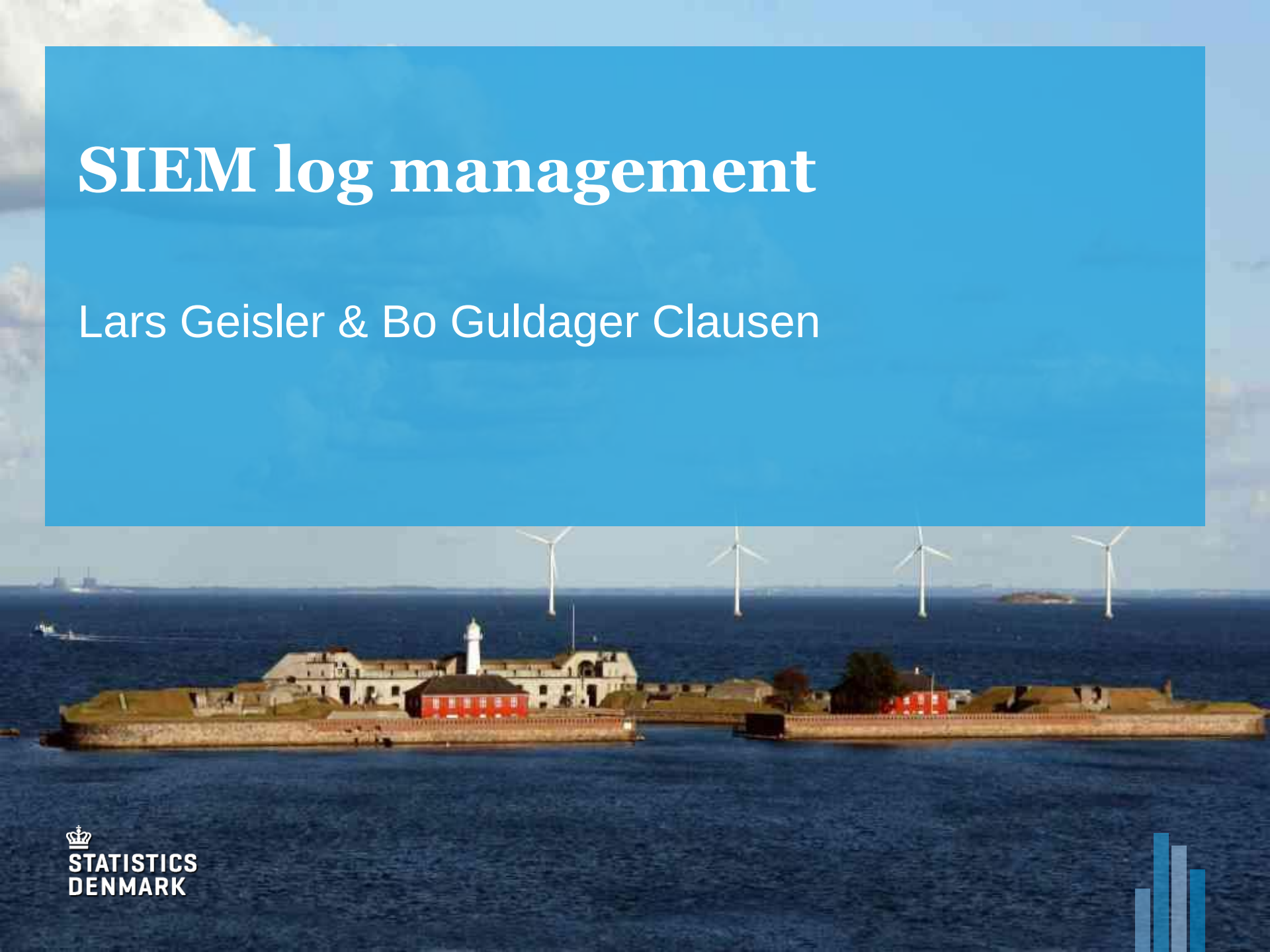
SIEM log management

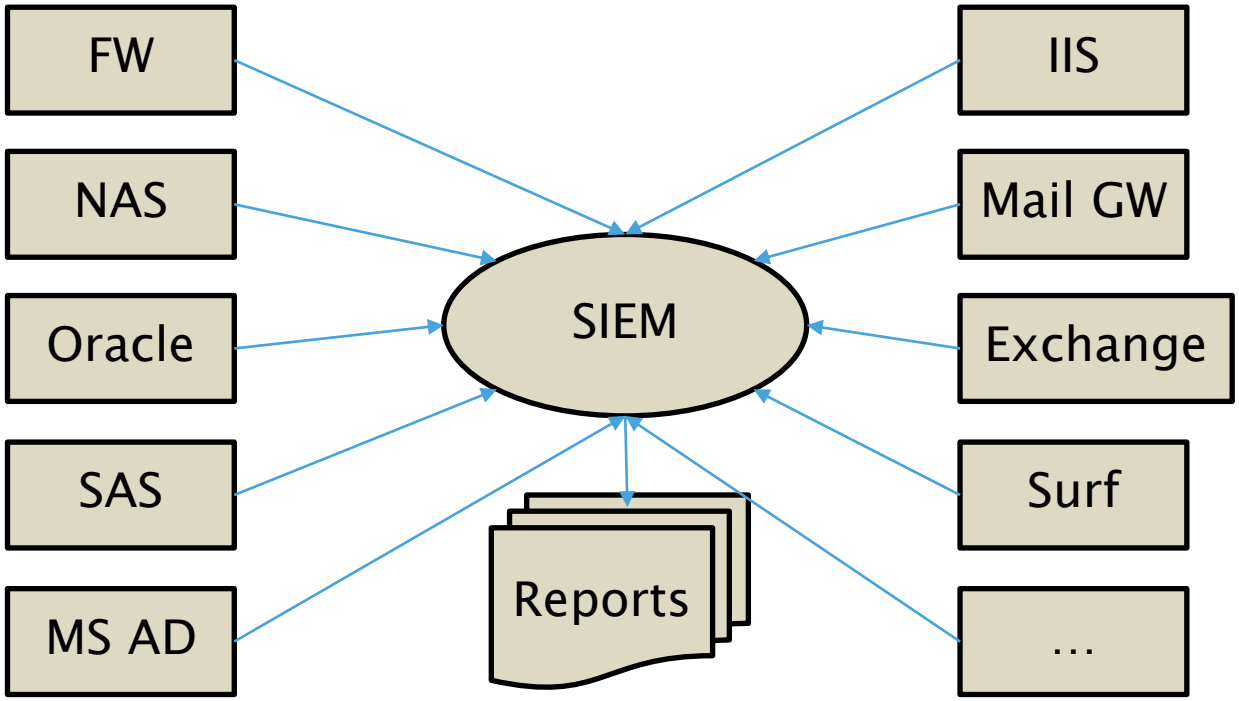
Lars Geisler & Bo Guldager Clausen



STATISTICS DENMARK

Security Information and Event Management

- Log consolidation from multiple sources
- Reporting on standard activities
- Combining logs from different sources
- Troubleshooting
  - Multiple logon – misconfigured Outlook
  - Internet use – misconfigured antivirus
  - Deletion of folders
  - …
- Logs are protected from deletion and changes
- Logs are stored for a predefined number of days


FW
NAS
Oracle
SAS
MS AD
SIEM
Reports
IIS
Mail GW
Exchange
Surf
…

Reports

- Internet use
- Mail
- Windows account operations
- Oracle
  - DBA activities
- Admin logins
- SAS dataset
- SAS CPR single search
- Future reports
  - Looking for abnormal behavior

Demos

- Reports
- Live demo