A Method for Reducing the Uncertainty Caused by a Power Outage During a Cyber Incident Response

Vitalii Zubok[1], Roman Drahuntsov[1]

[1] *G.E. Pukhov Institute for Modelling in Energy Engineering, 15 Oleh Mudrak str., Kyiv, 03164, Ukraine*

Abstract

It is well-known that modern war strategies widely include cyber-attacks along with kinetic strikes. Investigations are reporting that Russian aggressors use systematic cyber attacks on the Ukrainian power energy sector to increase the negative consequences of air strikes. Furthermore, vice versa, blackouts caused by air strikes make it challenging to respond to a cyber attack. Responding to and investigating any cyber incident during blackouts is notably complicated by an additional layer of uncertainty. A decision-making system simplification algorithm becomes necessary to address the challenges inherent in the decision-making process. This paper represents an overview of the impacts on cybersecurity caused by massive power outages, Specific challenges for cyber incident response, and some practical approaches to the loss of observability problem mitigation.

Keywords

preparatory cyber attacks, synchronous cyber attacks, power outages, cyber incident uncertainty, cyber incident response, cyber security, cyber resilience

1. Introduction

During the russo-Ukrainian war, the russian armed forces executed a multi-phased operation pursuing the objective of dismantling the Ukrainian power supply infrastructure and capabilities. Utilizing high-range missiles and Unmanned Aerial Vehicles (UAVs) to perform attacks resulted in extensive devastation to the national energy system, inflicting severe economic losses on Ukraine through widespread power outages. In response to these attacks, international allies and donors have prioritized the provision of critical components to repair damaged energy infrastructure and provide generators and fuel supply to protect the operation of essential facilities and services. NATO also provides additional weapons for the defence of critical energy infrastructure badly damaged by massive Russian missile and drone strikes. Nevertheless, these attacks have damaged up to 40% of the power system, with around 30 per cent of the country's power stations destroyed. That has substantially eroded the power grid's resilience and operational integrity.

The tense situation remains in the digital domain. Digital resilience is often referred to as a new KPI for digital transformation. Moreover, the most prioritized event which stresses the digital domain is the cascading effect of widespread power outages. Regular and unpredictable power outages considerably impacted the functionality of Information Technology (IT) systems within Ukraine. The primary impact vectors were identified as losses in system availability, while certain aspects of cybersecurity extended into the observability domain, tightly linked with the availability of information systems mentioned above.

The blackouts presented challenges in monitoring the state of IT systems, impeding effective log management and compromising the integrity of cybersecurity controls coverage. In such adverse conditions, managing a cyber incident — a process inherently characterized by high uncertainty — becomes a formidable challenge for Computer Security Incident Response Team (CSIRT) commands. The complexity is further compounded by an additional layer of uncertainty arising from the loss of observability. The efficacy of the decision-making process in cyber incident response hinges upon a

ITS-2023: Information Technologies and Security, November 30, 2023, Kyiv, Ukraine

vitaly.zubok@gmail.com (V. Zubok); draguntsow@yahoo.com (R. Drahuntsov)

0000-0002-6315-5259 (V. Zubok); 0000-0002-1781-7530 (R. Drahuntsov)

lucid comprehension of activities detectable within infrastructural components and a reliance on the veracity of the retrieved data. These requisites encounter substantial complexity due to observability losses deriving from extensive power outages. An algorithm for system decomposition and simplification (involving the sequential isolation and examination of components) can be applied to streamline the decision-making task within the cyber incident response. This paper delves into the intricacies of applying this algorithm to the cyber incident response process, aiming to enhance the support provided for decision-making processes within Computer Security Incident Response Team (CSIRT) commands.

2. Overview of impacts for cybersecurity caused by massive power outages

A military operation resulted in widespread power outages and other reasons for a massive state-wide energy crisis that imposed diverse impact vectors (see Table 1) on the cybersecurity of information systems and their capacity to respond effectively to a cyber incident. While certain impact vectors, such as losses in system availability, are evident, others are less apparent and bear a closer relationship to the cyber incident response process.

As evident from the above table, the cyber incident response process within an environment affected by extensive power outages faces multiple levels of uncertainty. Let us describe those levels more precisely.

The first and the most obvious is a full understanding of attack attributes. When a cyber incident occurs, the incident response team has limited knowledge of the harmful effects of the cyber attack and some prior insights about the attacker's tactic and significant properties. This set of attributes is generally presented by a party that experienced the impact of an attack or observed some misbehaviours in system functionality. In standard conditions, this prior knowledge suffers from inaccuracy, possibly caused either by insufficient security expertise of primary observers or intentional attackers' actions to lower its detectability. The obvious conclusion is that the system experiences a lack of full visibility in those conditions regardless of the reasons mentioned above. So, those conditions can become complicated dramatically when it comes to a system that experiences a massive power outage. The primary observers can experience side effects and availability loss caused by a power outage and thus confuse it with the impact of a cyber attack. The cyber incident response team receives distorted initial information, which impacts observability (as well as the power outage itself). This issue is widespread, even without any external negative factors, and becomes more important when the system experiences an observability loss. Clear and precise communication becomes crucial in such situations to avoid further confusion.

The second layer of uncertainty lies in the problem of system complexity. When a system comprises a significant number of distributed parts, separated facilities, or other partly independent components that may or may not have direct visibility from the cyber security response personnel, it creates the problem of the accurate incident scope evaluation. Simply put, it is impossible to be confident about which components of the distributed system were affected by destructive actions and which were not from a short-term perspective when an investigation is just going to be started. This uncertainty level (knowledge of attack scope) grows dramatically when the system experiences a massive power outage and observability loss.

The complexity inherent within a system's architecture significantly influences its observability, introducing an additional layer of uncertainty in the context of cyber incident response. This complexity arises both from the system's inherent structural intricacies and several critical attributes of the system. These include challenges in effective communication, constraints in the capabilities of logging mechanisms, limitations inherent in the deployed security systems, and the accessibility and reliability of data within the system. The multifaceted nature of modern systems, encompassing a wide array of interconnected components and services, often leads to intricate communication proto-

Table 1
Impact vectors of cyber attacks

Impact vector	Description
System availability [1]	The occurrence of a power outage in information systems facilities leads to disruptions in regular operations and influences information availability. It represents the most evident impact vector, serving as the root cause for subsequent effects.
System integrity [2]	While certain system components may experience downtime during the power outage, others may persist online. In the case of protective systems situated independently from the safeguarded entity, the integrity of the defence architecture may be compromised. Integrity impacts can also arise from power outages that momentarily disrupt data flow, with short restoration after a brief timeout. Instances of data transmission gaps, challenges in system state synchronization, and interruptions in ongoing operations susceptible to failure may constitute integrity risks for a system suffering from power outages.
System observability [3].	The ability to get a clear view of a system's functionality flow and history is crucial to its security architecture. When an information system's component goes offline, it stops sending logging information to the central console. However, this behaviour may be caused by at least three reasons: a power outage of the component, a power outage of some part of the data transmission channel, and a threat agent's activity aimed at breaking the visibility of a component. A power outage poses a danger to the system's observability, not only with a logging information shortage itself. Also, additional uncertainty arises of needing to separate a threat-caused observability loss from a natural one.
Response capability [4].	The ability to respond to a cyber incident is heavily dependent on a system's main parameters, impacted by power outages, as mentioned before. A large set of other factors heavily complicate the incident response process – broken communication channels caused by the power outage bring havoc into normal communication between CSIRT command members that may work in a power-shortened system component. That may also impact the ability to use several security systems and controls that may also go offline.

cols and networks. This complexity can impact clear and efficient communication pathways essential for timely and accurate incident response. The effectiveness of logging mechanisms is paramount in cyber incident investigations. However, the limitations in these mechanisms, such as incomplete logs, lack of synchronisation across systems, and insufficient granularity of logged data, compound the uncertainty in accurately reconstructing and understanding cyber incidents. The deployed security systems themselves may contribute to this uncertainty. Often, these systems are designed and optimised for known threats and may need more sophistication to detect novel or complex attack vectors. This gap in detection capabilities can leave significant blind spots in the system's observability. The accessibility and reliability of data within the system play a crucial role. In many instances, the data necessary for a thorough investigation may be inaccessible due to privacy constraints or encryption or may have been tampered with or destroyed by attackers. Additionally, data's sheer volume and complexity, especially in large and diverse IT environments, pose significant challenges in data analysis and interpretation. The impact of those observability vectors is valuable during the standard incident response flow, and its value rises dramatically when the system experiences a massive power outage.

Cyberspace introduces an additional burden on monitoring and analysing system states. Branched systems are often interconnected through the Internet, and these unified systems can have extensive distribution. The logical relationships between components in such amalgamations are constructed based on lower-level network topologies, resulting in highly intricate dependencies, even without delving beyond the network layer (as per the well-known OSI model). In TCP/IP networks, global routing issues are addressed through the conditional grouping of network address space into so-called network prefixes. These prefixes serve as routing elements globally, being announced among entities engaged in global routing, specifically autonomous systems (AS), thus forming routes. A specific prefix may vanish from the global routing system due to a cyber attack or equipment power outage that was supposed to announce it. At this juncture, an assailant could falsely announce this prefix, thereby creating deceptive routes that distort the Internet's topology. Exploiting this, an attacker could intercept traffic to a system segment. In some instances, it is possible to employ counterfeit devices or manipulate traffic, including operational traffic from monitoring system components. Traffic hijacking through manipulating the global routing system is one tactic in hybrid warfare [5]. Present-day solutions for protecting the BGP-4 global routing protocol do not warrant comprehensive security.

Specifically, the primary challenge in responding to and investigating a cyber incident under such conditions lies in the ability to differentiate between system components that have experienced a breach and those that have not. This is compounded by circumstances where trust in the logging data of components is compromised, and the logging data itself may be incomplete [6].

3. Specific challenges for cyber incident response during the power outage

Let us examine the nature of a system undergoing a breach in the context of extensive power outages. Consider a hypothetical system model, for instance, a geographically dispersed multi-component information system primarily situated in a country suffering from an energy crisis. The components within such a system can be conceptualized as the fundamental building blocks, encompassing data centres, networks, IP ranges, VLANs, and similar entities [7].

The initial imperative for a component is to exhibit some form of isolation from other components. While the boundaries between components may be virtual, the presence of attributes that fortify access restrictions from one component to another is essential. If such restrictions prove valuable during the incident response process, these components should be regarded as distinct entities. The second criterion involves recognizing that the impact of a power outage on a given component may differ for various reasons compared to surrounding components. If the component of an information system possesses a distinct reserve power source or exhibits a varying susceptibility to power outage impacts compared to its surroundings, it is worth consideration as a separate component. The final criterion for defining a component lies in business functionality. If a specific part of an information system supports a clearly defined business function that is not shared with other parts, that particular section should be acknowledged as a distinct component.

The given above system decomposition methodology is largely simplified [8]. Nevertheless, it gives enough abilities to imagine a model for a system suffering from an incident and one that will be investigated. Let us assume that an imaginary information system has two geographical facilities and one cloud-based resource. One of those facilities experienced considerable observability loss that may be linked to a cyber incident. However, the traces of a cyber incident can be found in all of the system's facilities as shown on Figure 1.

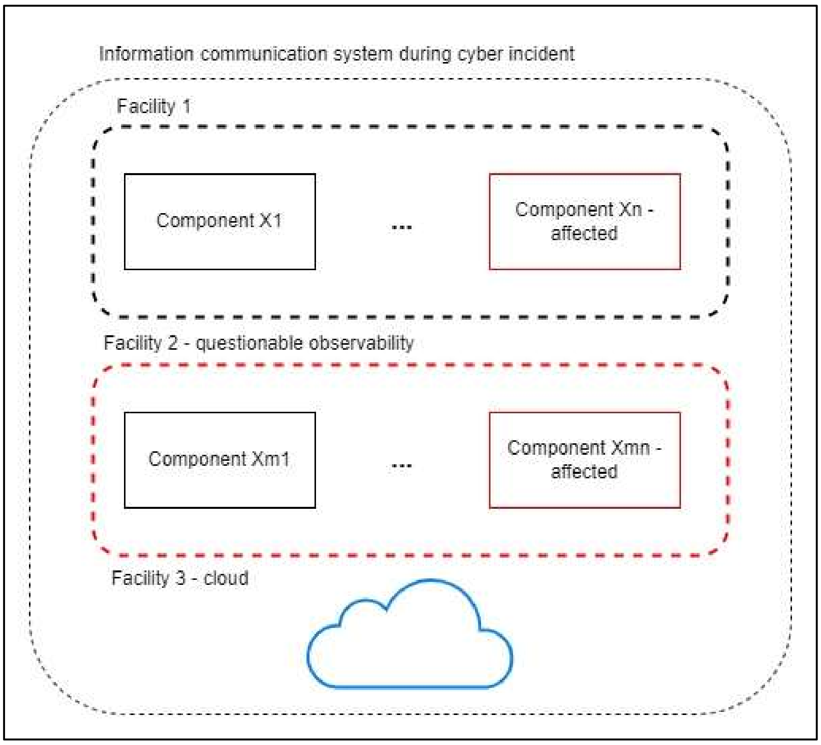

Figure 1: Uncertainty caused by observability loss

When a CSIRT command is aware of an incident that occurred in infrastructure and possesses all the information above, it faces some specific challenges:

3.1. Was the reason for the observability loss in Facility 2 caused by a power outage or by a threat agent?

From the perspective of cyber incident responders, encountering a scenario where there is a complete loss of visibility within a distinct component of a system can be regarded as a critical incident in its own right. This perspective gains particular relevance when a system concurrently undergoes a confirmed security breach alongside this visibility loss. Such circumstances significantly compound the complexity and urgency of the response required, as the absence of visibility impedes the responders' ability to effectively assess the scope, impact, and nature of the breach. In these contexts, the loss of visibility hinders the immediate response efforts and introduces significant challenges in formulating a comprehensive understanding of the incident. This lack of clarity and control over the affected system's component exacerbates the uncertainty surrounding the breach, complicating efforts to identify the intrusion's vectors, the data or assets compromised, and the steps necessary for mitigation and recovery. Addressing this compounded uncertainty requires more than straightforward solutions or conventional response strategies.

3.2. What logging information from Facility 2 was missing?

A specific challenge arises not from scenarios of complete observability loss but rather from circumstances where only partial logging data is missing. This nuanced situation introduces a significantly higher level of complexity for incident responders, primarily because discerning the true nature of the incident becomes substantially more difficult. The ambiguity between whether the gaps in logging data are the result of a cyber attack or due to more benign causes, such as a power outage, poses a unique set of challenges. Partial loss of logging data complicates the incident response process in several ways. Firstly, it creates uncertainty around the scope and impact of the incident. Unlike a total loss of visibility, where the assumption may lean towards a severe compromise, partial data loss leaves room for doubt regarding the extent to which the system's security has been breached. This uncertainty can lead to either underestimating the severity of the situation, potentially overlooking a subtle but significant intrusion, or overestimating it, which could allocate resources inefficiently. Secondly, the ambiguity in identifying the cause of the partial data loss complicates the diagnostic process. Cyber attacks, especially sophisticated ones, might selectively target or manipulate logging mechanisms to obscure their activities, making them appear as inconsequential or unrelated to security incidents, such as attributing the cause to operational failures like power outages. Distinguishing between these scenarios requires a nuanced understanding of both the system's normal operations and potential attack vectors, as well as a deep forensic analysis to uncover subtle indicators of malicious activity.

3.3. Is the observability of Facility 1 trusted or not?

Possessing comprehensive logging data from a specific facility does not unequivocally guarantee the reliability or integrity of that information. This stems from the inherent vulnerability of logging mechanisms to manipulation by threat actors. Therefore, the assumption that such data is inherently trustworthy can lead to oversight and misjudgment in the response process. Cross-verification of logging data with independent sources of information, such as network traffic analyses, intrusion detection systems, and raw log files, enhances the ability to identify discrepancies that may indicate tampering. This multifaceted approach not only aids in confirming the validity of the logging data but also enriches the incident response process by providing a more comprehensive and nuanced understanding of the cyber incident, but it requires many more resources to be allocated that may be inappropriate when the time of response is crucial.

3.4. What components in Facility 2 were targeted by a threat agent, and how may that be proven in low observability conditions?

The definitive knowledge that a threat actor has successfully infiltrated a specific facility does not straightforwardly translate into an understanding of the extent of access gained by the attacker or their capability for lateral movement within the network. This complexity arises from the multifaceted nature of cyber attacks, where the initial compromise is often just the beginning of a series of actions aimed at escalating privileges, exploring the network, and identifying valuable targets.

Analyzing the aforementioned questions, we can see the evidence that they are interlinked, each prompting the other. Addressing these concerns can prove challenging and resource-intensive when examining the system as an entirety. However, dissecting each component in isolation from others may introduce significant risks. These risks encompass the potential escalation of threat agents from one non-investigated component to another or from an uninvestigated component to an already scrutinized one. This likelihood characterizes a direct, component-based analysis as perilous and ineffective, introducing the issue of a 'horizontal threat shift.' This term denotes the threat agent's capacity to traverse between system components in conditions of low observability.

4. System simplification algorithm to defeat the challenge of observability loss

The investigation and response process can be facilitated and rendered more comprehensive by decomposing the system into the components mentioned above [7], with each component subsequently undergoing individual investigation. However, this approach is susceptible to the previously mentioned issue of horizontal threat shift. A potential remedy for this problem involves isolating each component and investigating its activity in isolation. However, a significant challenge arises in that it is only feasible to isolate every component with inflicting a substantial business impact. The isolation of all system components would result in a complete enterprise shutdown, an outcome inappropriate during any investigation.

To address this challenge, we propose an algorithm for system simplification aimed at supporting the decision-making process during cyber incident response. This proposed algorithm represents a strategic enhancement to conventional incident response methodologies by introducing a systematic approach to dissecting the entire information system into manageable segments or components. This methodological partitioning serves two critical functions in the preliminary stages of the incident response process: it significantly aids in the isolation of system components and refines the prioritization of investigative efforts. The core principle underpinning this algorithm is the targeted isolation of system components that can be segregated from the broader network without triggering adverse operational impacts. Such preemptive isolation is particularly pivotal in scenarios where the system's observability has been compromised by external disturbances, exemplified by extensive power outages.

Practically, the application of this algorithm begins with an assessment of the information system to identify and categorize its components based on their functionality, criticality to business operations, and interdependencies. This decomposition may be done by or in a timely manner when an incident arises. This evaluation enables the incident response team to determine which components can be temporarily isolated or taken offline without significantly disrupting essential services or business processes. By isolating these components, the team can mitigate the risk of further damage or contamination, thereby narrowing down the scope of the investigation and allowing for a more focused and efficient forensic analysis. For components that are deemed too critical to be isolated—those integral to the continuity of business operations—the algorithm assigns a higher priority level for immediate investigation. This prioritization ensures that the most crucial parts of the system, which cannot afford downtime, receive prompt attention to identify and address vulnerabilities or ongoing attacks. By doing so, the incident response team can concentrate their resources and efforts on areas with the highest risk and impact on the organization's operations.

The investigation process is designed to address whether an observability loss has transpired in the component and if it was instigated by the activity of a malicious actor. Additionally, it examines whether any traces of actor activity can be discerned within the component. Components confirmed to be impacted by a threat agent are unequivocally isolated and subsequently directed into the standard investigation flow. On the other hand, components for which there is no confirmation of threat agent activity, whether isolated or not, are unblocked and then channelled into the same investigation flow.

This algorithm represents a subtype of the decision tree algorithm specifically tailored for preprocessing incident investigations and responses under conditions of low observability. The graphical representation of the algorithm is illustrated in Figure 2 and Figure 3.

The algorithm's core advantage lies in its capability to generate a sorted and prioritized list of components for investigation, facilitating more effective coordination of actions and optimizing the use of limited resources. This significantly enhances the decision-making process during incident response. The list can be conceptualized as a vector of objects, arranged by their criticality from least critical to most critical. Components are further categorized into two groups: isolated ones $(X_1, X_2 ... X_n)$ and unblocked ones $(Y_1, Y_2 ... Y_n)$. The investigation function iterates through the vector in reverse order, moving from Y_n to X_1. The graphical representation of the components vector and its application is depicted in Figure 4.

Assuming we have a set S representing the information system and C representing the set of atomic components, the algorithm can be described as follows:

1. Define the information system as a set S where $S=\{c_1,c_2,...,c_n\}$
2. Each c_i is an atomic component of the information system.
3. Assign criticality values to each component using the function f: $f(c_i)$ gives the criticality of component c_i.

4. Identify components with lower criticality values.

5. Isolate or remove components with criticality below a certain threshold of inappropriate business impact. Let C_{imp} be the set of remaining important components:

6. $C_{imp} = \{ci \in C | f(ci) \geq Threshold\}$

7. Sort all components in C by their criticality values in descending order to obtain a sorted list.

8. Define the function Investigation:$C_{sorted} \rightarrow \{"legit", "illegal"\}$, where Investigation(ci) returns the status of the component c_i.

9. Apply the investigation function to each component in the sorted list from most critical to least critical.

10. Isolate components marked as "illegal" and pass them to the function StandardIncidentResponse.

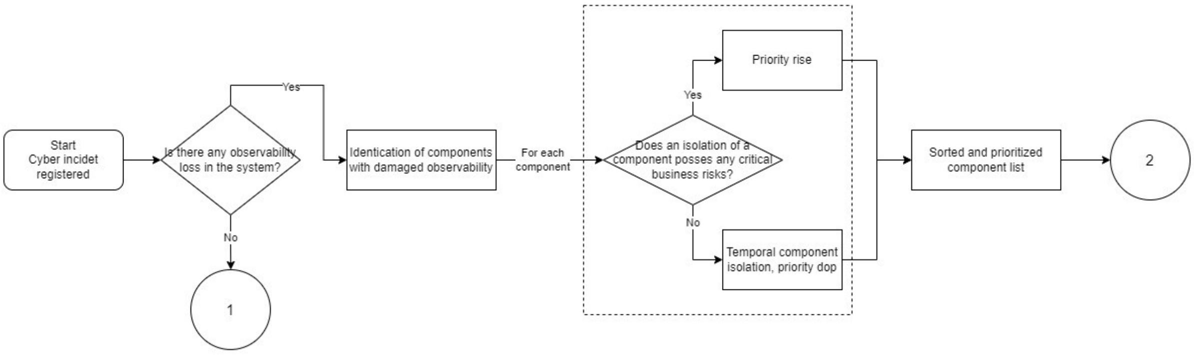
Start
Cyber incidet
registered
Is there any observability loss in the system?
Yes
No
1
Identication of components with damaged observability
For each component
Does an isolation of a component posses any critical business risks?
Yes
Priority rise
No
Temporal component isolation, priority dop
Sorted and prioritized component list
2

Figure 2. Incident response decision tree algorithm - part 1

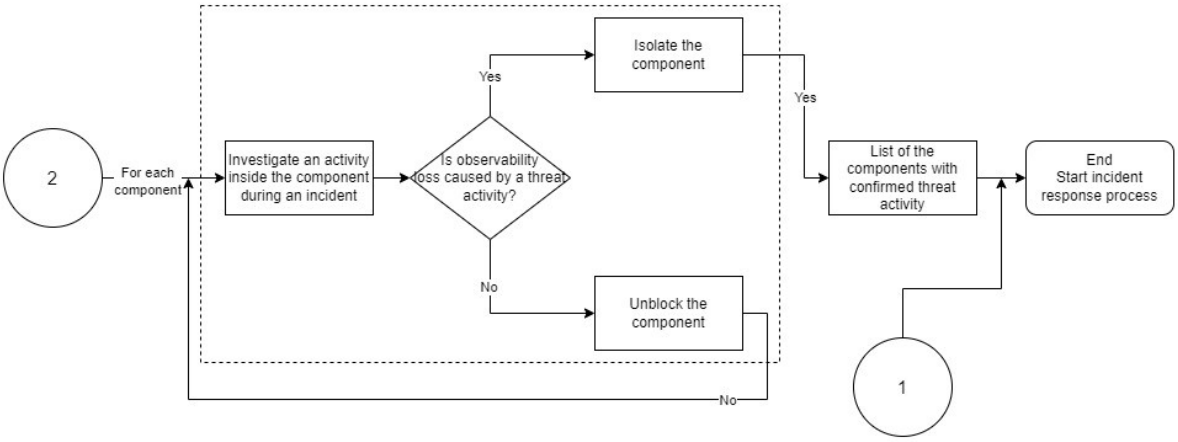
2
For each component
Investigate an activity inside the component during an incident
Is observability loss caused by a threat activity?
Yes
Isolate the component
No
Unblock the component
Yes
List of the components with confirmed threat activity
No
1
End
Start incident response process

Figure 3. Incident response decision tree algorithm - part 2

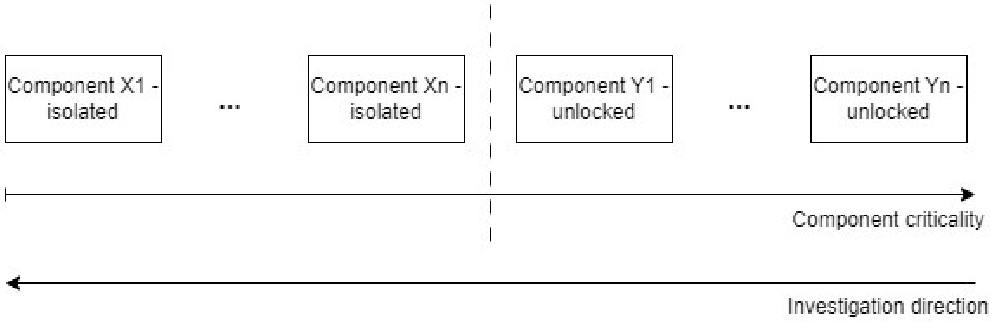

Figure 4: The components vector and its application

An implementation of this algorithm involves several practical steps:

1. System Mapping and Component Categorization. The development of a comprehensive map of the information system, identifying all components and categorizing them based on their criticality, functionality, and interconnectivity, rises the efficiency of the process in an emergent situation.
2. Risk Assessment and Isolation Feasibility. It is required to assess the feasibility of isolation for each component, considering operational dependencies and the potential for adverse impacts and conduct a risk assessment to determine the vulnerability and potential impact of each component that may be compromised.
3. Isolation and Containment. It is required to assure, that the system should implement containment capabilities to prevent the spread of the incident to other parts of the system.
4. Continuous Monitoring and Adaptation. Continuous monitoring of the system for changes in threat behaviour or additional signs of compromise in context of observability changes is essential in order to keep the process functioning.

5. System simplification algorithm – practical implementation caveats

The upper-mentioned algorithm has some practical caveats applicable to several environments:

5.1. A high amount of non-isolatable components

The component vector of a system, where the majority of components cannot be safely isolated without causing inappropriate business impact, is characterized by Xn significantly greater than Yn. This characteristic renders the algorithm less effective against horizontal threat shift, as a substantial portion of the components still needs to be unlocked and unobservable during the initial investigation. Achieving such a high degree of isolation or communication control required for ideal algorithm functionality within a complex information system is often a challenging endeavour. This inherent difficulty in completely segregating or controlling communication channels among system components adds layers of complication to the incident response process. In practical terms, the ability to isolate components or limit communications is crucial for containing a security breach and preventing its spread within the system. Several factors contribute to the challenge of achieving effective isolation:

1. Interdependencies among components. A typical information system is characterized by a high degree of interconnectivity and interdependence among components. Fully isolating a component can disrupt critical services or workflows, impacting business operations.
2. Complex network architectures. The complexity of network architectures, especially in large and diverse environments, makes it difficult to ascertain all communication pathways and, therefore, challenging to block or control them effectively.
3. Limited control over third-party components. Third-party components have “supply-chain” security issues. Systems often incorporate third-party components or services over which the organization has limited control, making complete isolation or communication restriction impractical.

This challenge can be addressed with several measures:

- Incorporating a less strict isolation procedure that avoids inappropriate business impact;
- Implementing multiple, stricter, and trustworthy controls to monitor the activity between unblocked components;
- Segmentation and micro-segmentation of network (where it is possible) to create smaller manageable zones within the network. This approach reduces the attack surface and provides better control over inter-component communication;
- Developing dynamic isolation capabilities for selective isolation of components;
- Establishing Fallback Procedures and Redundancy for critical services. This ensures that essential functions can continue even when a component is isolated.

5.2. Significant scale of the components

When the individual components of an information system exhibit significant scale, the essential investigation of each component will demand a substantial allocation of resources by the CSIRT. This can lead to an increased risk of horizontal threat shift and may amplify the repercussions of isolating the components that remain separated. In fact, isolating a particularly large-scale component may yield minimal benefits to the cyber incident response process. In large-scale components, the internal complexity often mirrors that of a smaller-scale complete system, encompassing multiple sub-components, diverse functionalities, and intricate communication networks. Such complexity presents several challenges:

1. High risk of internal lateral movement. Larger components with multiple sub-systems provide more opportunities for threat actors to move laterally within the component. This movement can be difficult to track and contain, making it challenging to isolate the attack effectively.
2. Resource-intensive investigation. As stated above, investigating a large-scale component requires significant resources. The scale of the component may necessitate a proportionally larger response effort, potentially diverting resources from other critical areas.
3. Potential for disruption. Isolating a large-scale component can have a substantial impact on business operations, especially if the component plays a central role in the organization's activities. The disruption caused may outweigh the benefits of isolation, and its cost rises in conditions of power outages.

To address this challenge, a CSIRT can implement more lenient requirements for the baseline investigation, focusing solely on checking for the reason behind the observability loss. This should suffice to ascertain whether a power outage has occurred and affected the system. Alternatively, another approach involves reducing the number of system components under investigation by segregating those components and facilities that have not been impacted by either a threat agent or a power outage with sufficient likelihood. There is also a way to implement a phased investigation when the algorithm is applied to a large component in the same way as for the whole system.

5.3. Inability to practically isolate a component

Poor observability conditions resulting from a power outage can lead to substantial degradation of active response capabilities, particularly the ability to isolate a component from others on various communication levels. This challenge may persist even when adequate security systems were not in place prior to the incident. As a rapid interim solution, compensatory monitoring-based controls can address this issue. By fixing and validating any communication between components, suitable capabilities can be deployed more swiftly compared to the implementation of comprehensive isolative measures.

While AI/ML methods and generative model usage are spreading in incident response and investigation [9], perhaps, in the future, investigation scenarios under conditions of uncertainty will be developed using generative models. The deployment of generative AI models can be highly instrumental in enhancing the aforementioned incident response algorithm, particularly in identifying priority targets for isolation, guiding decision-making processes regarding isolation actions, distinguishing between deliberate observability impairments by attackers and normal observability loss, and managing response procedures under conditions of limited visibility. The integration of these advanced AI models into cyber incident response frameworks can significantly elevate the effectiveness and efficiency of handling complex security incidents. In cyber incident scenarios, distinguishing between observability loss caused by malicious activities and that resulting from benign issues (like power outages) is crucial. Generative AI models can be trained to recognize the subtle differences between these scenarios by analysing patterns in the data that might indicate the presence of an attack, such as unusual network traffic or changes in system behaviour. In situations where visibility within the system is compromised or damaged, generative AI can play a pivotal role in guiding the incident response. The models can simulate potential scenarios based on the available data, helping to illuminate areas of the network that are not directly observable. This can aid responders in making informed decisions about where to focus their investigative and remedial efforts.

6. Conclusions

Massive power outages pose at the state level a significant challenge to the cybersecurity of an enterprise. Responding to and investigating any cyber incident in the midst of such blackouts is notably complicated by an additional layer of uncertainty. A decision-making system simplification algorithm becomes necessary in order to address the challenges inherent in the decision-making process. The system simplification algorithm, based on component isolation, serves as a precursor to a standard investigation flow, breaking down the complex task and mitigating the layer of uncertainty induced by observability losses. The practical application of the algorithm entails some noteworthy caveats, which can be mitigated by lowering isolation requirements and incorporating compensatory controls.

7. Acknowledgements

This research is partially sponsored by the Ministry of Education and Science of Ukraine (project №0123U102744 "Cyber Risks and Cyber Security of The Topology of Distributed Information Systems in Global Cyberspace") and the European Union (project № 101121356 "AGILE: AGnostic risk management for high Impact Low probability Events").

8. References

[1] E. Ahadu, The effect of electric blackout on the operation and productivity of small manufacturing enterprises, *IJRRIS* 6 (3) (2016) 11–21.

[2] OSA Internal Audit Services, Gap analysis risk management final report, 2019. URL: https://osa.sc.gov/wp-content/uploads/2019/11/Gap-Analysis-Risk-Management-Final.pdf.

[3] K. Scarfone, Cybersecurity log management planning guide, NIST SP 800-92r1, National Institute of Standards and Technology, Gaithersburg, MD, 2023. doi:10.6028/nist.sp.800-92r1.ipd.

[4] Forescout Research Labs, Threat report: Top defense evasion techniques used by malware, 2023. URL: https://www.forescout.com/resources/top-defense-evasion-techniques-used-by-malware/.

[5] A. Davydiuk, V. Zubok, Analytical review of the resilience of Ukraine's critical energy infrastructure to cyber threats in times of war, in: *Proceedings of the 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, Tallinn, Estonia, 2023, pp. 121–139. doi:10.23919/CyCon58705.2023.10181813.

[6] R. Drahuntsov, V. Zubok, Modelling of cyber threats related to massive power outages and summary of potential countermeasures, *Elektronne Modelyuvannya* 45 (3) (2023) 116–128. doi:10.15407/emodel.45.03.116.

[7] Cisco Public, Network visibility and segmentation, 2019. URL: https://www.cisco.com/c/dam/en/us/products/se/2017/9/Collateral/cisco-security-services-solution-overview-013119.pdf.

[8] P. Maynard, K. McLaughlin, S. Sezer, Decomposition and sequential-AND analysis of known cyberattacks on critical infrastructure control systems, *Journal of Cybersecurity* 6 (1) (2020). doi:10.1093/cybsec/tyaa020.

[9] D. Lande, O. Novikov, D. Manko, The analysis of cybersecurity subject area terms based on the information diffusion model, *Theoretical and Applied Cybersecurity* 4 (1) (2022) 55–60. doi:10.20535/tacs.2664-29132022.1.274122.