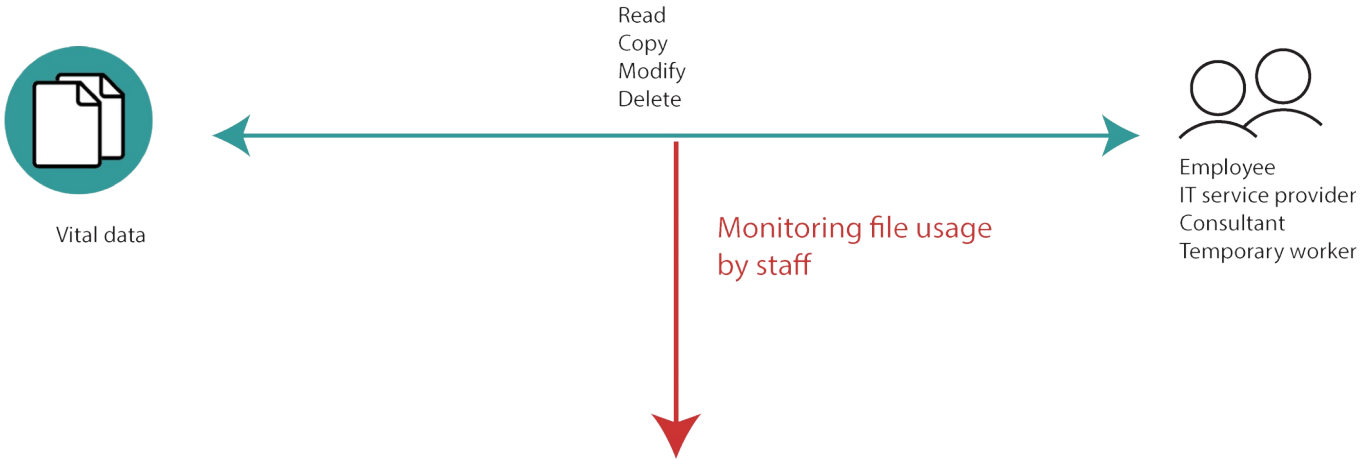
ing. Aukje Weening

VDSS and Security by design

VDSS Features

- Monitoring important and / or sensitive data
- Real-time
- Quarantaining ransomware
- Reports for management
- Fast implementation
- Scalable and affordable
- Dutch quality product

Staff



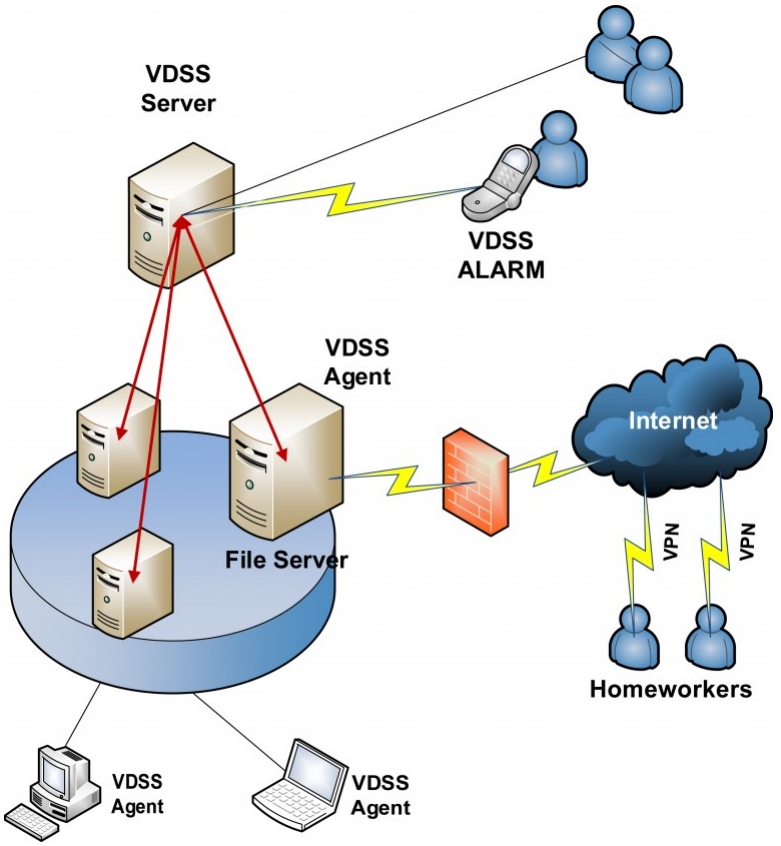
	2021-06-07 14:19:14	fileserver	Mutated: C:\development\windmill_sea\base.dwg mutated by MICHAEL with C:\autocad.exe
O	2021-06-07 14:17:37	fileserver	Listed: C:\development\confidential\patent.txt listed by MICHAEL with C:\Windows\explorer.exe
O	2021-06-07 14:17:34	fileserver	Opened: C:\development\windmill_sea\base.dwg Opened by MICHAEL with c:\autocad.exe
O	2021-06-07 14:17:10	fileserver	Listed: C:\development\windmill_sea\base.dwg listed by MICHAEL with C:\Windows\explorer.exe
	2021-06-07 14:17:10	fileserver	Listed: C:\clients.xls listed by MICHAEL with C:\Windows\explorer.exe

VDSS: Keep track of your data

- Your data, your responsibility
- Monitoring for information and data security (ISO27001)
- Essential for CISO
- Tool for Data Protection Officer (DPO)
- Unique addition to workstation management
- Intrusion Discovery as addition to the well known IDS (SOC)

VDSS in a network

- Agent
- Server (SaaS, DMZ, LAN)
- TCP/IP communication
- No backdoors
- No internet is needed



2FA

Supporting information:

Two factor authentication (or multifactor authentication) consists of multiple factors of authenticating according to veridiumid.com.

Duo writes that there are five popular factors that users can identify with. It says that factors are pieces of information that a user can provide to verify his or her identity. The following five authentication factors are listed by duo: the knowledge factor, the ownership factor, the biometric factor, the time factor and the location factor

...

2FA

Situation:

When implementing VDSS, there is an increasing pressure/demand from the customer to deliver 2FA.

Research questions:

– *Can you list the pros and cons for each factor?*

– *Which factor(s) can we best use for this?*

– *Do you have further advice for us how we can apply 2FA?*

SaaS or Hybrid

Software as a service, often shortend to SaaS, is also sometimes called software on demand. This is software that is offered as an online service. The customer does not have to purchase the software, but, for example, concludes a contract per month per user. The SaaS provider takes care of installation, maintenance and management, the user approaches the software over the internet with the SaaS provider.

Literally translated, ***on-premises*** in English means “on site” or “on location”. So when something is on-premises, the system is completely in-house, the software and data run on its own servers. The customer is responsible for the safety, availability and management of the system.

....

SaaS or Hybrid

Situation:

Business software over the internet is becoming more and more popular. Virtually all major software vendors and IT integrators offer only online services under the name SaaS. This is accompanied by dangers, especially in the field of information security, SaaS presents the necessary challenges.

Research questions:

– *What is your opinion if a security supplier only delivers its solution as SaaS?*
– *Can you list pros and cons?*
– *What is your advice in this?*

SIEM

SIEM stands for Security Information & Event Management and combines information from all possible Security and Monitoring applications in your network and ensures that you get an overview as if it were just one application.

Available features of the current SIEM toolings on the market, after research are:

- Detect threats from within (monitoring)

- Monitoring and Alerting

...

SIEM

We are increasingly asked by customers whether we can also arrange Security Information & Event (SIEM) connections. In the current situation, links are created manually with external tools by executing scripts.

Before the integration of SIEM connections can take place, we need to know which functions need to be arranged.

Research questions:

– Prioritize the functions, according to MoSCoW methodology, for a SIEM seen from a cyber security function.

– Can a SIEM solution offer added value within your company? And why?

Get to work

- Each table max 5 persons.
- Three research questions.
- 7 minutes for each research question.
- Each research has a paper to fill in (with post-its/write down)
- Each research has additional information printed on paper.
- Need help… just ask :-)

2FA How we work

- One time password via GSM (TOTP variant)
- This is a known and secure way of authentication according to Portwise (2011). Implementing and maintaining this variant is relatively little work by using PyOTP from PyPI (2020). for the developers. Registering is easy for the user. However, typing an extra code every time can be seen as a nuisance. There are many free apps that the user can use to authenticate (Sabarinath, 2020).
- Finally, this way of authenticating is available offline. Neither the server nor the user needs the internet for this system to work (Robinson, n.d.).

SIEM What we are going to do

- The purpose of this research was to look at the best practical solution for Triangle Solutions. Based on a points system in the longlist, a selection has been made of two solutions that score highest on the desired requirements and functions, namely Splunk and qradar. By means of an extensive function comparison of these, we looked at what best suits Triangle Solutions.
- Splunk fits best with Triangle Solutions, and can therefore be used as the first SIEM solution that can be linked to become.

Saas or Hybrid how we work

- VDSS as SaaS model is cost-effective, reliable, and completely free of any ongoing technical participation from the user. There are many factors to determine if SaaS is an ideal model for your company.
- However, VDSS can also be installed on servers directly onto a company’s infrastructure. This type of setup is popular among corporations that have strict security and privacy policies requiring software to be installed internally on the company’s infrastructure. No internet connection is needed!