* Windows Security Package - Monthly Patching (about 25 hours): Every second Tuesday of the each month, retrieve the latest security patches from Microsoft for Windows, build the patching package for the different OS supported and qualify on virtual machines (Windows 7, Windows 10 IOT 2016 and 2019, Windows Server 2016 and 2019)
  + Prepare the patching package using WSUS Offline Community Edition
  + Qualify on virtual machines (Windows 10 IOT 2016 and 2019 and Windows Server 2016 and 2019). If time allows it, investigate the possibility to automate the build and qualify process in Azure
  + Update compliance scripts with the latest KB information
  + Publish patching package on SecurOT sharepoint
* Windows Security Package - Support & Development (about 20 hours) : Participate in the development of the hardening package by integrating new security controls (based on our threat monitoring) and support the sites in the troubleshooting and the implementation of fixes.
  + Examples of new features to implement : integrate winPEAS and Windows-Exploit-Suggester in inventory scripts, evaluate Pester as an alternative to Inspec, Kiosk Mode, …
  + Develop a methodology to measure the performance impact on HMI of the hardening controls
  + Contribute to the creation of training package for technical teams (procedure, video, …)
* Windows Security Package - Implement Agile Methodology based on Github (about 15 hours) :
  + Migrate the source code of the Windows Security Package from Sharepoint to Github
  + Define & build development environment based on Github
  + Implement Agile Methodology (including security by design, code analysis, …) for the development of the Windows Security Package
* Kudelski Incident Response (about 10 hours) : Coordinate the incident response based on tickets opened by Kudelski on the CFC portal for the EMEA and SEA region (between 5-10 tickets/month)