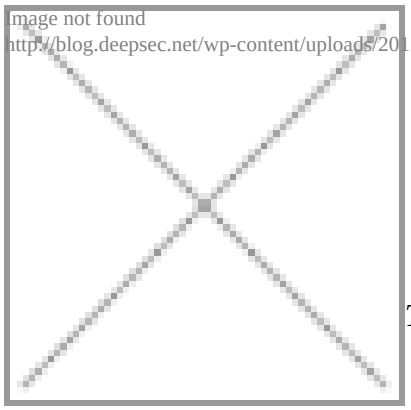
DeepSec 2017 Talk: OpenDXL In Active Response Scenarios – Tarmo Randel

Posted on **November 15,2017** by **sanna**

Automating response to cyber security incidents is the trend which is – considering increasing amount of incidents organizations handle and ever-increasing attack surface – already becoming mainstream. In this talk Tarmo explores the options of using OpenDXL in real life situation of mixed environments, legacy solutions and multiple vendors for connecting existing (and future) cyber security system components for coordinated information exchange and orchestrating incident response action.



Tarmo is a researcher at NATO Cooperative Cyber Defence Center of Excellence, various research projects and developing for large scale cyber exercises. He's also a developer at the Estonian eHealth Foundations, "Kickstarting" in-house development team. Tarmo's creating supporting infrastructure, preparations and execution of plans for taking over selected external vendor development projects. He's Head of Department at CERT-EE, Running Computer Emergency Response Team, Information security expert at CERT-EE, creating new tools and implementing existing to understand what is going on in networks. Tarmo's detecting and mitigating cyberattacks, analysing malware, planning and executing public awareness raising campaigns and supporting building trusted information security community network.

System administrator at Tele2 & Trigger Software, Converting legacy systems to modern, expandable high availability systems. Coding in PHP, C. Looking for and eliminating performance bottlenecks. Supporting development infrastructure.

Posted in:Conference | Tagged:DeepSec,Incident Response,OpenDXL,Talk | With 0 comments