A Game-Theoretic Approach to Reducing Alert Fatigue in SIEM Systems

Graduate

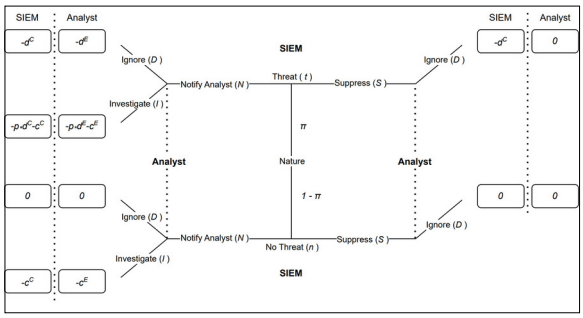
Severin Grimm

Initial Situation: The increasing frequency and complexity of cybersecurity threats have pushed organizations to depend heavily on Security Information and Event Management (SIEM) systems and Security Operations Centers (SOCs) to protect their digital infrastructure. However, the excessive volume of alerts generated by these systems, many of which are false positives, has led to a problem known as alert fatigue. This issue reduces analyst efficiency and increases the risk of missing critical threats.

Approach: This thesis explores the use of game theory as a solution to mitigate alert fatigue in SIEM systems. By modeling the interaction between SIEM systems and security analysts as a strategic decision-making process, the proposed framework evaluates incidents based on parameters such as signal quality, investigation costs, and potential damages. These parameters are used to determine whether an alert should be escalated to an analyst or suppressed.

Result: The results show that the framework effectively reduces false positives while maintaining the ability to detect critical incidents. This reduction in unnecessary alerts minimizes analyst workload and improves operational efficiency. This research demonstrates the potential of applying game-theoretic principles to real-world cybersecurity challenges, offering a practical tool to enhance the performance of SOCs and better support security analysts in managing increasing alert volumes.

Signaling Game
Own presentment



Strategy Matrix
Own presentment

	$\frac{\tilde{w}^C}{1-p} > \gamma_t$	$\frac{\tilde{w}^C}{1-p} \in (\gamma_n, \gamma_t)$	$\frac{\tilde{w}^C}{1-p} < \gamma_n$
$\frac{\tilde{w}^E}{1-p} > \gamma_t$	No Incident (Case 1)	No Incident (Case 1)	No Incident (Case 1)
$\frac{\tilde{w}^E}{1-p} \in (\gamma_n, \gamma_t)$	No Incident (Case 1)	Notify Analyst	No Incident (Case 1)
$\frac{\tilde{w}^E}{1-p} < \gamma_n$	No Incident (Case 1)	(Case 2)	Notify Analyst (Case 3)

Advisor
Dr. Daniel Tschudi

Co-Examiner
Dr. Christopher Portmann, Zürich, Zürich

Subject Area
Computer Science