Why collaboration tastes like more.

During the course of many of SURFs journeys, various security incidents occurred. Early on we learned that collaboration is very important. Maybe it all started, over 30 years ago, with *SURFcert*. The Computer Emergency Response Team for education and research in the Netherlands. According to the brochure: 24/7 support from experts in case of security incidents. In which SURF works closely together with (members of) connected institutions. SURFcert helps to analyze and neutralize various types of DDoS attacks. We also learned the importance to share threat intelligence.

Knowing the power of collaboration, we later established *SCIRT* (the SURF Community of Incident Response Teams): working together to battle cyber security threats. Where we share information about current security challenges and exchange the latest tips and tricks between security experts. Over the years SCIRT proved to be a very active community. SCIRT works together with the platform for information security officers in higher education: *SCIPR*. SCIPR focuses on security policy and governance; SCIRT on operational matters. The areas of focus are very closely related to each other, and the number of touchpoints is increasing. As a result, cooperation is becoming increasingly close.

A very valuable source for security information has been “unused” IP-space (darknet). Which proved us last year with an excellent example of incident response and recovery. Due to an Emerging Threat: ransomware. Which will be briefly addressed in this presentation. However, recently one of our connected institutions drew our attention to the fact that this information source contained rather unusual traffic. Likely encoded DNS queries which seemed to have originated from oneself. Ignore or investigate?

The explanation of the potential threat required along the way a lot of collaboration. On European level, national level and within SURF and academics. Sometimes this went very smooth, sometimes it took more effort than expected. When we all could benefit from close collaboration. We will show all the various steps we took including the results and what we have learned from it.

One of the potential obstacles for collaboration sometimes seem to be perceived privacy obstacles. Can you have access to all available resources and can you share information with anyone? We will present two random examples within our community. The first one showing a rather long struggle, the other a much more pragmatic approach. Hopefully aiding to improved security for many.

In the end this presentation clearly demonstrates the miracles that can occur when everyone collaborates closely and works toward a shared goal.