# Article information:

Insider Threat Detection Using Log Analysis and Event Correlation - ScienceDirect  
<https://www.sciencedirect.com/science/article/pii/S1877050915004184>

# Article summary:

1. This article discusses the use of log analysis and event correlation to detect insider threats.

2. It proposes a probabilistic approach to illustrate the frequency of occurrence of events while still considering false alarm rate.

3. The article references various sources such as SimpleEventCorrelator, Log watch, SLAPS-2, A New Architecture for Managing Enterprise Log Data, Logsurfer, Swatch, SEC – A Lightweight Event Correlation Tool, LoGS, Towards Insider Threat Detection using Web Server Logs, SEC – Open Source and Platform Independent Event Correlation Tool, Splunk | IT Search for Log Management, Operations, Security and Compliance, Towards an information –theoretic framework for analysing intrusion detection systems, Extending UNIX System Logging with SHARP , The base-rate fallacy and its implications for the difficulty of intrusion detection , A Conceptual Framework for Network Management Event Correlation and Filtering Systems , Event Correlation Services – Designer's Guide , SMARTS , NerveCenter , Syslog Server | Syslogng .

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

The article is generally reliable in terms of its content. It provides a comprehensive overview of the use of log analysis and event correlation to detect insider threats. The article is well-referenced with multiple sources being cited throughout the text. This provides evidence that the claims made are supported by research from other sources. Additionally, the article does not appear to be biased or one-sided in its reporting; it presents both sides equally and does not promote any particular point of view or agenda. Furthermore, potential risks are noted throughout the text which adds to its trustworthiness and reliability.

The only potential issue with this article is that it does not explore counterarguments or provide evidence for some of its claims. For example, when discussing the proposed probabilistic approach there is no evidence provided to support this claim or any counterarguments explored as to why this approach may not be effective in detecting insider threats. Additionally, there is no discussion on how this approach could be improved upon or what other approaches could be used instead.

In conclusion, overall this article is reliable in terms of its content but could benefit from further exploration into counterarguments and providing evidence for some of its claims made throughout the text.

# Topics for further research:

* Probabilistic approach to detecting insider threats
* Counterarguments to log analysis and event correlation
* Alternatives to log analysis and event correlation
* Improving log analysis and event correlation
* Evidence for log analysis and event correlation
* Benefits of log analysis and event correlation

# Report location:

<https://www.fullpicture.app/item/3b4736ef8507c5276ecee48203f29316>