









Cybersecurity Specialist

Bart Busschots — September 2024

What do I Do?

-  **Respond** — react to alerts, respond to incidents, etc.
-  **Monitor** — keep a watchful eye on our systems
-  **Check** —measure (metrics), test & audit
-  **Maintain** — keep our defenses up and running at their best
-  **Learn** — always new trends, new risks & new technologies
-  **Enhance** — there's always room for improvement
-  **Engage** — in the department, in the university, with other universities, with national bodies, with companies ...
-  **Advise** — input to projects and decisions

What do we Protect?

- **Endpoints** — servers, PCs, tablets, phones ...
- **Identities** — accounts for people, devices & apps
- **Services** — Office365, learning systems, Student Records Systems, Finance Systems, HR Systems ...
- **Data** — emails, files, databases ...
- **Infrastructure** — campus network, data centre, cloud ...

From Who?

- **Cybercriminals** — steal money, steal data to sell, extortion ...
- **Hostile Governments** — espionage, sabotage ...
- **Activists** — publicity, sabotage ...
- **Insiders** — cranky staff or students, over-eager students ...
- **Opportunists** — notoriety (basic hacking tools are not hard to find)

With what Tools?

- **Security Operations Center (SOC)**
 - 24/7 monitoring by experts (in our case from the Netherlands)
- **Identity Protection** — conditional access, 2FA/MFA (*2/Multi Factor Authentication*) ...
- **Endpoint Protection** — evolved from traditional antivirus (AV)
 - Centrally managed and configured
 - Checks for more than just viruses (EDR – *Endpoint Detection & Response*)
 - Reduces risk — enforces settings & blocks risky behaviors (ASR – *Attack Surface Reduction*)
 - Responds to threats (the R in EDR)
 - Powered by AI
- **Infrastructure Protection (XDR – *Extended Detection & Response*)**
 - Monitors services (Office365, Active Directory, Entra ID, Azure cloud ...)
 - Automatically responds to threats (*SOAR — Security Orchestration, Automation & Response*)
 - Powered by AI
- **Network protection**
 - Firewalls — campus, data centre, cloud, servers ...
 - Security Appliances — WAF (*Web Application Firewall*), ADC (*Application Delivery Controller*), NGFW (*Next Generation Firewall*)
- **Central Logging** — a single pane of glass (SEIM – *Security Information & Event Management*)

Questions?