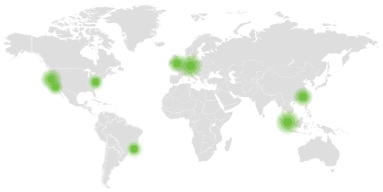
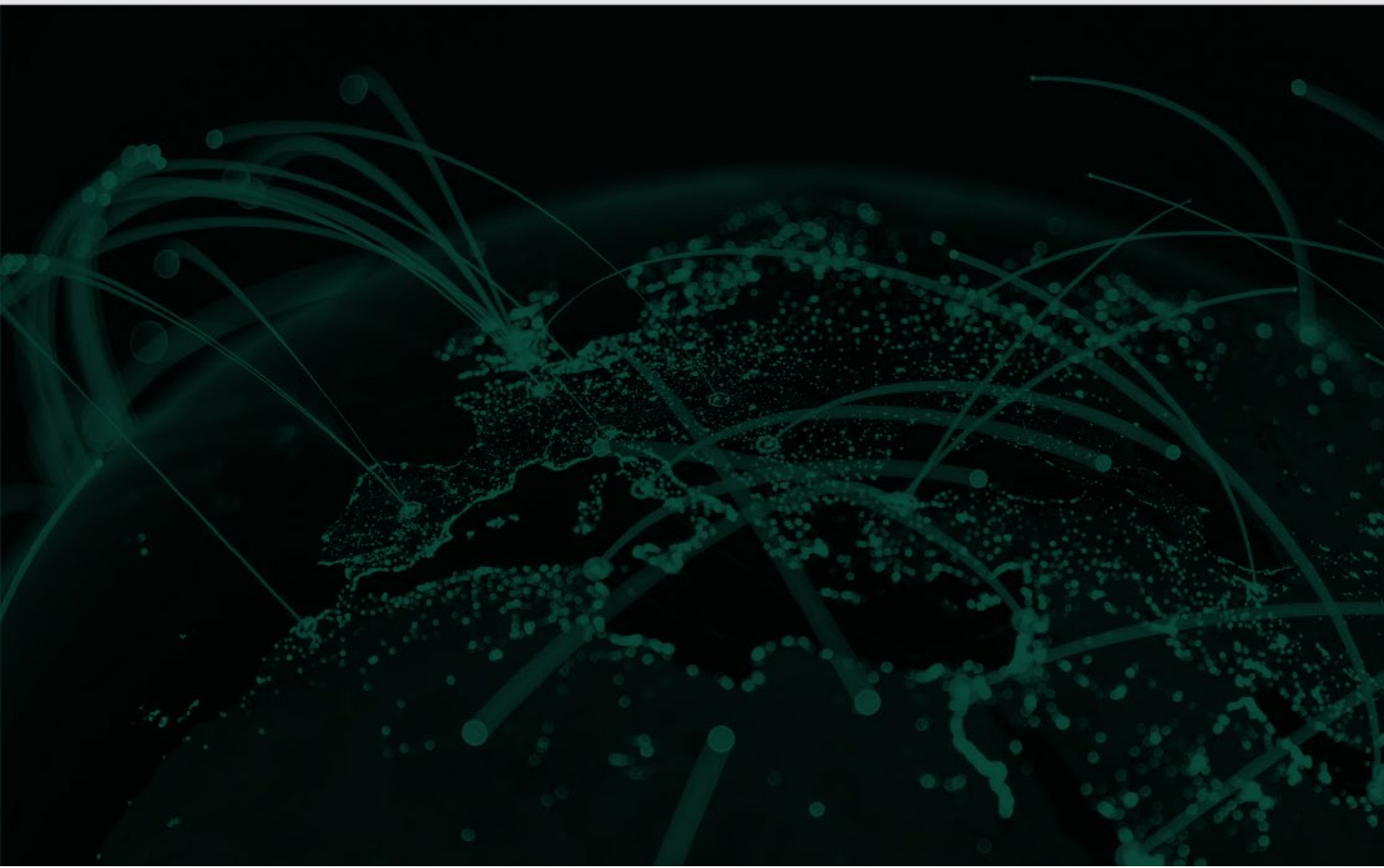
WHITEPAPER



2023

AISecOps Whitepaper



Executive Summary

With the boom of the global digital economy, cybersecurity is converging with the Internet of Things (IoT), industrial Internet, cloud computing, and 5G, bringing about disruptive changes to security in various aspects, including traditional physical security, biological security, public security, and national security. Meanwhile, the attack surface keeps expanding in cyberspace as malicious attackers, larger in size, are well trained and organized to update its arsenal with automated intelligent attack technologies. In view of the current complicated situation, the traditional approach to deploy protective devices at network borders has gone out of date.

As the offensive-defensive battle is getting more intense, Security Operations (SecOps) is born to enable integration between personnel, techniques, and processes, facilitating collaboration of global security defense resources. Currently, SecOps has become the most direct and critical step to make the defense system work to its best when dealing with advanced threats.

Predictably, as more proven technologies are used for collection and intelligent analysis of security big data, the advent of the AI-based Security Operations (AISecOps) method greatly streamlines threat detection, risk assessment, automated response, and other critical operation phases, in sharp contrast to traditional solutions with overdependence on experts' experience. This method significantly lowers overall security risks facing critical information infrastructure and data assets of enterprises, organizations, and even the whole country. However, for AISecOps currently in its infant stage, systematic reviews and combings need to be done for its system architecture, evaluation methods, data integration, and technological direction. Therefore, NSFOCUS released the AISecOps Whitepaper to give an overview of the critical concepts, hype cycle, and techniques of AISecOps. Offering a fresh view on security operations, this document is prepared to demonstrate how to speed up technical upgrade of cybersecurity operations by building an AISecOps ecosystem.

This whitepaper has the following findings:

- **Due to a dire shortage of security experts, it is imperative to intelligentize security operations.**

Owing to vast amounts of security operations data in the digital era, it is impossible for the traditional expert-driven security operations approach to work.

- **AISecOps is not simply putting together AI-based operations (AIOps), AI-based security (AISec), and SecOps.**

In the cyberspace featured by intense antagonism, AISecOps makes intelligent human-machine integration possible on the basis of correlative analysis of multidimensional and multisource data regarding behaviors, environments, intelligence, and knowledge. In this way, AISecOps ensures the implementation of core indicators and key phases of SecOps risk control, improving the automation level of SecOps in an all-round manner.

- **AISecOps is evolving rapidly, with subtechnologies to be refined.**

By establishing the technical framework and technical maturity matrix for AISecOps, we find that key technical capabilities in various phases are not yet mature and more research effort needs to be devoted to sharpen them.

- **Only operable technologies can effectively support cybersecurity operations.**

For data intelligence-driven methods, improvements should be made to operable attributes like security semantics adaptation, attack intention understanding, decision-making credential transparency, and in-depth interaction to promote a closer integration of machine intelligence and data and knowledge of security operations experts.

- **"Secret" graphs concerning AISecOps technology should be created to combat organized, large-scale, and weaponized threats.**

Isolated single-point security intelligence applications are insufficient to meet systemic security operations requirements. A fine-grained, scenario-based, and appropriately abstract operational technology capability center should be built to support intelligent security operations development throughout the entire lifecycle.

- **Trusted security intelligence marks the future of AISecOps.**

Only transparent, legitimate, and compliant security intelligence that features high predictability, interpretability, and security robustness can inform critical decision-making for cybersecurity operations and increase operations automation.

- **Efforts should be made to promote the development of the AISecOps technique ecosystem to achieve defense in depth.**

For AISecOps still in its infancy, we should build a technique ecosystem, formulate relevant standards, organize data and technology sharing, and cultivate talents, with a view to building a sound technical environment in the era of intelligent cybersecurity operations.

Table of Contents

1. SecOps Development Background and Trend

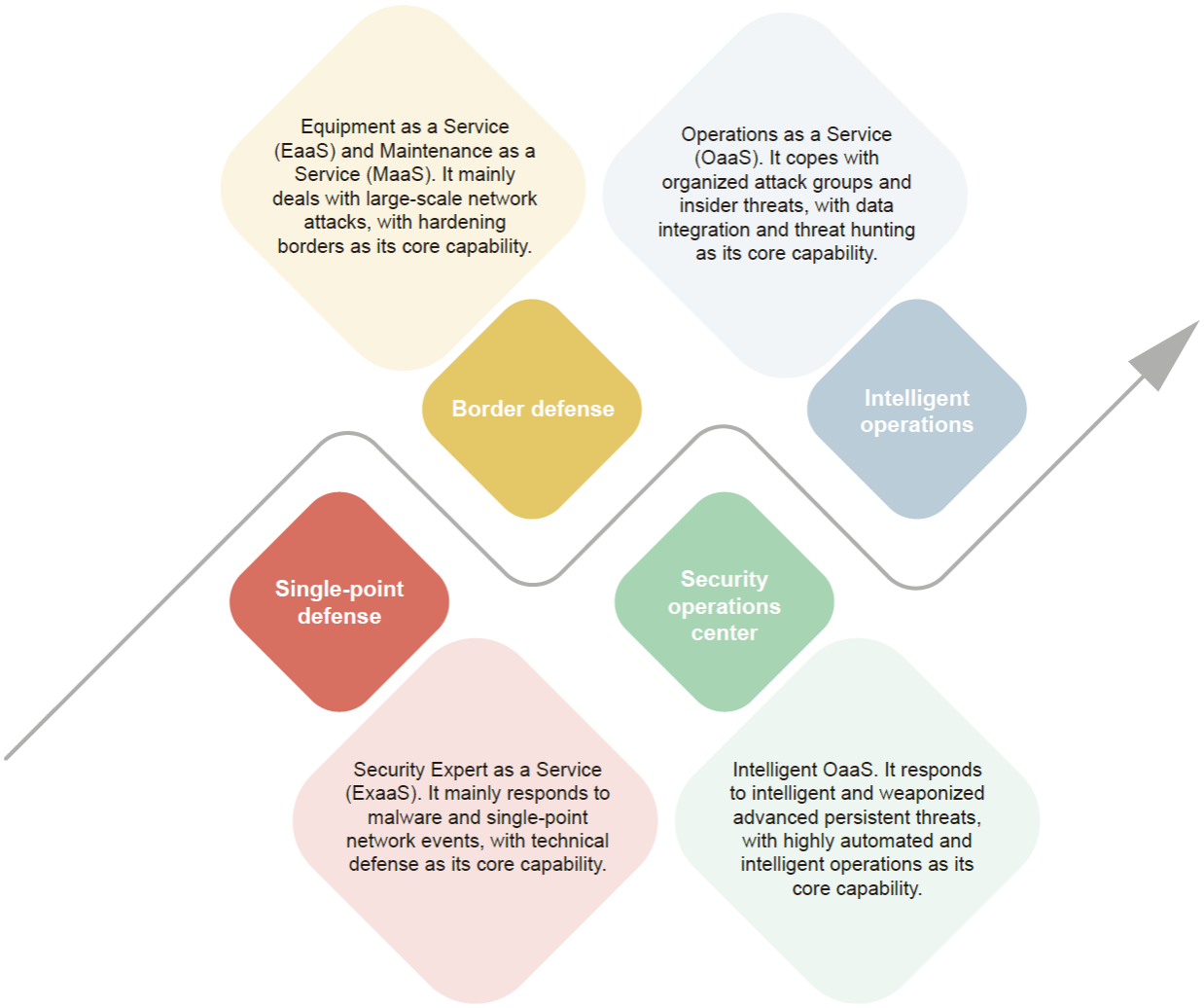


Figure 1 SecOps evolution process

Reflecting on the cybersecurity history composed of computer security, information security, cyberspace security, and digital security, we observe that for the conceptual evolution of the security industry, the core trend is that network informatization pushes forward the development of security technologies in each era. However, the attack surface keeps expanding in cyberspace as malicious attackers, larger in size, are well trained and organized to update its arsenal with automated intelligent attack technologies. In view of the current complicated situation, the traditional approach to deploy protective devices at network borders has gone out of date. As offensive/defensive battles keep escalating, the traditional security defense solution focusing only on security borders is gradually being replaced by a more mature and complete sliding-scale protection approach. Shift left of border defense is a systematic intrinsic security mechanism, while shift right is intelligence-driven proactive defense. Thanks to its features such as zero trust, threat capture, threat hunting, security development, and security operations, the intrinsic proactive defense approach has become a widely recognized solution in the security industry. **For both shift left and shift right, SecOps has increasingly become a must-have security capability.**

SecOps is intended, via processes, technologies, and services, to provide enterprises and organizations with vulnerability identification and management and threat detection and response among other security capabilities, in an effort to ensure effective control of security risks[i]. **Conceptually, the core of SecOps is management of risks that needs to be measured in a dynamic, continuous, and relative way.**

Since security operations is driven by risks, it evolves with progressive risk perception. Overall, going through the single-point defense, border defense, and security operations center phases, security operations finally moves towards intelligent operations.

- **Single-point defense:** With the advent of the Internet era, malware targeting personal computers first emerged. The threat trend of the Internet world gradually entered the public view. With malware looming largest among other security risks, numerous security experts were engaged in antivirus software research. The concept of SecOps has yet taken shape, security capabilities are delivered typically as Expert as a Service (ExaaS).
- **Border defense:** For the sake of financial gains, attacks and threats have gradually become organized and industrialized. At the same time, a great number of software vulnerabilities are exposed with the rapid evolution of large-scale Internet services and IT system software. In response, NSFOCUS Anti-DDoS System (ADS), NSFOCUS intrusion Detection System (NIDS), and NSFOCUS Remote Security Assessment System (RSAS) were launched to quickly build the network border protection system. With the deepening of attack and defense research and fast iteration of threat scenarios, security operations make rapid progress, penetration testing and risk assessment teams are set up, thus forming the prevailing Equipment as a Service (EaaS) and Maintenance as a Service (MaaS).
- **Security operations center:** The emergence of advanced persistent threats (APTs) and relevant events have brought a huge impact on border defense. Multi-layered security policies and regulations are combined to form compliance requirements. The aggregation of multiple factors leads to radical changes in the whole cybersecurity cognition. It has become a consensus in the industry to conduct normalized, collaborative, in-depth, and intelligent defense. The SecOps concept and architecture have gradually taken shape, and security operations centers (SOCs) have flourished everywhere. SOCs manage threats, vulnerabilities, assets, and other risk-related procedures and data in a centralized manner and adopt such advanced security technologies as behavior analysis, honeynet capture, threat hunting, and intelligence fusion so as to improve the security operations efficiency. Operations as a Service (OaaS) is becoming a critical trend for cyberspace protection. Against this background, the Continuous Adaptive Risk and Trust Assessment (CARTA) architecture and concept are popularized.
- **Intelligent operations:** The security operations team plays a central role for centralized running of SecOps. The development process of SecOps reflects the upgrade of technologies and interpersonal confrontation. Currently, as the data volume grows explosively and technologies become more complicated, attackers and defenders are fighting increasingly arduous battles, but on the defensive part, the current human capacity is far from sufficient to achieve risk control objectives. In view of key features of the digital era, a major breakthrough should be made to cybersecurity operations that merely depend on security experts. In this context, making security operations techniques and processes more automated and intelligent has become a prerequisite for cybersecurity risk governance and control. Intelligence-empowered security operations provide a solid foundation for OaaS in the digital era.

Intelligent security operations has become an inevitable trend. More and more technologies including traffic analysis, behavior analysis, sample analysis, threat association, and automated response use machine learning algorithms, graph algorithms, and reinforcement learning algorithms. Even so, the development level of security intelligence still cannot satisfy security operations requirements in threat discovery timeliness and accuracy, automated event traceback, and risk decision-making automation. There is still a long way to go before AISecOps services are mature.

2. Challenges of AISecOps

For security operations, the difficulty in analyzing massive data comes down to the imbalance between attacks and defense. In the cyberspace where defenders fight against attackers hiding in the dark, collection and analysis of massive data are a prerequisite for AISecOps. Processing massive data has posed unprecedent challenges to security operations teams that might be haunted by dependence explosion, alert fatigue, and threat identification from too many events. Due to technological bottlenecks, lack of skilled professionals, and less operable processes, security operations eventually cannot work out for the best. The following figure displays a threat analysis system framework that Is based on terminal traceback data and involves multiple data processing and analysis modules. Critical technological challenges brought by big data in security operations can be summarized as follows:

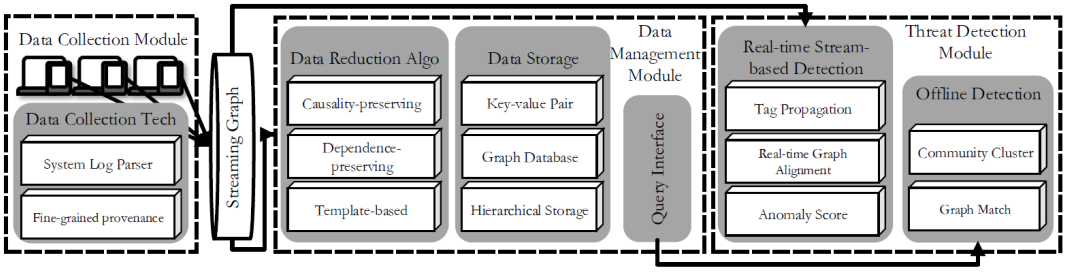


Figure 2 General technical framework of the traceback data analysis system[ii]

- Data access: data expansion and system bottlenecks. Explosive growth of security operations data places unparalleled performance pressure on the network, storage system, and processing system.
- Data fusion: multisource heterogeneity and ontology modeling. Due to the lack of a uniform graphical model design for multisource and multidimensional data, it is urgent to form associable data views via ontologization and standardization.
- Clue discovery: retrieval models and a high rate of false positives. For instance, anomaly detection models tend to have a high rate of false positives due to the lack of contextual support for threat events retrieved by using key signatures or patterns.
- Event deduction: semantic fuzziness and dependence explosion. Data-driven analysis methods usually lacks security semantics modeling or the analysis of causal relationships involved in data dependence.
- Human-machine collaboration: black-box models and low interaction. Opaque and complex models and operations platforms featuring low interaction or even no interaction reduce the effectiveness of human-machine collaboration during security operations.
- Intelligent engine: attack expiration and data risks. As more attacks are targeting intelligent models, the security robustness of models should be increased to prevent model data theft.

3. AISecOps System

3.1 Core Connotations

Literally, AISecOps is composed of three core technologies, i.e. AIOps, AISec, and SecOps.

AISec-enabled technology fusion brings new expectations to the industry. Both AI security and AI-based security applications have become hot topics in academia and industry. AI has been successfully applied in multiple single-point security technologies and specified scenarios, such as malware classification, identification of malicious traffic, and intrusion detection.

AIOps (intelligent IT operations) is a research focus in the whole Internet and intelligent computing fields[iii]. It focuses on anomaly detection, root cause orientation, alert analysis and diagnosis, and other critical technologies in complex IT system environments. Unlike SecOps, AIOps lacks systematic modeling of core risk factors, such as network threats, vulnerabilities, and assets. In addition, AIOps-related technological experience cannot be used in SecOps scenarios.

Serving as both an application scenario and objective, SecOps mainly consists of three core elements: process, person, and technique. Here, we focus on the technology element. For traditional security operations, technical capabilities are provided by security experts, including alert classification and grading, threat hunting, sample analysis, and threat traceback. However, security experts' operations capability falls short of what is required to respond to quickly expanded protection requirement. The severe talent shortage and bottleneck is increasingly apparent. Thus, it is pressing to explore the AISecOps solution.

Figure 3 Breakdown of core technical capabilities of AISecOps

This paper summarizes core connotations of AISecOps to make clear how this technique is implemented and evolves:

"Geared towards security operations goals, AISecOps, based on integration of personnel, processes, and techniques, and data, serves security risk control and key defense phases, including prevention, detection, response, predication, recovery, and other critical links in cybersecurity risk control and attack and defense confrontation. Establishing a data-driven and highly automated trustworthy intelligent security technology stack, it provides the perception, cognition, and action capabilities and even replace manual security operations services in a dynamic environment."

Unlike single-point integration of intelligent technologies and the security field during AISec practices, AISecOps, in alignment with core operations indicators, implements systematic, in-depth, and multidimensional intelligent technique solutions to adapt to different security operations phases and scenarios. This imposes new requirements for the robustness, credibility, and security of AI technologies.

3.2 Indicator System

As mentioned above, security operations goals guide the development of technical capabilities. Considering critical security operations requirements, here we present AISecOps's indicator hierarchy from top to bottom: vision, operational indicators, and technical indicators. Technical indicators can be further divided into data indicators and analysis indicators.

Security operations goals give direction and guidance to cybersecurity operations capabilities. AISecOps's indicator hierarchy is used to access the effectiveness of technical implementations. At the top of the hierarchy is the security operations vision of the enterprise, organization, or country. Under the guidance of the vision, security operations indicators are developed shown in the middle of the hierarchy. Furthermore, the indicators are broken down into data indicators and analysis indicators at the bottom of the hierarchy.

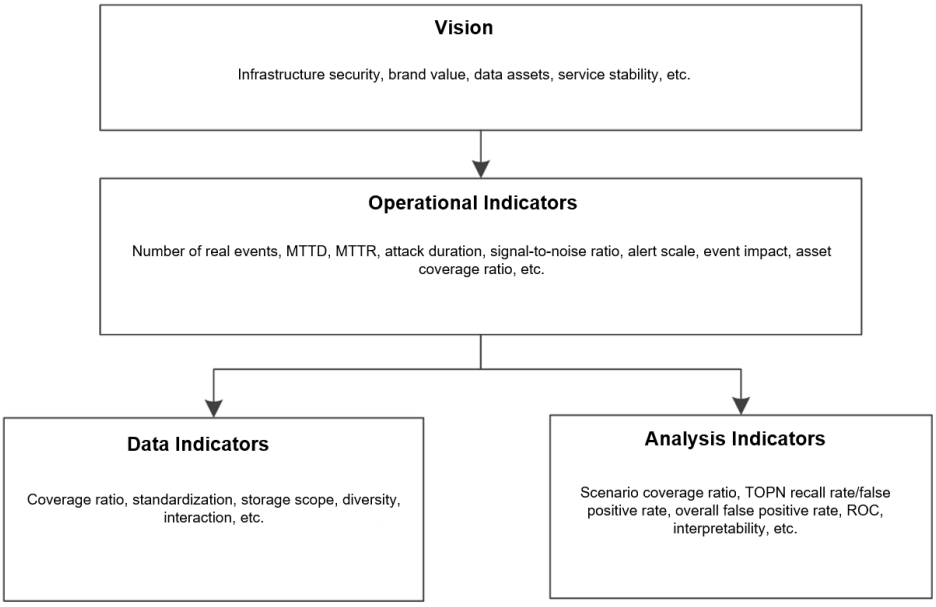


Figure 4 AISecOps indicator hierarchy

The vision refers to core goals for security, services, and business of enterprises, organizations, and countries, such as maintaining stable operation of IT infrastructure, protecting core data assets, and ensuring the security of the brand value. The vision is inseparable from the development goals of subjects.

Consistent with the security operations vision, operational indicators are developed to access security operations capabilities. The data fusion capability and data analysis capability are evaluated to promote the iteration of technical capabilities.

In terms of data, we need to consider such indicators as the coverage ratio, standardization, storage timeliness, diversity, and interaction. In addition to technique (such as machine learning) assessment indicators like predication accuracy, recall rate, and ROC, we should focus on the scenario coverage ratio, TOPN recall rate/false rate positive, overall/single-point false rate positive, model interpretability, and other indicators for operability and ease of operations, with a view to promoting the deep integration between techniques, personnel, and processes.

3.3 Data Classification

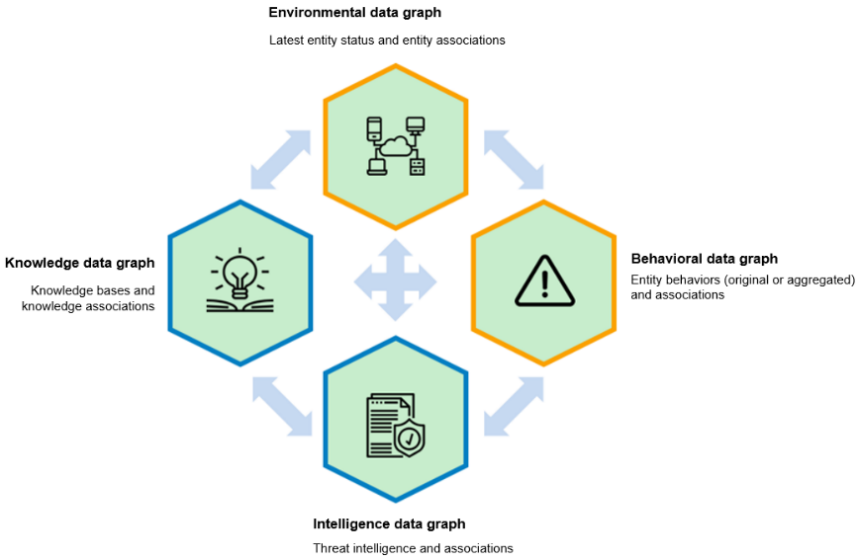


Figure 5 Core data graphs of AISecOps

- Currently, access to massive multidimensional security big data opens a new door to discovering and handling network security threats through data analysis. Considering limited resources available for storage and computing, it is especially important to identify security data sources and manage them in a unified way. With an aim to protect assets and crack down on threat actors in the given cyberspace, intelligent data analysis should focus on data collection and development of the following data graphs. This makes a sharp contrast to DIKW's[iv] and hierarchical data model and CyGraph's[v] cybersecurity/mission knowledge stack:
- Environmental data graph: presenting assets, vulnerabilities in assets, files, users, and the IT system architecture.
- Behavioral data graph: including network-side alerts, device-side alerts, file analysis logs, application logs, honeypot logs, and sandbox logs.
- Intelligence data graph: various types of external threat intelligence.
- Knowledge data graph: various types of knowledge bases (such as ATT&CK[vi], CAPEC[vii], and CWE[viii]).

Various types of security association data (including but not limited to the preceding four) have been adopted in many big data analytics scenarios, but a mature and unified standard is not yet developed to represent the classification and use patterns of such data. Based on practices in analyzing cyber threats, the preceding four types of data are organized in the form of graphs to associate data of the same type and data of different types, so as to meet fundamental tactical requirements of cyber warfare for control of the environment, understanding of threat actors' motives, integration with external intelligence, and accumulation of basic knowledge. Though independent, the four graphs are associated with one another via entities of a specified type, thus ensuring clear representation of data while achieving global linkage.

3.4 Technical Framework

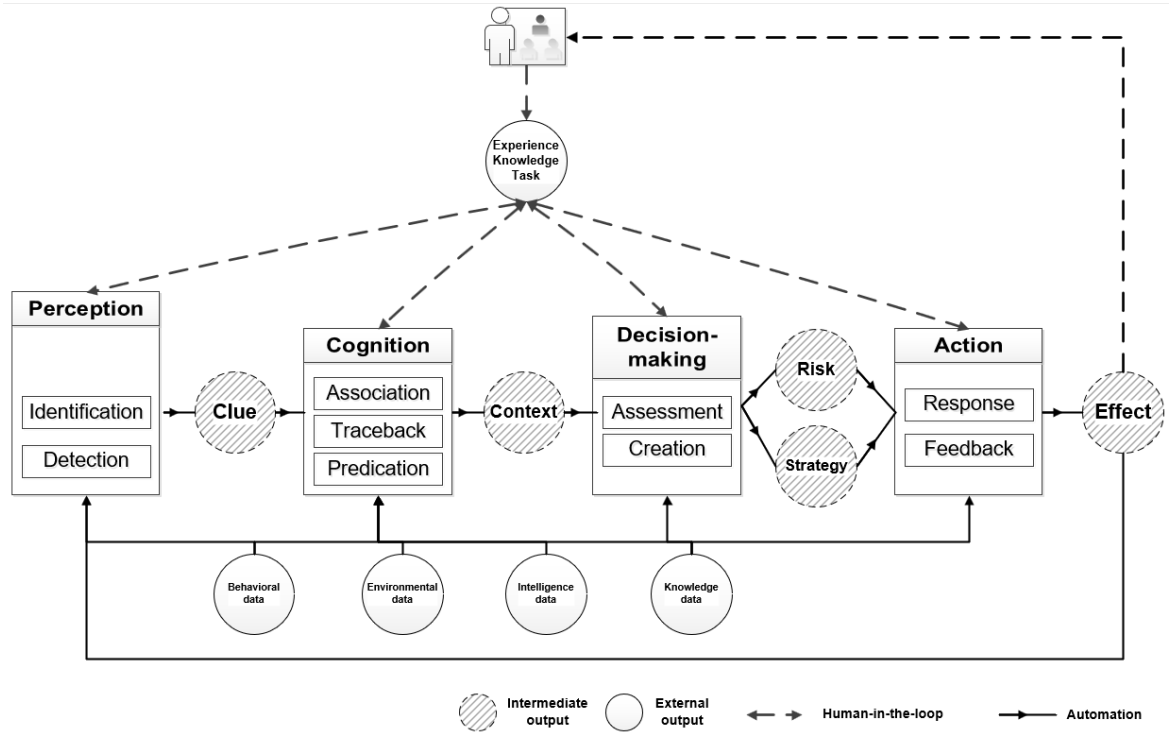


Figure 6 Technical framework of AISecOps

By reference to the classical paradigm of AI (perception – cognition – decision-making – action) and classical version of the OODA loop model (Observe – Orient – Decide – Action)[ix], this framework divides the security operations process into several stages, each of which involve different child tasks. The following details each stage and related child tasks.

- **Perception:** data fusion and information tagging, including identification and detection child tasks. Identification child tasks categorize, deduplicate, and standardize entities (assets, signatures, vulnerabilities, etc.) and their behaviors in massive data to promote fusion of multisource heterogeneous data. Detection child tasks capture and tag anomalies, vulnerabilities, threat signatures, and other critical dynamic and static information from the massive data pool to provide critical clues for threat analysis, hunting, and risk analysis.
- **Cognition:** retrieval and building of clues and event context information through child tasks for association, traceback, and predication. Association child tasks provide an exhaustive information connection view through integration of various types of multidimensional information that spans a long time period. Traceback child tasks, through traceback and root cause analysis, identify and ascertain event sources and determine the casual relationship and dependency between events. Based on the current information context, predication child tasks rely on path predication and trend analysis to predict potential attacks and high-risk vulnerabilities, so as to getting ahead of attacks by rapidly identifying the attack intentions and adopting appropriate protection methods.
- **Decision-making:** generation of assessment and creation child tasks through risk assessment in accordance with the predefined goals. In alignment with the core operations indicators, assessment child tasks, based on critical information such as behavior, environment, and knowledge, provides the ongoing overall situation and network risk level, informing optimal risk reports under a certain operating cost. Based on dynamic environments and behaviors, creation child tasks adaptively choose and generate effective risk-informed action plans and policy to clarify specific action steps.
- **Action:** accomplishing action goals through collaboration of action units, in accordance with plans, policies, and steps. This phase involves child tasks for response and feedback. Response child tasks involve policy dispatch, device deployment, patch update, error tolerance, and other risk response actions by platforms, modules, or devices, or via instruction sets. Feedback child tasks continuously collect response action execution results to generate feedback reports that aggregate data for interaction of multiple operating elements (process, person, and technique), informing subsequent automated tasks.

The preceding stages and their related child tasks are critical capabilities to enable cybersecurity operations to evolve towards higher automation. Overall, the technical framework of AISecOps contains two major loops. One is the machine self-loop in the area enclosed with solid lines in the figure, which is the ultimate goal pursued by AISecOps for automation of critical operation tasks. The other is the human-in-the-loop (HITL) in the area surrounded by dotted lines, which highlights human interaction during each key operations automation phase and manual acquisition of data feedback from machines. The key to high-level operations automation still lies in hierarchical analysis and digging of "data-information-knowledge" in response to dynamic cyberspace environments and highly interactive combats between attackers and defenders. Therefore, we can see only by increasing hierarchical task capabilities of cyberspace data can security task automation be achieved. The current intelligence level of threat identification, traceback, predication, and other critical technical capabilities hardly gives full support for SOAR-based precise responses. Various types of technical bottlenecks, such as false positives, mistaken connection blocking, and black boxes in decision-making, make it hard to achieve more highly automated intelligence in high-risk security scenarios that involve critical decision-making. Thus, fully integrated human-machine intelligence is especially critical at the current stage.

3.5 Technology Readiness Levels

Given the fact that traditional intelligent security practices hardly match urgent needs of security operations, NSFOCUS proposes multi-stage AISecOps Technology Readiness Levels (TRLs), i.e. a method of establishing a matrix of automation capabilities. This method allows the use of uniform semantics for horizontal and vertical location of the development level, status quo, application scope, and application depth of relevant technologies with a unified meaning.

Automation Level	Name	Definition	Task Stage									Data Interaction (DIKW Model)
			Perception		Cognition			Decision-making		Action		
			Identification	Detection	Association	Traceback	Predication	Assessment	Creation	Response	Feedback	
L0	No automation	All SecOps tasks are completed by the SecOps personnel.										Data collection
L1	Operations auxiliary	An automated operations system completes multiple child tasks in perception, cognition, and decision-making stages. Other operations are performed manually.										Data integration and information processing
L2	Partial automation	For designated preliminary tasks, an automated operations system completes child tasks throughout the operations process and completes data interactions with operations personnel.										Information fusion and knowledge acquisition
L3	Conditional automation	An automated operations system completes all child tasks throughout the process, including those in the action stage. Manual responses are required at critical stages.										
L4	High automation	Under restricted scenarios, an automated operations system completes all child tasks throughout the process, including those in the action stage. Manual responses are not necessarily required.										Knowledge understanding and accumulation
L5	Full automation	In any scenario, an automated operations system completes all child tasks throughout the process, including those in the action stage. Manual responses are not necessarily required.										

Completed by the operations personnel — Without the participation of the operations personnel

Figure 7 AISecOps TRLs

By reference of automation levels of self-driving[x], we came up with a taxonomy of automation levels (from no automation to full automation) to measure the ability to automate key security operations tasks. The important part of security operations is conceptually divided according to the classical AI paradigm "perception – cognition – decision – making-action". The whole process corresponds to the OODA loop model consisting of four elements: Observe – Orient – Decide – Action. The perception layer features identification (such as entity identification and classification) and detection (such as threat detection) tasks; the cognition layer involves association (such as analysis of multisource data integration), traceback (tracing back attack paths), and predication (predicating attack behaviors) tasks; at the decision-making layer, assessment (such as comprehensive risk assessment) and creation (such as policy and scheme generation) tasks are performed; at the action layer, response (such as policy deployment) and feedback (such as active reporting) tasks are executed. Whether the tasks at each level are effective depends on the maturity of the upper level. The following briefly describes the different levels of AISecOps automation capabilities:

- **L0 (no automation):** All security operations tasks are completed manually. AI and other analysis technologies can provide identification and detection capabilities at a certain level which refer to high-level data collection capabilities, but have nothing to do with any security operations tasks.
- **L1 (operations auxiliary):** In line with security operations indicators, the automated operations system participates in some child tasks for environmental perception, information processing cognition, and risk assessment. At this automation level, the system provides routine data analysis as an auxiliary means, instead of performing any child tasks of automated action.

- **L2 (partial automation):** In certain single environments, the automated operations system take part in child tasks throughout the security operations process and make continuous data and knowledge interactions with operations personnel.
- **L3 (conditional automation):** Under all task scenarios, the automated operations system completes all child tasks, including those in the action stage. Manual responses and system takeover are required at critical stages
- **L4 (high automation):** Under restricted complex scenarios, the automated operating system performs security operations in a fully automated way in accordance with predefined operational indicators, without manual interventions.
- **L5 (Full automation):** Under any complex scenarios, the automated operating system performs security operations in a fully automated way in accordance with predefined operational indicators, without manual interventions.

AISecOps technology readiness levels relieve technical practitioners of a bother of the technology bubble. Currently, the security operations intelligence is mainly in L1 and L2 levels, with higher-level breakthroughs in multiple single-point technologies.

3.6 Frontier Techniques

AISecOps is evolving at a rapid pace, with quick iterations in applied technical solutions. To explore the direction of future AISecOps development and identify bottlenecks in key capabilities, we draw a technical graph to present 16 fundamental frontier techniques for automated and intelligent security operations, with a view to creating a technical graph for cybersecurity operations scenarios.

Horizontally, the technical graph divides attack identification techniques into several types from micro to macro levels: fingerprint and signature, technique and behavior, tactic and intention, group and organization, and campaign and situation. Vertically, the technical graph categorizes classic AISecOps techniques into fusion modeling at the data layer and risk perception, causal cognition, robust decision-making, and reliable action at the analysis level. Meanwhile, vertical techniques are indicated by color in terms of core data sources that contribute environmental data, knowledge data, behavioral data, and multidimensional comprehensive data. A clear division of AISecOps into 16 types provides a solid basis for fine-grained abstraction and integration of technical schemes and building of basic capabilities of the AISecOps platform.

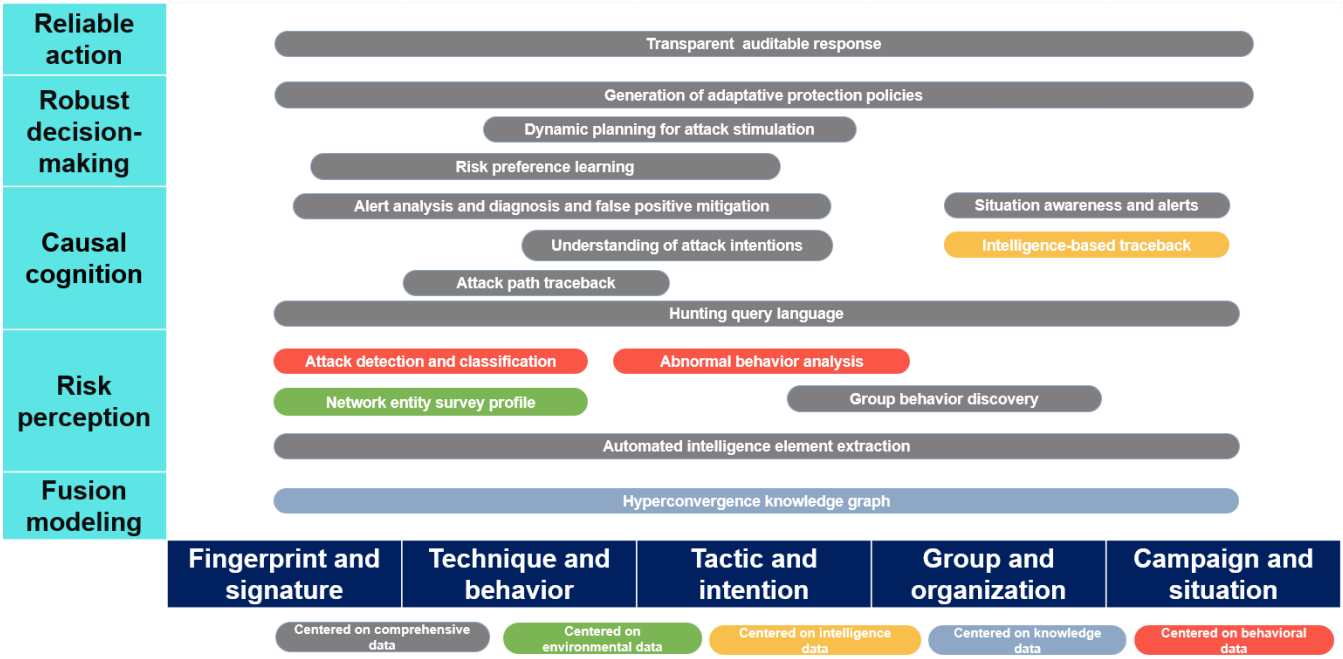


Figure 8 Graph of frontier AISecOps techniques

4. AISecOps Development Trend

As an old saying goes, "Rome was not built in a day", it is impossible to build AISecOps capabilities simply by following the example of other businesses. In fact, the most topical and mature AI technology is widely applied, but needs to be delved a little deeper. For instance, typical intelligence services like intelligence speech and image recognition only implements low-level perception. In security, economic, and political scenarios and life-critical technical scenarios like military, finance, healthcare, self-driving, and legal rulings, the current AI techniques can achieve partial automation for critical task decision-making, but remained far from achieving full automation. Cybersecurity operation is among the scenarios. Essentially, the reason why AI techniques fail to penetrate deeply in various sectors is because these techniques are not mature enough to win people's trust. In view of this, in this chapter, we look ahead of the development of intelligent security operations techniques by explaining how to build a trustworthy intelligent security system and an AISecOps technique ecosystem.

4.1 Building a Trustworthy Intelligent Security Technology System

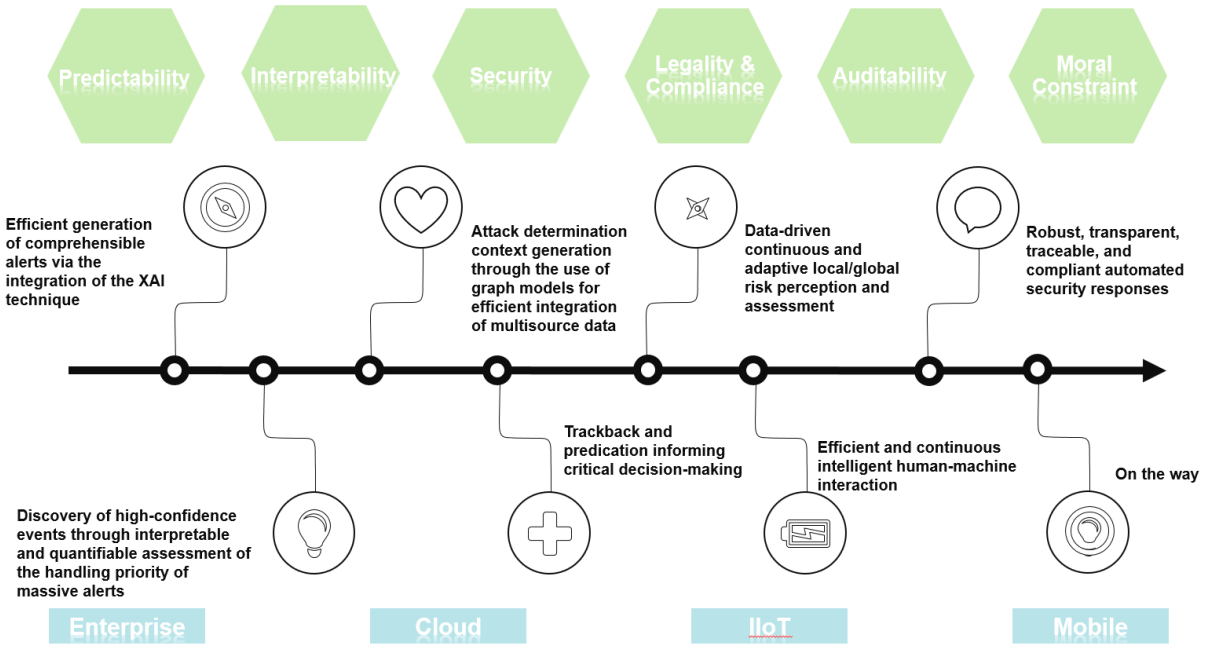


Figure 9 Technological elements of a trustworthy intelligent security system

Anyway, building a trustworthy AI system to make up people's inherent defects in handling massive data is the ultimate pursuit of practitioners. AI techniques that empower cybersecurity can be directly used in non-core scenarios and processes of cybersecurity data analysis to contribute to security assurance. For instance, use the natural language processing technique to analyze threat intelligence, build a conversational bot powered by the expert system, or use a mature image processing technique to detect malicious images and videos. Moreover, it is essential to sharpen AI technologies to apply them in core security phases like threat detection, assessment, association, and response. As shown in the preceding figure, from the perspective of building technical trust, to increase the automation of critical security capabilities, trustworthy intelligent security must meet the requirements of the following core technological elements: 1. Predictability: able to be adapted to highly dynamic network environments and attack scenarios. 2. Model algorithm: features transparency, interpretability, security robustness, and privacy protection. 3. Intelligent technique: ensuring legitimate, compliant, and auditable technique applications and application results; consistent with the code of ethics when applied for decision-making. These technological elements complement and depend on each other, and consideration should be given to them at the early design stage. Just as we prefer to work with those people that have good character, excellent communication skills, are able to work efficiently under great pressure, and observe laws, we can build trust in AI only if it has the same good traits to be competent to accomplish security operations tasks in a highly automated way.

While seeking to build a trustworthy intelligent security system, we need to fully integrate explainable artificial intelligence (XAI), privacy protection technology, graph mining and analysis, intelligent decision-making system, risk assessment, and human-machine interaction among other multidisciplinary and multifield intelligent technical capabilities so as to empower tasks at perception, cognition, decision-making, and action stages of the security operations process.

4.2 Building an AISecOps Technique Ecosystem

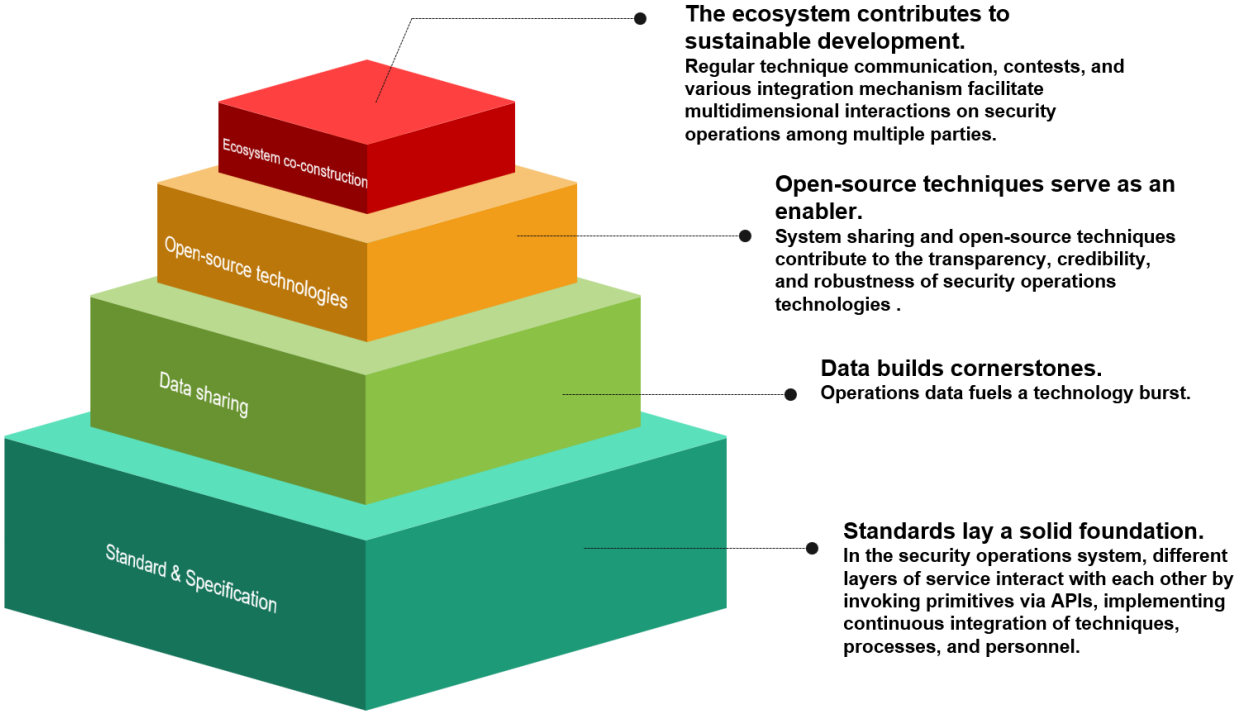


Figure 10 Building an AISecOps technique ecosystem

Therefore, it is urgent to build an AISecOps technique ecosystem, no matter whether to satisfy actual needs or better adapt to technique development. As shown in the preceding figure, the AISecOps technique ecosystem consist of four levels: standard & specification, data sharing, open-source technologies, and ecosystem co-construction. By establishing industrial and national standards, we can develop uniform and normative critical security operations process and technical interface to ensure a clear division of labor. Through data sharing, we should set up a test arena for security operations technologies to encourage competition and contests of technical capabilities. Making techniques open source, we should build a thriving technical community to attract and cultivate more security operations talents. Finally, we should set up a communication platform and mechanism to facilitate communication and cooperation, ensuring regular technical exchanges in all aspects.

5. Conclusion

Cybersecurity technologies have entered a new stage of development that centers on adaptative control and operations of security risks throughout the lifecycle. Given the influx and integration of massive, multisource, and high-dimensional operations data, it is vital to build a trustworthy and operable AISecOps system in a new era of digital infrastructure to advance towards a highly intelligent and automated cybersecurity defense system while greatly facilitating security operations. For this reason, we propose the AISecOps system after a comprehensive dissection of critical technical challenges for analyzing security operations big data. In this whitepaper, revolving around security operations practices, we go deep into the technical connotations, indicator system, data classification, technical framework, and AISecOps technology readiness levels, present the graph of frontier AISecOps techniques, and predict the development trend of AISecOps techniques. We expect this whitepaper to provide useful guidance for advancement of the AISecOps system and ecosystem co-construction, giving a practice-driven impetus for the development of cybersecurity operations technologies.

6. References

[i] Security Operations Primer for 2020, Gartner, https://www.gartner.com/en/documents/3978969/security-operations-primer-for-2020

[ii] Li Z, Chen Q, Yang R, et al. Threat Detection and Investigation with System-level Provenance Graphs: A Survey[M]. arXiv preprint arXiv:2006.01722, 2020.

[iii] Dang Y, Lin Q, Huang P. AIOps: real-world challenges and research innovations[C]// 2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), 2019: 4-5.

[iv] Rowley, J. The wisdom hierarchy: representations of the DIKW hierarchy[J]. Journal of information science, 2007, 33(2): 163-180.

[v] Noel S, Harley E, Tam K H, et al.: CyGraph: graph-based analytics and visualization for cybersecurity, Handbook of Statistics: Elsevier, 2016: 117-167.

[vi] https://attack.mitre.org/

[vii] https://capec.mitre.org/

[viii] https://cwe.mitre.org/

[ix] Grant T. Unifying planning and control using an OODA-based architecture[C]. Proceedings of Annual Conference of the South African Institute of Computer Scientists and Information Technologists, 2005: 111-122.

[x] https://en.wikipedia.org/wiki/Self-driving_car