Supporting Means-Ends Reasoning In Cybersecurity-critical Case Management Using Integrated Ecological Interface Design Process

Rohit Negi
Department of Computer Science and Engineering
Indian Institute of Technology Kanpur
rohit@cse.iitk.ac.in

Abhinaya Pranaikumar
Department of Design
Indian Institute of Technology Kanpur
abhinayap23@iitk.ac.in

Aparna Singh
Department of Design
Indian Institute of Technology Kanpur
aparnas23@iitk.ac.in

Vivek Kant
Department of Design
Indian Institute of Technology Kanpur
+91-721-985-1945
vkant@iitk.ac.in

Abstract. Case management plays a critical role in safeguarding organizations from potential security threats by providing comprehensive and real-time insights into system activities, user behaviours, and anomalies. Effective case management can be conducted by leveraging the importance of meaningful information design for effectively handling cases, using HMI design processes, such as Integrated Ecological Interface Design (iEID). The means-ends reasoning or practical reasoning of the analysts is first modelled using the abstraction decomposition space of iEID and is used as a basis for design ideations. Based on the insights of the field study and the Abstraction Decomposition Space (ADS) model, the information design and interface elements were developed. The interface uses a part-whole partitioning of information and supports the analyst's means-ends reasoning process. The paper demonstrates that human-centred design of security-critical systems is possible by using methods to design interfaces that support the analyst in the endeavour of case management in cybersecurity operations.

1 Introduction

In today’s digital era, the role of human-centric cybersecurity has become of great importance to safeguarding private and sensitive information in large organizations. The challenge in these setups is to understand how humans can be supported in these large systems through the appropriate design of information for successful cybersecurity practices. The article takes a Human Systems Integration (HSI) approach towards human-centric design. HSI is a branch of study that is “transdisciplinary, sociotechnical, and management approach of systems engineering to ensure that the system's technical, organizational, and human elements are appropriately addressed across the whole system life cycle, service, or enterprise system”

(INCOSE, 2023). One essential focus of HSI is to comprehend and design for complexity in a human-centric manner. The current article takes this approach by adopting a systemic methodology for interface design in cybersecurity practices (integrated Ecological Interface Design, iEID), which is amenable to HSI approaches of model-based systems engineering.

Ecological Interface Design (EID), and its latest instantiation of iEID, is an interface design process for designing interfaces in complex systems (Hajdukiewicz & Burns, 2017; Kant & Sudakaran, 2022). It has been successfully used for designing HMIs in complex sectors like defence, aviation, and healthcare (Bennett & Flach, 2019; Mulder et al., 2019). This EID process has also been used in cybersecurity as a sector (e.g., Bennett et al., 2018; Spero, 2023 for system security). In this current paper, we extend this ongoing direction of EID to the design of case management interfaces using iEID process from an HSI perspective. iEID is specifically suited to HSI focussed methodologies because it utilizes functional modelling to chart the elements required for the operator's decision making and then uses these for interface design. The focus is to use this human-centric functional model called the abstraction decomposition space to serve as the basis of the elements required for designing interfaces. Therefore, this modelling approach fits in with model-based systems engineering.

The major challenge in case management in cybersecurity is the assignment of the severity of a case and the way in which the decision is made. This requires an understanding of the various elements present in the system and the practical logic in which the security analyst makes these decisions based on cybersecurity rules as well as past experiences. Therefore, iEID serves as a good design process to handle the problem of case management using the Abstraction Decomposition Space (ADS), and the relevant reasoning is captured by modelling of means-ends reasoning or practical reasoning of the operators.

The paper comprises of five sections. Section 2 gives us details about the importance of case management and how it is carried out in operation centres. Section 3 details the iEID process used to develop the HMI. The article concludes with a discussion of iEID and future challenges that need to be addressed in the cybersecurity sector (Sections 4).

2 Case Management Systems

Case management plays a critical role in orchestrating responses to security incidents (Anastopoulos & Katsikas, 2017). In cybersecurity setups, various attacks and security incidents can be automatically captured in the form of logs. Cybersecurity analysts treat these various security incidents as individual cases to be analysed. The systematic collection and analysis of case logs in the field of cyber security can gain valuable insights into security incidents. These insights include and are not limited to unauthorised access and anomalous activities, which play a critical role in safeguarding organisations from potential cyber security threats. This proactive approach enables monitoring of the cybersecurity landscape, incident analysis, investigation, and auditing and reduces the risk of compromise (Anastopoulos & Katsikas, 2017; Donaldson et al. 2015).

The process of managing a case begins when initial alerts are consolidated by the system in the form of logs (Figure 1). These logs undergo stringent scrutiny, wherein they are first intercepted by the central firewall. Next, the incoming alerts serve as vital indicators for comprehending the compromised state of devices or assets within the network. This comprehensive analysis involves scrutinising log signatures, identifying unrecognised patterns, monitoring blocked IPs, examining phishing emails, and detecting bots. Depending on the severity of these cases, analysts either escalate the alert to form a case or discard it. However, case management is not simply a task involving classifying and filtering existing information about security attacks. A significant effort in terms of reasoning is required to conceptualise, categorise and act upon a case in these security-critical environments. Operators use means-ends reasoning or practical reasoning to formulate a case and then solve it. This reasoning process is supported by the functional modelling of the ADS.

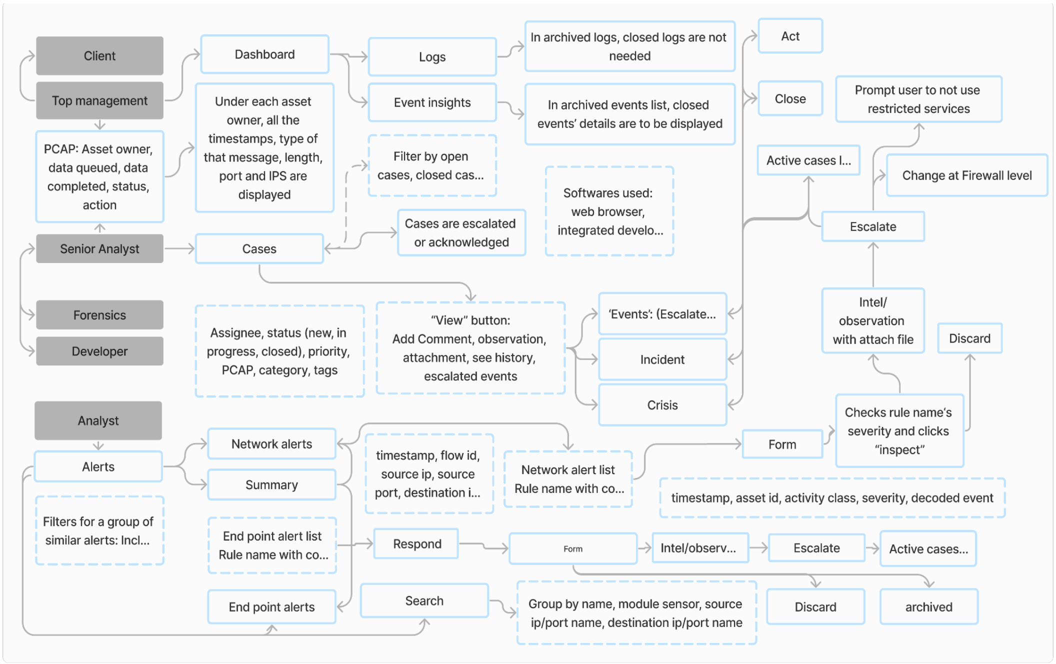

Client
Top management
PCAP: Asset owner, data queued, data completed, status, action
Senior Analyst
Forensics
Developer
Analyst
Alerts
Filters for a group of similar alerts: Incl...
Dashboard
Under each asset owner, all the timestamps, type of that message, length, port and IPS are displayed
Cases
Assignee, status (new, in progress, closed), priority, PCAP, category, tags
Logs
Event insights
Filter by open cases, closed cas...
Cases are escalated or acknowledged
In archived logs, closed logs are not needed
In archived events list, closed events' details are to be displayed
Softwares used: web browser, integrated develo...
"View" button: Add Comment, observation, attachment, see history, escalated events
'Events': (Escalate...
Incident
Crisis
Act
Close
Prompt user to not use restricted services
Active cases l...
Change at Firewall level
Escalate
Intel/ observation with attach file
Discard
Checks rule name's severity and clicks "inspect"
Form
Network alerts
Summary
End point alert list Rule name with co...
End point alerts
timestamp, flow id, source ip, source port, destination i...
Network alert list Rule name with co...
timestamp, asset id, activity class, severity, decoded event
Respond
Form
Intel/observ...
Escalate
Active cases...
Search
Group by name, module sensor, source ip/port name, destination ip/port name
Discard
archived

Figure 1. Operator's workflow (senior analyst and analyst were direct stakeholders, the rest were secondary stakeholders)

The Data Collection System, Data Storage System, Log Analysis and Alerting System, and Performance Analysis and Disaster Recovery System are the four sub-systems that make up the case management system. Applications, security appliances, and network devices are just a few of the sources from which the Data Collection System gathers logs and sends them to the central firewall, which plays a crucial role by allowing actionable alerts to enter the system while blocking others. Those alerts are then centrally stored for analysis by the Data Storage System. In order to ascertain the degree of attention required by the analysts, pertinent data based on severity score, rule category, or rule name is extracted. This attention may be directed towards preventing malicious conduct by escalating or discarding the case and remediating false alerts by editing the rules.

The analyst is displayed with an overview of the alerts and the alerts generated, as well as the details of the source and destination IP addresses, time, severity, and message. Based on the analysis done by the analyst, it can be either resolved, archived, or escalated to a senior analyst for further action. This dynamic between the analyst and the senior analyst is pivotal; the senior analyst, possessing more experience, may take direct action or reassign the case to another analyst by adding his observations on that case and If the case is severe, it is forwarded to forensics for an in-depth investigation. Both analysts and senior analysts can identify false alerts and add corresponding rules, though the senior analyst has the authority to edit rules added by the analyst. Conversely, rules added by the senior analyst cannot be altered by the analyst, who can, however, append notes for the senior's review. This hierarchy underscores that alerts are dealt with more cautiously and with attention to detail, which is overseen by senior analysts along with top management monitoring organization performance through alert statistics and the graph showing false positives plotted against rules added or modified fosters collaboration— creating an environment where security professionals work together on cases. This collaborative setting led by senior analysts enhances the organizational security and performance of the case management system by providing support analysts with regular interactions and feedback.

In order to efficiently handle these cases, an essential component is an HMI that avoids becoming overwhelmed with unnecessary or repetitive data (Johnston et al., 2003; Tantawy et al., 2020). The primary objective is to empower operators with comprehensive information to make informed decisions (Miloslavskaya, 2016). Numerous researchers in cyber security have focused on HMI, exploring the role of data logging in intrusion detection and emphasising the significance of cyber security in various domains. For instance, (Findrik et al., 2018; Choi et al., 2019) conducted a study for identifying cyber intrusions using Historical Data-based log comparison. Frigård, (2019) and Asghar et al. (2019) highlight escalating cybersecurity threats to industrial automation systems. Additionally, Fan et al., (2018) simulate accident scenarios in HMI safety analysis and Miller & Holley (2022) highlights the potential for human error in complex systems. These papers stress the importance of human factors countermeasures to reduce the consequences of cyber-attacks using HMI design, particularly in the context of centralised case management.

3 iEID Process for HMI for Case Management

3.1 Defining Scope and Understanding Work Domain

In order to design the interface, a field study was conducted, and the problem scope was formulated. The field study was conducted in a large cybersecurity operations centre that works in the research and development of cybersecurity operations. Along with developing cybersecurity applications, this organisation also provides consultancy solutions and policy recommendations to various organisations (both public and private). In all, we were closely involved with about five members of the case management team who were closely involved from the beginning to the end of the design project. In addition, other members of the organisation provided detailed insight into the broader functioning of cybersecurity as a sector. The field study consisted of observations and interviews and lasted for about two months, starting August 2023. The whole of the design process consisted of iterative work up till December 2023.

3.2 Conceptualising scenarios.

In this step, we list a few frequent scenarios as well as the ones that are non-frequent but are important. Frequent scenarios include,

- Initial process of generating alerts : The process begins by collecting logs from various sources, with the event type 'alert'.
- Dealing with cases generated from alerts : These alerts are analysed using its log metadata to either escalate it to the event type 'case' or discard it.
- Local rule addition : They are strategically employed to curtail the volume of alerts generated initially, aiding in minimising noise and emphasising the most critical alerts, thereby alleviating the analytical workload for security analysts. Based on the modified rule, the backend code may assign a updated severity score or rule name, or rule category or may even block a similar alert next time.

In addition, non-frequent scenarios includes,

- False positive : If the analysts analyses an alert as false positive ,they change the rules.
- System library update : When a new app is installed or updated, it may not be supported.
- Collection rate of logs : The source of the sudden increase or decrease in log collection rate are analysed.
- Change in log storage system : Can cause the system to malfunction and difficult to locate them.
- Overall action when system crashes : Utilising a monitoring system, the developer seeks to identify the causes and takes action during system crash.
- PCAP loss : When gathering logs, any delay in the process can impact the PCAP storage and analysis of alert is affected without its PCAP.

3.3 Developing the Abstraction Decomposition Space

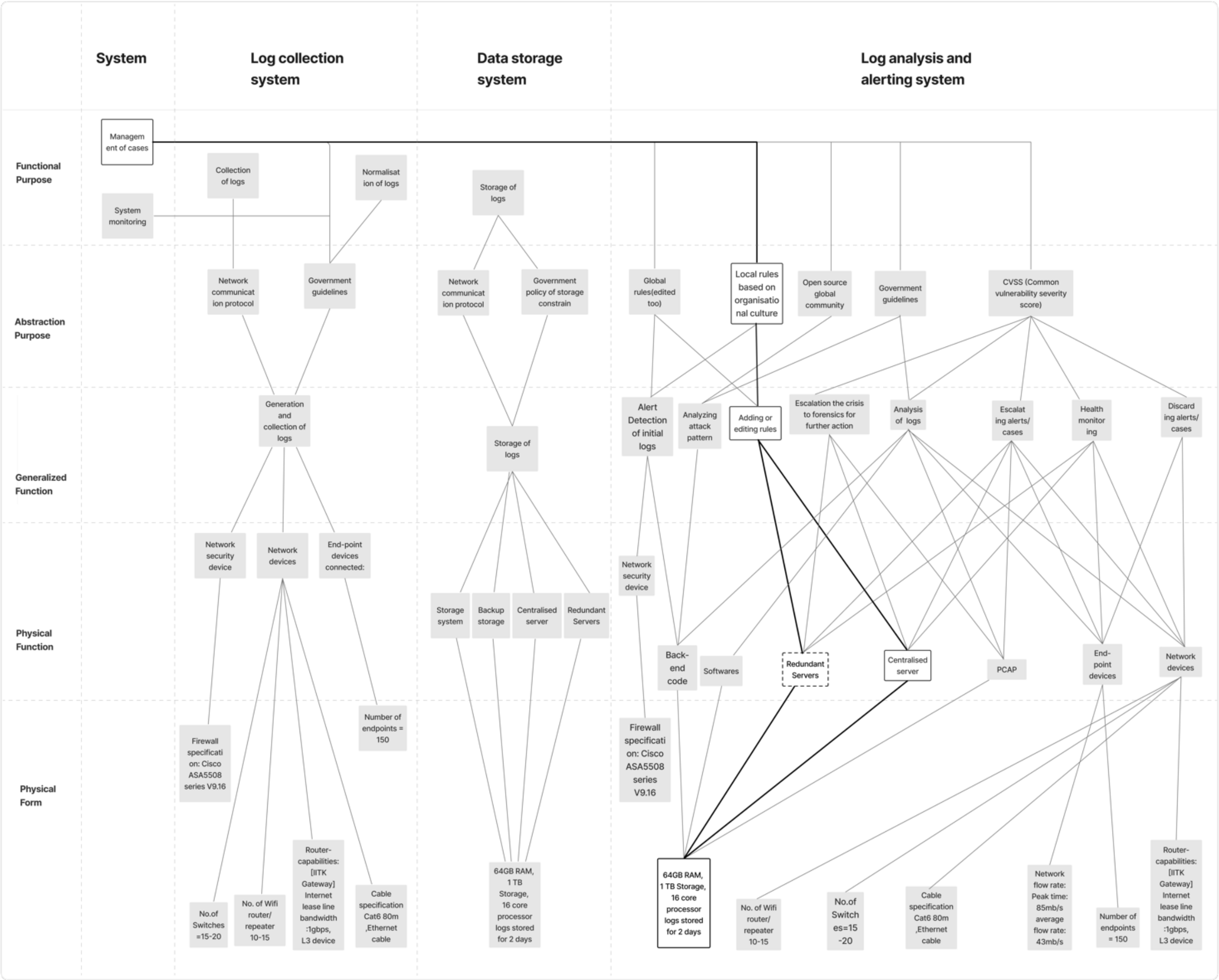

System
Log collection system
Data storage system
Log analysis and alerting system
Functional Purpose
Abstraction Purpose
Generalized Function
Physical Function
Physical Form
Management of cases
System monitoring
Collection of logs
Normalisation of logs
Storage of logs
Network communication protocol
Government guidelines
Network communication protocol
Government policy of storage constrain
Global rules(edited too)
Local rules based on organisational culture
Open source global community
Government guidelines
CVSS (Common vulnerability severity score)
Generation and collection of logs
Storage of logs
Alert Detection of initial logs
Analyzing attack pattern
Adding or editing rules
Escalation the crisis to forensics for further action
Analysis of logs
Escalating alerts/ cases
Health monitoring
Discarding alerts/ cases
Network security device
Network devices
End-point devices connected:
Storage system
Backup storage
Centralised server
Redundant Servers
Network security device
Back-end code
Softwares
Redundant Servers
Centralised server
PCAP
End-point devices
Network devices
Firewall specification: Cisco ASA5508 series V9.16
Number of endpoints = 150
No.of Switches =15-20
No. of Wifi router/ repeater 10-15
Router-capabilities: [IITK Gateway] Internet lease line bandwidth :1gbps, L3 device
Cable specification Cat6 80m ,Ethernet cable
64GB RAM, 1 TB Storage, 16 core processor logs stored for 2 days
Firewall specification: Cisco ASA5508 series V9.16
64GB RAM, 1 TB Storage, 16 core processor logs stored for 2 days
No. of Wifi router/ repeater 10-15
No.of Switches=15 -20
Cable specification Cat6 80m ,Ethernet cable
Network flow rate: Peak time: 85mb/s average flow rate: 43mb/s
Number of endpoints = 150
Router-capabilities: [IITK Gateway] Internet lease line bandwidth :1gbps, L3 device

Figure 2. Local rule addition scenario mapped onto the ADS. The transparent boxes show the main elements, whereas the dotted box shows the secondary elements involved

In this step, the Abstraction Hierarchy (AH), Decomposition Hierarchy (DH), and Abstraction Decomposition Space (ADS) were developed. The AH consists of five levels that address the system in terms of functional levels ranging from the purpose of the system to its attributes. The second DH addresses the system in structural terms, consisting of various subsystems and constituent elements. In this case, the various elements of the decomposition axis is the System (Case-management), Log collection subsystem, Data Storage subsystem, and the Log analysis and alerting subsystem. The AH and DH were put together as dimensions of a matrix to create the ADS and represent the system in human-centric terms of function and structure to address systemic complexity (Figure 2). Next, these models were tested for completeness by mapping the scenarios on to them. These models were also discussed with the log management team to ensure that they were correct and complete. ADS (Figure 2) also helped to understand the complex relationships between different functional and structural elements. In this ADS, the *local rule addition scenario* is mapped to show how the various elements are interrelated and what elements are involved when the analysts address that case.

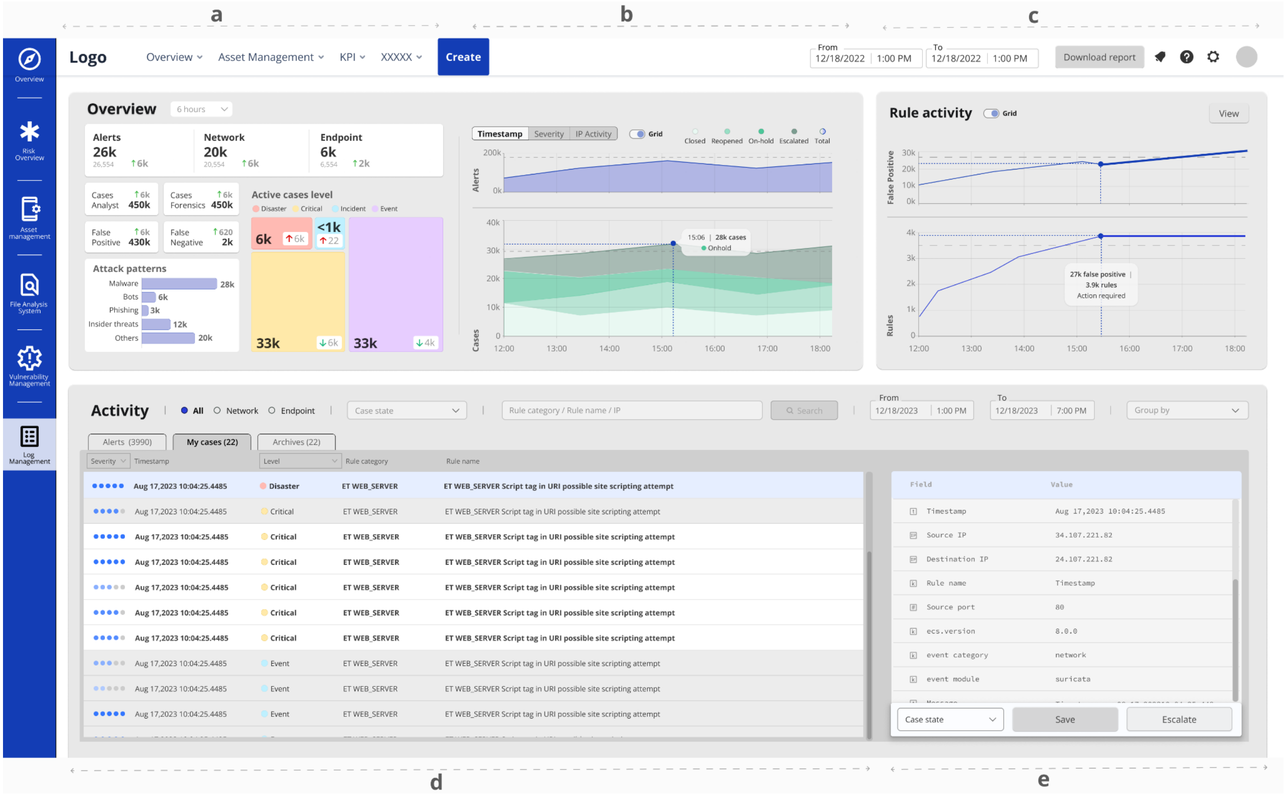
3.4 Interface Design

The rest of the steps of iEID consist of developing the preliminary design frames, developing wireframes, low-fidelity prototypes and finally integrating all the elements together to complete the final interface. Wireframes and the Information Architecture were created to turn the early conceptions into concrete representations of the user interface and were tested with Analysts and Senior Analysts. Feedback on the wireframes was received by the senior analyst and analyst.

After the wireframes, low-fidelity prototypes were created and user feedback was received on these low-fidelity prototypes. The next step involved creating the information design elements and represent them in light of the many elements, relationships, and restrictions of the domain received from the ADS. For instance, one of the critical purposes of the interface created is to improve the efficiency in taking action on an alert, despite dealing with a deluge of information. Therefore, information is incorporated in such a way that overall system is captured in a single display, along with temporal information, in the form of trends, that facilitate the analyst's functioning (e.g., Hancock & Szalma, 2003). The other purpose is to reduce the alerts generated to enable ease of operations. In general, the organisation constantly edits or adds rules for cybersecurity based functioning. During the steps of scenario development and the ADS creation, an important relationship between the rule addition and false positives was found. This relation is represented in (Figure 3, Region c) of the interface.

After deciding on the informational elements, the interface components were designed. The focus of the interface was to present all the necessary information and designed in a way where they can take actions on the case swiftly by both the analyst and the senior analysts. The senior analyst had access to more information and had a larger locus of control than the analyst. For example, along with all the elements that the analyst has, a senior analyst also has a count of escalated cases to forensics and analysts. Further, the senior analyst has the access to edit a number of cybersecurity rules directly but analysts do not have the ability to do so and they have to take permission to edit the rules added by the senior analysts. Here for the sake of ease, we are demonstrating the senior analyst screen and the various steps by which they were the formulation thereof (Figure 3).

In Senior Analyst Overview page, the Overview stats is depicted on the top left corner, helping them to make more informed decisions about what to take action on (Figure 3, Region a). Statistics includes the count of cases escalated to analysts, forensics and count of cases occurred in different types of attack patterns. The overall cases and alerts that the system receives are plotted as an area graph against three factors of severity scores, timestamp and IP address locations shown in world map (Figure 3, Region b).



Severity	Timestamp	Level	Rule category	Rule name
●●●●●	Aug 17,2023 10:04:25.4485	Disaster	ET WEB_SERVER	ET WEB_SERVER Script tag in URI possible site scripting attempt
●●●●○	Aug 17,2023 10:04:25.4485	Critical	ET WEB_SERVER	ET WEB_SERVER Script tag in URI possible site scripting attempt
●●●●●	Aug 17,2023 10:04:25.4485	Critical	ET WEB_SERVER	ET WEB_SERVER Script tag in URI possible site scripting attempt
●●●●●	Aug 17,2023 10:04:25.4485	Critical	ET WEB_SERVER	ET WEB_SERVER Script tag in URI possible site scripting attempt
●●●○○	Aug 17,2023 10:04:25.4485	Critical	ET WEB_SERVER	ET WEB_SERVER Script tag in URI possible site scripting attempt
●●●●○	Aug 17,2023 10:04:25.4485	Critical	ET WEB_SERVER	ET WEB_SERVER Script tag in URI possible site scripting attempt
●●●●○	Aug 17,2023 10:04:25.4485	Critical	ET WEB_SERVER	ET WEB_SERVER Script tag in URI possible site scripting attempt
●●●○○	Aug 17,2023 10:04:25.4485	Event	ET WEB_SERVER	ET WEB_SERVER Script tag in URI possible site scripting attempt
●●○○○	Aug 17,2023 10:04:25.4485	Event	ET WEB_SERVER	ET WEB_SERVER Script tag in URI possible site scripting attempt
●●●●●	Aug 17,2023 10:04:25.4485	Event	ET WEB_SERVER	ET WEB_SERVER Script tag in URI possible site scripting attempt

Field	Value
Timestamp	Aug 17,2023 10:04:25.4485
Source IP	34.107.221.82
Destination IP	24.107.221.82
Rule name	Timestamp
Source port	80
ecs.version	8.0.0
event category	network
event module	suricata

Figure 3. Senior Analyst overview page

By utilising the ADS, correlation between the addition of local rules and the occurrence of false positives (Figure 3, Region c) is identified and displayed. In the event of a false positive, analysts are prompted to modify the rules accordingly. A notable observation emerges when evaluating extended periods of increasing false positives; it suggests a potential correlation with the absence of recent rule modifications. This highlights the critical role of rule refinement in addressing false positives and underscores the significance of this relationship as a valuable metric for organisational performance analysis. Lastly, the activity area (Figure 3, Region d) has all of the alerts generated. When an alert is clicked, its metadata appears (Figure 3, Region e). Senior Analysts uses it to modify the alert's status or do additional analysis in order to elevate it or assign it to different Analyst.

Other pages not shown in Figure 3 but of interest to the senior analyst are the *Rules activity page* obtained on clicking ‘View’ button on top right corner (Figure 3,Region c) which can be used to modify the security rules. Further, clicking of the escalate button on the bottom right corner (Figure 3, Region e), navigates to *Inside Case page* which involves metadata and is used to examine interactions further. Based on all the elements discussed here the senior analyst is able to make decisions in order to support the activity of case management such that the threats are reduced and the cyberattacks can be successfully prevented by addressing them in a timely manner.

4 Discussion and Conclusion

The paper discusses the implementation of HMI for centralised case management system and emphasises the importance of system for analysing alerts and taking action to mitigate cyber threats. The study incorporates the iEID process to understand the system at a functional and structural level with more clarity to support analyst activities to give them more control over the system. The current interface was a concept interface and it was subjected to formative testing at each step of the design process within the members of the organisation. There is a need to conduct summative testing with a larger group of analysts to develop a generic marketable product. In addition to this, additional variables can be incorporated into the examination of the historical interactions originating from the source generating an alert. This can help in the comprehensive analysis and identification of attack patterns, thereby enhancing the capability to anticipate and mitigate future security threats. Further studies could focus on the development of advanced HMI systems that integrate artificial intelligence and machine learning to provide real-time insights and decision support for cybersecurity operations.

References

Donaldson, SE, Siegel, SG, Williams, CE & Aslam, A 2015, "Managing a Cybersecurity Crisis," *Apress eBooks*, accessed <https://doi.org/10.1007/978-1-4302-6083-7_10>.

Miloslavskaya, N. (2016, August 1). Security Operations Centers for Information Security Incident Management. https://doi.org/10.1109/ficloud.2016.26

Johnston, J M., Eloff, J H P., & Labuschagne, L. (2003, December 1). Security and human computer interfaces. Computers & Security, 22(8), 675-684. https://doi.org/10.1016/s0167-4048(03)00006-3

Findrik, M., Smith, P J., Quill, K., & McLaughlin, K. (2018, August 1). PLCBlockMon: Data Logging and Extraction on PLCs for Cyber Intrusion Detection. https://doi.org/10.14236/ewic/ics2018.12

Frigård, J. (2019, October 1). Security Information and Event Management Systems Monitoring Automation Systems

INCOSE (2023). INCOSE Systems Engineering Handbook, 5th Edition, 2023. ISBN-13 978-1119814290

You, Y., Lee, J., Oh, J., & Lee, K. (2018, January 1). A Review of Cyber Security Controls from An ICS Perspective. https://doi.org/10.1109/platcon.2018.8472757

Tantawy, A., Abdelwahed, S., Erradi, A., & Shaban, K. (2020, September 1). Model-based risk assessment for cyber physical systems security. https://doi.org/10.1016/j.cose.2020.101864

Choi, J H., Kim, H., Choi, S., Yun, J., Min, B., & Kim, H. (2019, July 2). Vendor-Independent Monitoring on Programmable Logic Controller Status for ICS Security Log Management. https://doi.org/10.1145/3321705.3331007

Miller, M D., & Holley, S. (2022, January 1). Assessing Human Factors and Cyber Attacks at the Human-Machine Interface: Threats to Safety and Pilot and Controller Performance. https://doi.org/10.54941/ahfe1002204

Fan, C., Chan, C., Yu, H., & Yih, S. (2018, November 1). A simulation platform for human-machine interaction safety analysis of cyber-physical systems. https://doi.org/10.1016/j.ergon.2018.06.008

Hajdukiewicz, J R., & Burns, C M. (2017, July 12). Ecological Interface Design. CRC Press eBooks. https://doi.org/10.1201/9781315272665

Anastopoulos, V., & Katsikas, S K. (2017, June 1). A structured methodology for deploying log management in WANs. Journal of Information Security and Applications, 34, 120-132. https://doi.org/10.1016/j.jisa.2017.02.004

Bennett, K B., & Flach, J M. (2019, March 15). Ecological Interface Design: Thirty-Plus Years of Refinement, Progress, and Potential. Human Factors, 61(4), 513-525. https://doi.org/10.1177/0018720819835990

Mulder, M., Borst, C., & Paassen, M V. (2019, January 1). Improving Operator Situation Awareness Through Ecological Interfaces: Lessons from Aviation. Communications in computer and information science, 20-44. https://doi.org/10.1007/978-3-030-32965-5_2

Kant, V., Karthikeyan, V V., & Sharma, N. (2022, August 16). Ecological interface design and emergent users: Designing for small-scale trucking ecology in India. Human Factors and Ergonomics in Manufacturing & Service Industries, 33(1), 55-68. https://doi.org/10.1002/hfm.20970

Kant, V., & Sudakaran, J S. (2021, September 27). Extending the Ecological Interface Design process—Integrated EID. Human Factors and Ergonomics in Manufacturing & Service Industries, 32(1), 102-124. https://doi.org/10.1002/hfm.20933

Hajdukiewicz, J R., & Burns, C M. (2017, July 12). Ecological Interface Design. CRC Press eBooks. https://doi.org/10.1201/9781315272665

Asghar, M R., Hu, Q., & Zeadally, S. (2019, December 1). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165, 106946-106946. https://doi.org/10.1016/j.comnet.2019.106946

Hancock, P A., & Szalma, J L. (2003, April 1). Operator Stress and Display Design. Ergonomics in Design, 11(2), 13-18. https://doi.org/10.1177/106480460301100205

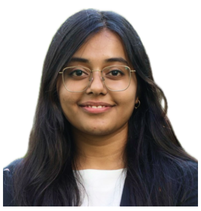
Bennett, K B., Bryant, A R., & Sushereba, C. (2018, May 9). Ecological Interface Design for Computer Network Defense. Human Factors, 60(5), 610-625. https://doi.org/10.1177/0018720818769233

Spero, E. (2023, July 18). User Interfaces, Mental Models, and Cybersecurity. https://doi.org/10.22215/etd/2023-15533

Biography

Rohit Negi. His research focuses on cybersecurity practices across various industry verticals, including seaports, oil and gas refineries, and power generation companies. His primary area of interest is the detailed design, development, installation, and commissioning of real-world Industrial Control System (ICS) test-beds and simulators, which are essential for simulating and addressing cybersecurity challenges in critical infrastructure.

Abhinaya Pranaikumar. She holds an undergraduate degree in Computer Science Engineering and is currently pursuing a Master's of Design at IIT Kanpur. Her research interests focus on enhancing human-machine interactions by applying cognitive design principles and user-centred methodologies across diverse domains.



Aparna Singh. She is currently pursuing a Master’s of Design at IIT Kanpur, focusing on UX design and research. Her research interests include human-computer interaction, user behavior, and emotional design, with a focus on bringing innovation to design and crafting impactful user experiences.

Vivek Kant. He is an active researcher in the field of systems design, human factors (cognitive ergonomics/cognitive engineering), sociotechnical systems, and history and philosophy of design engineering. He heads the Human Factors and Sociotechnical Systems studios at the Department of Design, Indian Institute of Technology Kanpur.