Published: 01 April 2025
Online AM: 06 March 2025
Accepted: 03 March 2025
Revised: 24 February 2025
Received: 24 February 2025

INTRODUCTION

Introduction to the Special Issue on Incident Response

SAMUEL J PERL, Carnegie Mellon University, Pittsburgh, PA, United States

JEROEN VAN HAM-DE VOS, University of Twente, Enschede, Overijssel, Netherlands

THOMAS SCHRECK, Munich University of Applied Sciences, Munich, Bayern, Germany

Open Access Support provided by:

University of Twente

Carnegie Mellon University

Munich University of Applied Sciences

Introduction to the Special Issue on Incident Response

Background

The beginnings of coordinated internet security can be traced back to the late 1960s and early 1970s, when the first computer networks were developed and then further connected to form the ARPANET. In the early days, there was a relatively low level of security and fewer concerns about malicious users. Not long after, computers and networks became increasingly widespread. There was an explosion in the growth of connected devices, access to systems, connected networks, critical services, and sensitive data all being exchanged through inter-connected networks (the internet). A clear need to protect sensitive information and prevent unauthorized access has emerged.

One of the earliest recorded internet-wide security events took place in 1986, when a computer virus called the "Morris Worm" disrupted the operation of thousands of computers. Many network administrators were unprepared to deal with computer programs or users that deliberately affected file integrity, guessed passwords, or exploited vulnerabilities to disrupt systems. After the event, the community began exchanging lessons learned and preparing for the new eventuality of malicious users. This event also demonstrated the need for a coordinated approach to internet cybersecurity incidents. In the aftermath of the attack, DARPA asked the Software Engineering Institute to establish a computer emergency response team, which has come to be known as CERT coordination center.

The internet is a different place today. Many organizations now have their own dedicated **Computer Security Incident Response Teams (CSIRT)** to help perform cybersecurity operations including managing, responding to cyber incidents, and helping mitigate the impact of cyberattacks. The cybersecurity threat environment facing organizations has also changed dramatically [1]. CSIRTs are often responsible for coordinating within their organization and with outside groups and agencies to share information and resources about the threats they are facing, the methods they are using to combat those threats, lessons learned, experiences shared, assistance requested, and much more.

Despite this growth, academic research in the field of Incident Response has been relatively limited. Challenges to the research include (1) a lack of access to open data for evaluation, (2) overcoming many hurdles (including non-disclosure agreements) in obtaining and using sensitive security data, and (3) task performance or information exchange occurring without researcher involvement (if it happens at all).

However, as cybersecurity incidents continue to accelerate in both speed and impact on organizations, there are growing calls for traditional and interdisciplinary research approaches to the study and improvement of cybersecurity Incident Response. Research has historically come from the field of computer science and cybersecurity, but we feel there is great potential for incorporating and applying perspectives from other fields as well including philosophy, psychology, human computer interaction, business operations, law, and more. Managing incidents is the responsibility of the whole organization, and more teams are incorporating talent from traditional

ACM Reference format:
Samuel Perl, Jeroen van der Ham-de Vos, Thomas Schreck. 2025. Introduction to the Special Issue on Incident Response. *Digit. Threat. Res. Pract.* 6, 1, Article 1 (March 2025), 3 pages.
https://doi.org/10.1145/3722125

ACM 2576-5337/2025/3-ART1
https://doi.org/10.1145/3722125

functions such as legal departments, businesses, supply chain management, and more into their CSIRT and cyber operational teams.

We have some great contributions in this special issue.

Unveiling Cyber Threat Actors: A Hybrid Deep Learning Approach for Behavior-based Attribution. Attribution is a common challenge in incident response and can help steer the response. Ertan et al. have applied natural language and machine learning tools to perform automatic attribution based on the behavioral patterns of these threat actors. They show the accuracy of their methodology on different types of datasets with different levels of information, showing some promising results.

Automated ATT&CK Technique Chaining. The MITRE ATT&CK framework serves as a valuable resource for classifying adversary behaviors across different attack stages. However, it does not inherently provide insights into what most likely occurred before or after a given technique used by attackers. Eian et al. enhance the framework by introducing semantic analysis and open source tools that can better link the most likely stages of an attack, allowing incident responders to hunt for the most likely adversary's tactics first. By integrating semantic modeling of expert knowledge with data-driven techniques trained on real-world security incidents, their approach helps answer critical questions. Given an observed attack behavior, what technical changes most likely preceded it? and what are the most likely next steps for the adversary? This advancement improves threat analysis, enabling security teams to respond more effectively to cyber incidents by better anticipating, responding, and mitigating potential threats in real time.

FedNIDS: A Federated Learning Framework for Packet-based Network Intrusion Detection System. Network intrusion detection systems have traditionally been an important tool in the toolbox of an incident responder. Recently, **Deep Learning (DL)** capabilities have been applied in this context to great success. However, the DL approach can only be applied in a centralized solution, or at least one where the data processing can be done centrally. Nguyen et al. propose a decentralized approach based on federated learning, which has the added advantage that it can be tuned differently for different segments of a network. Different individuals, groups, and departments in an organization will frequently have different network baselines. There is no "one size fits all" network baseline. Decentralized network analysis research and new models to perform traffic analysis intend to reduce the number of false positives for incident responders.

On Collaboration and Automation in the Context of Threat Detection and Response with Privacy-Preserving Features. Nitz et al. examine the challenges organizations face in cybersecurity defense, particularly in the context of privacy-preserving collaboration. Through interviews with professionals from eight different organizations, they explore how privacy concerns impact the adoption of collaborative threat intelligence sharing and response automation. Their study highlights both the potential benefits and the obstacles associated with implementing privacy-preserving techniques in threat detection and Incident Response. To address these challenges, they propose a reference architecture for secure data sharing, aimed at improving collaboration while maintaining organizational and user privacy. Their findings provide valuable insights by outlining the specific current limitations, offering a foundation for future research and the development of more effective, privacy-conscious cybersecurity strategies.

Building a Better SOC: Towards the Ontology for Security Operations Center Assistance and Replication (OSCAR). **Security Operations Centers (SOCs)** play a crucial role in cybersecurity, yet there is no unified framework that comprehensively defines the key components required to develop an effective SOC. While various tools, strategies, and methodologies exist, they often address individual aspects rather than providing a holistic approach. Novak et al. aim to bridge this gap by proposing the **Ontology for SOC Creation Assistance and Replication (OSCAR)**. This ontology is designed to systematically outline the critical people, processes, and technologies involved in SOC development. Leveraging data-driven insights from cybersecurity experts through interviews and surveys, the research captures and structures decision-making processes, identifying how constraints impact

SOC implementation. By formalizing this knowledge into an ontology, OSCAR provides a structured and replicable framework that enhances our understanding of SOCs, facilitates more effective discussions, and supports organizations in building, assessing, and optimizing their security operations.

Samuel Perl
Carnegie Mellon University, Pittsburgh, PA, USA

Jeroen van der Ham-de Vos
University of Twente, Enschede, The Netherlands

Thomas Schreck
HM Munich University of Applied Sciences, Munich, Germany

Guest Editors

Reference

[1] Robin Ruefle, Audrey Dorofee, David Mundie, Allen D. Householder, Michael Murray, Samuel J. Perl. 2014. Computer security incident response team development and evolution. *IEEE Security & Privacy* 12, 5 (2024), 16–26. DOI: https://doi.org/10.1109/MSP.2014.89