



MonSys: A Scalable Platform for Monitoring Digital Services Availability, Threat Intelligence and Cyber Resilience Situational Awareness

George Sharkov^{a, b},  (✉), **Yavor Papazov**^{a, b}, **Christina Todorova**^{a, b}, , **Georgi Koykov**^{a, b} and **Georgi Zahariev**^{a, b}

^a European Software Institute – Center Eastern Europe, Sofia, <https://esicenter.bg/>

^b Cybersecurity Laboratory at Sofia Tech Park, <https://sofiatech.bg/>

ABSTRACT:

Today's digital society implies interconnectivity between the online operations of different sectors of everyday life and economy alike. As a consequence, malicious activities targeted towards a single online service could hurt entire industries and multiple private and public organizations. This interdependence between online services and economic units is an imperative for targeted efforts ensuring the integrity and availability of individual systems and complex systems-of-systems alike. This article presents MonSys, a flexible, robust, and scalable monitoring platform, implemented as a cloud-based service and an on-premise solution, specifically designed to address the need for ensuring service availability at an individual level. MonSys provides several standardized services availability checks, such as web-based services from multiple geographical locations, and a flexible platform and tools for defining customized complex services. Particular attention is paid to the processes of metrics collection, processing, storage, and querying. MonSys can perform custom availability checks for different types of infrastructures, such as various black-box, grey-box, and white-box availability checks/metrics. The article presents also results from piloting the platform on performance and scalability and options for integration in early-warning and intelligent signaling, based on behavioral pattern analysis and predictive simulations.

ARTICLE INFO:

RECEIVED: 7 JULY 2020

REVISED: 31 AUG 2020

ONLINE: 7 SEP 2020

KEYWORDS:

scalability, cyber threat, vulnerability analysis, cyber risk, resilience, early warning, situational awareness



Creative Commons BY-NC 4.0

Background

The rapid development of the information and communication technologies (ICT) sector has a profound effect on the quality of everyday life both at an individual level, as well as on economical, and national security level alike.^{1, 2} Although ICT increases the efficiency and effectiveness of various services and industries, in the meantime, it provides opportunities for malicious actors to cause significant damage without exercising physical coercion.^{3, 4, 5} Among the core values of a digitized society are its interconnectivity and reliability.^{6, 7} This ultimately leads to interdependence between economic sectors and to an amalgamation between the digital and analogue business operation, while in the meantime allowing for an ever-growing attack surface.⁸ The pervasive interconnectivity implies as consequence the progressively dangerous perspective that malicious activities targeted towards online services, could strategically be employed to hurt entire sectors as well.⁹ This reliance and loose coupling between online services from different sectors and operational units implies a need for targeted efforts to ensure the integrity and availability of individual systems as well as of the complex composite systems-of-systems (SoS) alike.¹⁰

In this contribution, we provide a detailed summary on the development of MonSys, a flexible, robust, and scalable monitoring platform for situational awareness and monitoring of online services, developed by our team and implemented as a cloud-based platform and an on-premise solution. MonSys is a scalable platform for monitoring digital services availability, threat intelligence and cyber resilience situational awareness. We will further present some key findings and core future directions for development and contextual implementation of the platform.

This paper is organized as follows. Within the *Accessible and Dynamic Monitoring of Services Availability*, we provide information about the context, which necessitated the provision of the public and private sector with tools for early warning, threat intelligence and vulnerability monitoring. Following that, in the *Monitoring Platform* chapter, we provide insight into the functionality of the platform, with relevant information divided into the following categories: *Architecture, Deployment, Alerting, Frontend (Dashboarding, Managing services, Subscription transparency)*. We then go on to summarize some of the *Key Findings and Use Cases* and provide *Conclusions*.

Accessible Dynamic Monitoring of Service Availability

Over the last two decades, cyber-attacks ranging between malicious activities against personal computers and critical infrastructures and online services and operations of organizations from both the private and the public sector, have been on the rise.¹¹ This fueled a world-wide research in the field of intrusion detection and intrusion prevention. Although Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) research has begun during the later years of the past century,¹² the rapid technological development and against the progressively complex backdrop of the cyber-attacks has led to an increased effort in intrusion prevention research during the recent years.¹³

A vast majority of both the scientific and the commercial advances in the field however, are focused on developing complex solutions for either large enterprises or specific infrastructures, which makes it profoundly inaccessible for small and medium sized enterprises (SMEs), academic and non-profit organizations to be able to afford, administrate, manage or even consider employing IDS/IPS to their context. Furthermore, as some network-based IDPSs (Intrusion Detection / Prevention Systems), such is to a certain degree the MonSys platform as well, have been associated with high rates of either false positives or false negatives (which require a lot of manual filtering), as well as the need to administer and put a lot of effort into the customization to the monitored environments,¹⁴ a lot of the smaller or not as IT-intensive companies and organizations, have been reluctant to consider adopting IDPS into their organizational cybersecurity and cyber-defense strategies.

However, IDPSs serve a crucial role in the improvement of the overall cybersecurity posture within an organization, and by inference, of an entire sector or a network of interconnected online services. An anomaly-detection intrusion prevention system, such as MonSys, would most commonly gather historical data regarding the standard baseline of activity and availability of a given service. Then, based on parameters, key metrics and historical intelligence, such systems would monitor, detect and alert the owner of a system of key services dropout, malicious or suspicious activities, etc., and some systems would further issue an automatic response to these activities.¹⁵

This context calls for efforts in creating accessible and intuitive platform, build into robustness, flexibility, and adaptability, while offering possibilities for personalized tests, recommendations, alerts and many more.

This contribution presents an approach for making intrusion prevention and detection more accessible to organizations of various contexts, size and line of action, in order to improve the cyber-stability and the overall cybersecurity posture on a larger scale and build cyber-resilience and sectoral capabilities and awareness on the topic of cybersecurity. Furthermore, with the development of the MonSys platform, the implementation team aimed at improving the cybersecurity situational awareness of organizations from both the public and private sector, by providing them with information and sector-relevant cybersecurity statistics and research-informed and data-driven recommendations through the integration of the previously developed by the same team Cyber-Map Bulgaria instrument within the MonSys platform.

Monitoring Platform

MonSys aims to provide a *flexible*, *robust*, and *scalable* monitoring platform. Particular attention is paid to the processes of metric collection, processing, storage, and querying.

Architecture

To provide a *scalable* base for the implementation of the MonSys platform, the team chose the Kubernetes platform, which builds upon existing container infrastructure, however, provides a different and higher-level set of abstractions,

designed to empower and improve modern development and IT operations and their respective workflows.

Among the core advantages of the Kubernetes platform choice were the following:

- scalability – in a Kubernetes cluster, scalability refers to the ability of the cluster to grow while staying within its service-level objectives (SLOs).¹⁶
- loose coupling (another staple of the microservice / container-oriented approach), and particularly the ability to combine technologically diverse components and manage versioning of separate components in an independent manner.
- security and availability – Kubernetes has an in-built enterprise access control toolkit, as well as simple (self-)monitoring tools.

To provide the other main claim of the architecture design – flexibility, the team utilized an innovative computational paradigm – Function-as-a-Service (FaaS). With FaaS technologies, the “consumer” of the service can provide custom source code to be executed in the designated runtime environment, usually in the form of a container, running dynamically mounted code. This code must run in a timely manner (standard limitations are between 5 and 15 minutes) and should have similar granularity to that of a function (thus explaining the name of the paradigm). By utilizing the FaaS paradigm, MonSys can perform custom availability checks for different types of infrastructure, such as various black-box, grey-box, and white-box availability checks/metrics.

The flexibility and scalability, being the core advantages of the platform, would allow for applications in challenging areas, such as:

- Monitoring fleets of millions of IoT devices, in either push or pull mode.
- Collecting data on availability and/or security for entire vertical or horizontal supply chain segments.
- Extracting real-time data from highly specialized services that require specific test setup, process, or infrastructure.

Some notable drawbacks of the current architectural approach are:

- *Cost*: the current platform has a high “at rest” runtime cost. In practical terms, this means that under 0 % external load, a platform deployment will still require substantial funds to operate (on a public cloud provider). However, with a higher load (number of domains/services and test frequency) the cost per test is much below 0.005 cents.
- *Not fully tested*: due to the innovative architecture, the informal knowledge base of the technologies involved, as well as the ‘best practices’ in integrating them, are still under continual development and pilot testing.

Deployment

The team implemented the above architecture in a (mostly) minimal configuration, foregoing some operational concerns, such as High Availability (HA), backup and multi-region availability. These can be trivially (although at a noticeable price) addressed at the Kubernetes implementation level.

The platform also necessitated the development of a somewhat standard three-tier Web application that serves as the UI for the project. This Web application was developed in Python and deployed as an FaaS application on the Kubernetes cluster.

The platform builds on top of one of the most common monitoring components – Prometheus. As the native monitoring solution for Kubernetes, it provides additional architectural and implementational cohesion, due to the number of pre-developed plugins/extensions that can be used to attach Prometheus to many standard infrastructure setups and products.

Within the platform and to further facilitate cybersecurity situational awareness, the development team further integrated the functionality of a previously developed instrument, called CyberMap Bulgaria¹⁷. Cyber Map Bulgaria is a fully-functional software system which provides and visualizes data that could be further used for conducting multi-faceted analysis on topics such as chronic vulnerabilities of the Bulgarian cyberspace per domain or sector or identifying critical points in the Bulgarian IT public and private infrastructure. For the creation of CyberMap Bulgaria, the implementation team developed and implemented a method for the non-intrusive collection of technical, geographical, organizational, and other data for the experimental database of more than 55,000 Bulgarian domains and domain groups.

A simplified architecture of the platform is visualized below in Fig. 1:

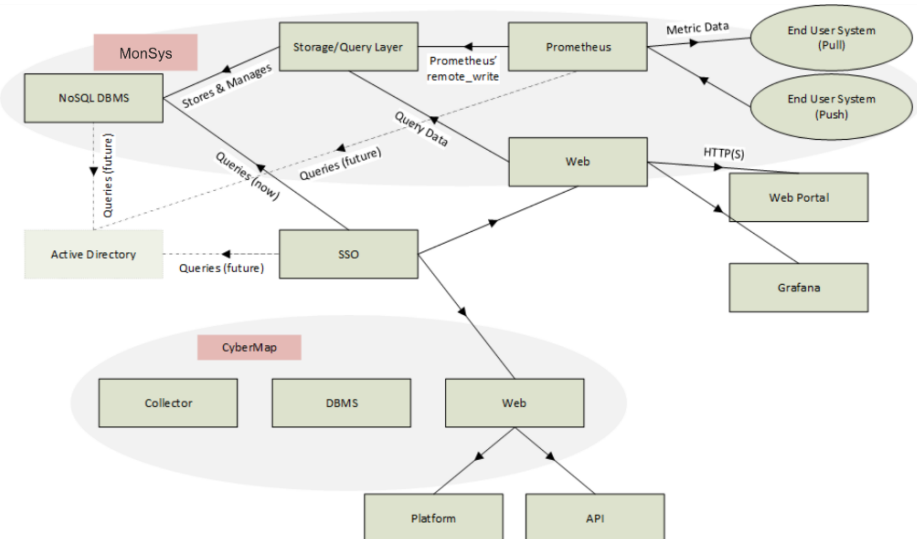


Figure 1: General Architecture of MonSys and the integration of CyberMap Bulgaria within it.

Unlike most other monitoring products and platforms, MonSys treats Black-box tests as first-class objects and a significant amount of effort has been allocated towards servicing and orchestrating such tests in an easy and maintainable fashion. Black-box tests are particularly relevant to the quality of the end-user experience and satisfaction, as (contrary to what most monitoring tools assume), the actual end-user is very rarely, if ever, present within the datacenter or server room, which is the accuracy domain of white-box tests. Real-world service availability and quality also depends on the service supply chain and even on the end-user's network infrastructure, such as their ISP. White-box tests do not account for any of those factors, since they (by definition) monitor only infrastructure the service provider has control over.

To improve the available facilities for black-box testing, the team addressed some underlying technological limitations, such as the execution time for FaaS tests (which is theoretically unlimited in MonSys, unlike most public cloud FaaS services). The team also invested in the development of several black-box tests and test tools that can be leveraged to provide better insight into the availability of the respective services.

The following tests and test frameworks were implemented:

- In-Browser Black Box Testing Toolkit – based on Selenium (as a starting point), this framework allows for running user-provided functional tests on Web pages and applications. Support for other in-browser testing platforms, such as cypress.io and puppet, is possible, but not implemented at present.
- WordPress – being the most widely used platform for content-management and blogging (Built With 2020), WordPress has abundant user-base that can benefit from improved availability data transparency.¹⁸

Alerting

Among the core functionalities of MonSys is the alerting functionality. The platform revolves around the concept of user customization, and through this prism, MonSys records, analyses, and visualizes statistics with the aim of not only bringing situational awareness to the cybersecurity context of the monitored service, but also to alert the organization for a deviation from the standard line of behavior, suspicious activity or key services or functionalities dropout.

When designing the alerting functionality, the implementation team first and foremost focused on the customization of alerting and alerting mechanisms. Currently, MonSys alerts users through the platform's dashboard, e-mail and/or SMS based on pre-defined and fully customizable sets of criteria for alerting. This provides the user with autonomy over the quantity and types of alerts received, as well as the channels through which alerts of different types of priorities are received.

Support for custom alerts is implemented in a vastly similar manner to the custom tests – the alerts are running within a FaaS environment, providing (alert request) response data over HTTPS.

The alerts by default consist of automated informational and actionable items. An informational item is an item, which concerns news and information about the security status or features of applications, services, etc., employed by the monitored service. An actionable item, on the other hand, is employed when the active engagement of the user is required, such as updating of a core service, and others.

Finally, MonSys allows for human-sent notifications, such as notification by the platform's maintenance team. Those alerts are, by default, prioritized within the platform over informational or actionable alerts, however the user is fully empowered to set a customized priority on different types of alerts.

Frontend

The development of the platform also put forth the prerequisite of the development of a standard three-tier web application, which serves as a user interface for the platform. Due to internal preferences of the implementation team, the web application was developed in Python and deployed as an FaaS application on the Kubernetes cluster, allowing for a high utilization of the available resources, thus decreasing the 'at rest' cost. For the frontend component of the MonSys platform, the implementation team focused on employing a minimalistic approach to put forward usability and intuitiveness of the user interaction with the platform. The minimal design enables users to easily manage and customize the dashboards, services, alerts, tests and much more.

Following a series of interviews with relevant stakeholders regarding the user-interface of the platform and its interactivity features, the following core functionalities came forth as usability milestones, which the team managed to implement throughout the course of the front-end development.

Visualization Dashboard

The dashboard of the platform is the monitoring and control panel for the end user, where they can observe the services, customize the visualization of results, and conduct retrospectives. To support the organizational robustness, the end users needed an agile, easily customizable and adaptable dashboarding service, where they can combine and refine metrics, visualizations in a clean and minimal environment, where they can still expand and research metadata and contextual information for activity spikes, incidents and customizable service monitoring metrics.

Service, Test and Alert Management

The users of the platform emphasized the importance of being able to easily manage the services they would like to dynamically monitor and test. This means the freedom to easily add and remove services, create, and customize additional tests for separate services and the ability to customize the collected metrics, as well as alerting for specific services.

Key Findings and Use Cases

Although generally following a minimalistic paradigm of software development, the efforts of the implementation brought to fruition a robust, easily adaptable, scalable, and flexible monitoring platform.

The “classical” monitoring and alerting service for a set of standard layer-7 services (such as https, http, tcp as well as DNS availability) has been tested as a pilot for more than 6 months with more than 20 web-sites and critical information sources (governmental and public administration), as well as multiple G2B, G2C and B2B services (such as banks, revenue agency, etc.). The platform proved to be easy scalable and expandable, and useful for services saturation alerting and early warnings. Among the findings, in one particular case a typical profile of a DOS attack was detected early and alerted. Subsequently it was well correlated with the internal reports from an independent DOS-protection platform being used (Cloudflare). A typical profile of a detected by MonSys DOS attack with preparation and execution phase is shown in Figure 2.

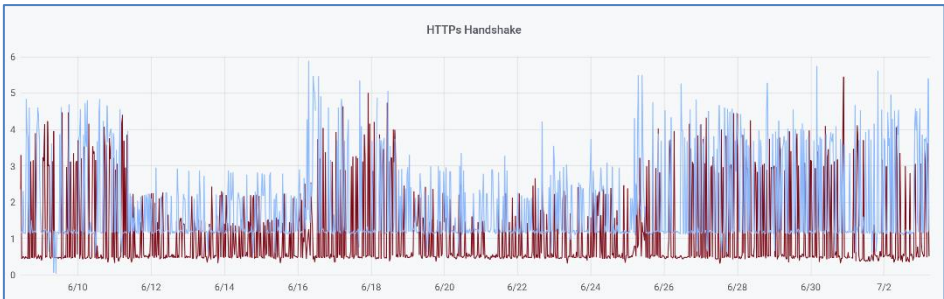


Figure 2: Typical profile of a DOS attack (over https) as detected by MonSys with clear preparation and execution phase (although not manifested at full power). Availability tests performed at frequency 5 minutes from two test points (Western Europe and USA, dark red and light blue lines respectively, delay time in seconds).

Another test case was performed to validate the use for monitoring the functionality and availability of complex interdependent services. A model of an advanced supply chain and logistics services was used for monitoring the integrity of the supply chain. Expected further benefits of practical use include Identification of “hidden dependencies” and unknown attack vectors, cascade saturation and degrading of services by response time patterns and anomalies. Monitoring the “end-service” availability and response times along with some selected key services (web or dedicated) involved in the supply chain allow to establish a generic and standardized behavior pattern. This will allow the use of tailored AI/ML methods, as in many cases (like military supplies and operations logistics) there is natural deficit of ML training data available. On the other hand, the entire logistics and supplies lifecycle is based on interoperability of interconnected systems, processes and organizations and required resilience is achieved by composite performance and risk management rather than the

“sum” of individual security and availability.¹⁹ Therefore, MonSys could be very useful by tuning to monitor and report the overall performance as well as possible compromise of web-accessible or internal (isolated services) in one integral platform and dashboard. This would help to achieve an adaptive supply chain cyber risk management.²⁰

Several pilot tests have been performed by simulating application web-forms or composite services requests in two areas - e-administration and banking/financial services by using Selenium testing toolkit. Although functional testing turned to be easy achievable (based on natural use of Selenium for black-box quality tests), the entire service response time monitoring and alerting would require additional organizational and administrative arrangements, as well as intelligent behavior benchmarking. Pilot implementations are ongoing, including testing of machine-learning methods.

Another pilot use of MonSys was for cyber/hybrid exercising. A dedicated tenant of MonSys was tuned to monitor services availability in entirely isolated platform (Exercise Cyber Range) and in real time assist the blue-teams for focused, rapid and intelligent big data search (e.g. network traffic log files, application level forensics) to identify attack signals and evidences.

The ongoing experimental work is dedicated to intelligent alerting by ML-based behavioral analysis. That also includes the exploitation of platform scalability and elastic resources management for on-demand rapid extension of testing services over thousands or millions of devices (for example, numerous IoT and IIoT) and benefit from a minimum activation time due to FaaS approach (both for lambda on AWS, or locally deployed lambda on OpenWhisk). Moreover, this is elastic enough to scale to measure up or down depending on the needs.

Conclusion

This paper examined the cybersecurity problem of early warning, prognosis, vulnerability analysis and threat prevention, which motivated the development and functionalities of a scalable platform providing tools for the dynamic monitoring of digital services availability.

The ever increasing cyber-attack surface, empowered by the interconnectivity of digital services and against the modern economical backdrop, were among the key motivators for the development of this platform, which further reflects on the need for improving the limited capability for applying cybersecurity controls, analysis and preventive measures on a national and international scale.

The development of MonSys, employed multiple research methods and state-of-the-art technical platforms for the creation of a series of interconnected instruments that work together to provide a working product, that aims at allowing an end client to use tools, means and methods for the dynamic monitoring and analysis of the behavior (availability) of the web systems of specific target groups, by adding mechanisms for monitoring, historical retrospective and identification of symptomatic behavior models, which will allow for the early warning for mass cyber-attacks and large-scale crisis threats. The native quick scalability and

customization makes the integrated MonSys platform usable at higher level for national or sectoral cybersecurity picture monitoring and resilience, as well as any complex system-of-systems, including internal enterprise and industrial systems, not necessarily internet or web based. In addition, the customizable and scalable platform allow custom services testing approach in such complex systems-of-systems, as the global supply chains, where only probing and checking the availability of entire composite services could be an indicator of hidden dependencies, subject of increasing interest of modern APTs.²¹

Our belief is that with such instruments and services we will be able to improve the efficacy of predicting, preventing, and handling cybersecurity incidents and improve the overall cybersecurity posture of Bulgaria or any other cyber ecosystem. By providing a flexible, scalable, accessible, intuitive, and highly customizable platform, the implementation team's overall goal is to encourage more organizations, ideally and especially from Bulgaria, to employ IDPSs capabilities as part of their cybersecurity strategy, and ultimately help increase the overall cyber-resilience of entire sectors and networks of interconnected services.

Acknowledgements

The pilot version of MonSys is a project, financed under agreement № D-094 / 27.09.2019 by the Research and Development and Innovation Consortium (Sofia Tech Park JSC) and Nemetschek Bulgaria. The activities under the project were carried out within the period October 2019 - March 2020 by the Cybersecurity Lab at Sofia Tech Park JSC with the support of the European Software Institute - Center Eastern Europe (ESI CEE) and CyResLab of ESI CEE.

The part of the work performed by ESI CEE was supported by the ECHO project which is funded by the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943.

References

- ¹ Evon M.O. Abu-Taieh, "Cyber Security Body of Knowledge," *IEEE 7th International Symposium on Cloud and Service Computing*, 2018, pp. 104-111, <https://doi.org/10.1109/SC2.2017.23>.
- ² Klaus Schwab and Nicholas Davis, "Shaping the Future of the Fourth Industrial Revolution," *Currency* (November 2018).
- ³ Todor Tagarev, George Sharkov, and Nikolay Stoianov, "Cyber Security and Resilience of Modern Societies: A Research Management Architecture," *Information & Security: An International Journal* 38 (2017): 93-108.
- ⁴ Rossouw von Solms and Johanvan Niekerk, "From Information Security to Cyber Security," *Computers & Security* 28 (October 2014): 97-102, DOI: 10.1016/j.cose.2013.04.004.
- ⁵ Todor Tagarev and Dimitrina Polimirova, "Main Considerations in Elaborating Organizational Information Security Policies," *CompSysTech '19: Proceedings of the 20th*

- International Conference on Computer Systems and Technologies*, June 2019, pp. 68-73, <https://doi.org/10.1145/3345252.3345302>.
- ⁶ Adéle da Veiga, Liudmila Astakhova, Adéle Botha, and Marlien Herselman, "Defining Organizational Information Security Culture – Perspectives from Academia and Industry," *Computers & Security* 92 (May 2020), 101713, <https://doi.org/10.1016/j.cose.2020.101713>.
 - ⁷ Alessandro Sforzin, Félix Gómez Mármol, Mauro Conti, and Jens-Matthias Bohli, "RPiDS: Raspberry Pi IDS - A Fruitful Intrusion Detection System for IoT," *Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress*, 2016, pp. 440-448, <https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0080>.
 - ⁸ Jeannette Wing and Pratyusa Manadhata, "An Attack Surface Metric," *IEEE Transactions on Software Engineering* 37, no. 3 (May-June 2011): 371-386, <https://doi.org/10.1109/TSE.2010.60>.
 - ⁹ Hatma Suryotrisongko and Yasuo Musashi, "Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective," *IEEE 12th Conference on Service-Oriented Computing and Applications, Kaohsiung, Taiwan*, 2019, pp. 162-167, <https://doi.org/10.1109/SOCA.2019.00031>.
 - ¹⁰ George Sharkov, "From Cybersecurity to Collaborative Resilience," *ACM Workshop on Automated Decision Making for Active Cyber Defense, New York, NY, USA*, 2016, pp. 3-9, <https://doi.org/10.1145/2994475.2994484>.
 - ¹¹ Masato Kikuchi and Takao Okubo, "Power of Communication Behind Extreme Cybersecurity Incidents," *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress, August 2019*, DOI: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00065.
 - ¹² Robert Bridges, Tarrah Glass-Vanderlan, Michael Iannacone, Maria Vincent, and Qian (Guenevere) Chen "A Survey of Intrusion Detection Systems Leveraging Host Data," *ACM Comput. Surv.* 52, no. 6 (January 2020), DOI: 10.1145/3344382.
 - ¹³ Hao Zhao, Yaokai Feng, Hiroshi Koide, and Kouichi Sakurai, "An ANN Based Sequential Detection Method for Balancing Performance Indicators of IDS," *Seventh International Symposium on Computing and Networking (CANDAR), Nagasaki, Japan*, 2017, pp. 239-244. <https://doi.org/10.1109/CANDAR.2019.00039>.
 - ¹⁴ Liu Hua Yeo, Xiangdong Che, Shalini Lakkaraju, "Understanding Modern Intrusion Detection Systems: A Survey," *arXiv:1708.07174* (2017).
 - ¹⁵ Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih and Kuang-Yuan Tung, "Intrusion Detection System: A Comprehensive Review," *Journal of Network and Computer Applications* (January 2013), <https://doi.org/10.1016/j.jnca.2012.09.004>.
 - ¹⁶ "Kubernetes Scalability and Performance SLIs/SLOs," *GitHub*, 2020, <https://github.com/kubernetes/community/blob/master/sig-scalability/slos/slos.md>.

- ¹⁷ George Sharkov, Yavor Papazov, Christina Todorova, Georgi Koykov, Martin Georgiev, and Georgi Zahariev, "Cyber Threat Map for National and Sectoral Analysis," *Computer and Communications Engineering, Workshop on Information Security 2019, 9th Balkan Conference in Informatics, September 2019*, pp. 29-33.
- ¹⁸ Olajide Ojagbule, Hayden Wimmer, Rami J. Haddad, "Vulnerability Analysis of Content Management Systems to SQL Injection Using SQLMAP," *IEEE, SoutheastCon 2018, St. Petersburg, FL, USA, October 2018*.
- ¹⁹ Christopher A. Nissen, John E. Gronager, Robert S. Metzger, Rogers Joseph O'Donnell, and Harvey Rishikof, *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience* (Washington, DC: MITRE, 2019).
- ²⁰ Stefan Schauer, Martin Stamer, Claudia Bosse, Michalis Pavlidis, Haralambos Mouratidis, Sandra König, and Spyros Papastergiou, "An Adaptive Supply Chain Cyber Risk Management Methodology," Hamburg International Conference on Logistics, Project MITIGATE, October 2017, <https://doi.org/10.15480/882.1491>.

About the Authors

George **Sharkov** is an Adviser to the Minister of Defence and served as a National Cybersecurity Coordinator for the Bulgarian Government in the period 2014-2017. He was leading the development of the National Cybersecurity Strategy of Bulgaria, adopted in 2016. He has PhD in Artificial Intelligence, with specialization in applied informatics, thermography, genetics, and intelligent systems. Since 2003, he is the Director of the European Software Institute – Center Eastern Europe and Lead of the Cyber Resilience Lab (CyResLab) of ESI CEE in partnership with CERT-SEI, Carnegie Mellon University. Since 2016 he is also the Head of the Cybersecurity Lab at Sofia Tech Park. He is a trainer and an appraiser in software engineering quality management, cybersecurity, and resilience (SEI/CERT RMM), while also lecturing in software quality, cybersecurity, and business resilience in three leading Bulgarian universities.

Yavor **Papazov** is the technical manager of the CyResLab (Cyber Resilience Lab) – the cybersecurity division of the European Software Institute – Center Eastern Europe since its inception. He is a core content creator and leading lecturer for most of the cybersecurity trainings at CyResLab and has a wide practical research background in the field of information security, cyber ranges and simulation platforms and architectures, and cyber exercises.

Christina **Todorova** is a researcher at the European Software Institute – Center Eastern Europe and an expert in the Research and Development and Innovation Consortium (Sofia Tech Park JSC) in the with a particular area of expertise being design of digitally enhanced learning experience and curricula, especially through educational robotics, mobile applications and virtual learning environments. Her most recent research focuses on projects for cybersecurity education for teachers and high-school students, cybersecurity trainings and exercises.

Georgi **Koykov** is a software and DevOps security specialist at the CyResLab (Cyber Resilience Lab) – the cybersecurity division of the European Software Institute – Center Eastern Europe. With extensive practical experience in user experience and web development, Georgi is not only at the core of most development projects of the CyResLab, which require a user interface, but he is also among the core experts in the team with relation to web security and vulnerability analysis.

Georgi **Zahariev** is a cybersecurity specialist at the CyResLab (Cyber Resilience Lab) – the cybersecurity division of the European Software Institute – Center Eastern Europe, and an expert at the Research and Development and Innovation Consortium (Sofia Tech Park JSC). Georgi is a content creator and lecturer for cybersecurity trainings at CyResLab and is among the core experts in the team with relation to web security and vulnerability analysis.