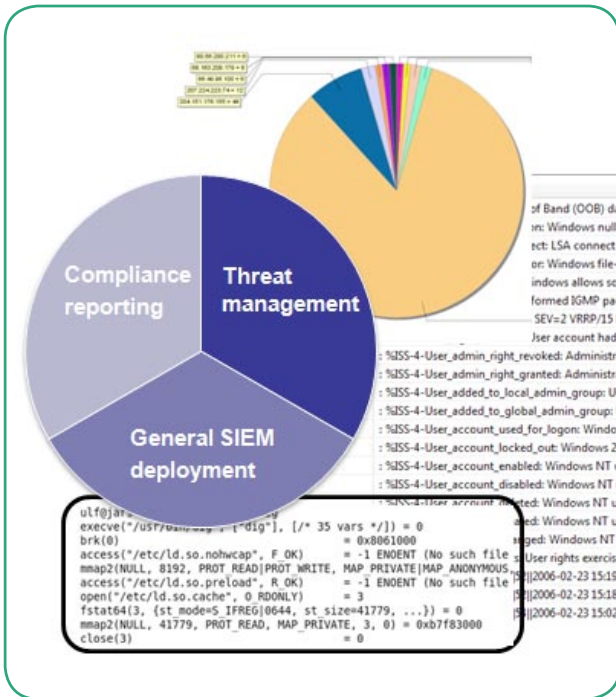


Log management and SIEMs – an overview



Log management, and in particular Security Information and Event Management systems (SIEMs) have received much attention in the last years. Prime reasons for this attention are ability to prove compliance with regulations, mitigating the loss of income from cyber attacks, and the ability to gather digital evidence to convict insiders.

In this talk, I will provide an overview of log management and SIEMs. I start off by describing the data life cycle from generation to disposal of data. I then focus on different variants of SIEMs, how they relate to the steps of the data life cycle and how they assist organizations in proving compliance and detecting attacks.

Finally, I will discuss some common problems with logging and provide some research directions.



Date: October 15, 11.30 – 12.30

Title: Log management and SIEMs – an overview

Speaker: Tekn. Dr. Ulf Larson, Omegapoint. The presentation will be held in English.

Location: Security Lab, Lindholmospiren 5, Göteborg

Registration: E-mail amalan@lindholmen.se no later than October 12. The seminar is open to all who have an interest in societal security and the use of information technology. The number of participants is limited. We offer a light lunch before the seminar.

Road description: Visit www.lindholmen.se

More information: Bo Norrhem, Lindholmen Science Park, E-mail: bo.norrhem@lindholmen.se, Phone number: +46 (0)31 764 70 25

Security Arena Lindholmen

Security Arena Lindholmen carries out research, methods and technology development applied to all phases of crisis management. Besides the research the work aims to conceptual development and pilot projects in collaboration between the industry, academia and end-users. This is a joint work between Lindholmen Science Park, Swedish Civil Contingencies Agency, Volvo, Saab, Ericsson and Chalmers. One of the goals is to spread knowledge about societal security and we are pleased to invite you to a series of free seminars about the research taking place at Security Arena Lindholmen.

Welcome!



LINDHOLMEN
SCIENCE PARK