Analysis of a HIPS Solution Use in Power Systems

Tomas Svoboda(✉), Josef Horalek, and Vladimir Sobeslav

Faculty of Management and Informatics, University of Hradec Kralove, Hradec Kralove, Czech Republic
{tomas.svoboda,josef.horalek,Vladimir.sobesdlav}@uhk.cz

Abstract. The aim of this paper is to conduct a performance comparative analysis of open-source HIPS (Host Intrusion Prevention System) solutions in order to improve security measures in power systems. First, the HIPS technology is introduced with an emphasis on its use for increasing security within power systems. Secondly, selected HIPS solutions are introduced in order to conduct the comparative analysis. Finally, the results of the comparative analysis of the individual solutions are presented with an emphasis on the use of system resources in the deployment of HIPS solutions on Windows workstations.

Keywords: Security · Cybersecurity · Power systems · SCADA · HIPS · Windows

1 Introduction

Currently, the modern society cannot function without the existence of communication connection via computer networks and access to the Internet [1]. The use of this type of communication can be observed throughout the society, be it in systems falling under critical infrastructure of individual countries, in ordinary work activities, or in private home Wi-Fi networks. With the use of these technologies comes the necessity of securing them against unauthorized use, which can, in the field of critical infrastructure and power systems, have a negative impact on the society as a whole.

Significant progress in the field of improving security of power systems was not madeuntil 2010 when Stuxnet was discovered [2]. Considering the cyberattacks on power companies in 2016 and 2017 [3, 4], it is obvious that the area of power systems security is still a current topic. [5] Nowadays, a large number of security solutions are implemented within power systems. These solutions, however, only cover a certain part of security of these systems. [Ponemon] With the increasing number of progressively more sophisticated cyberattacks, which are mostly carried out on the national level and focused on cybernetic espionage, an adequate response to these attacks also requires an increasing degree of sophistication [6]. Currently, the typical defence against cyberattacks targeting power systems is realized by protecting the communication infrastructure by means of

P. C. Vinh and A. Rakib (Eds.): ICCASA 2020/ICTCC 2020, LNICST 343, pp. 255–264, 2021.
https://doi.org/10.1007/978-3-030-67101-3_20

firewalls [7], proxy servers, etc., and critical components of control systems (SCADA server, communication servers, etc.) using anti-malware protection, for instance. [8] However, the use of such security mechanisms does not solve the main security problems of power systems: firstly, the integration of equipment to which standard security policies cannot be applied, and secondly, the existence of internal incidents related to security breaches of power systems [8, 9].

The solution is the implementation of a complex security solution which addresses both of the aforementioned security problems of power systems. The HIPS technology is one of such complex security solutions [10].

The HIPS is one of the intrusion prevention systems which monitors activity on a particular device. The HIPS has defined rules within which it restricts unsolicited access to specific data. The HIPS usually extensively logs data related to the detected situation.

The HIPS technology also monitors suspicious activity on a particular terminal. The monitoring is performed by analyzing network events on the device. The HIPS technology uses a database of monitored objects of the system, which is used to identify a potential intrusion into the computer network by analyzing system calls, application logs and modification of the file system. Simultaneously, a register of trustworthy programs is created [11]. If a program goes beyond its authorization, it is blocked by the HIPS for performing unauthorized actions. Via the HIPS, these mechanisms identify security breaches and violations of a security policy in work with power systems. With the ability to block suspicious activities related to security breaches, an organization can prevent internal incidents in power systems. [12]

The main aim of this paper is to conduct a performance comparative analysis of selected open-source HIPS solutions and their use for protection of power systems. Requirements for processes and operations performed within power systems place heavy demands on them being performed within limited time intervals. These are mainly requirements for data processing speed, data consistency and synchronization. To ensure that operations are performed in the shortest time possible, it is essential to implement a HIPS solution with minimal requirements for system resources. The implementation of a HIPS solution which would lead to consumption of a large amount of system resources would result in extension of time intervals needed for necessary operations within power systems.

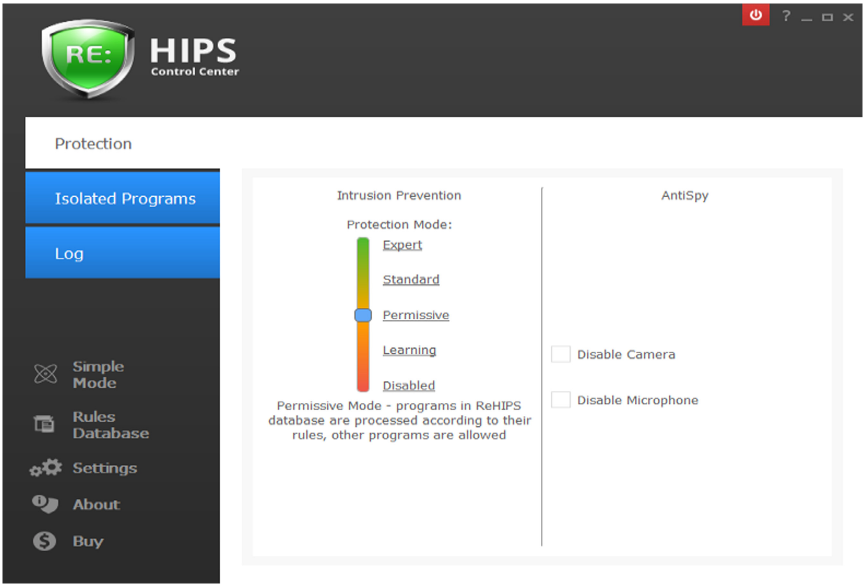
2 Methods of the HIPS Solution Analysis

As the methodology of the HIPS tools analysis, the analysis of third-party tools with an emphasis on system resource usage (CPU, RAM and SWAP partition of HDD) was chosen. These tools have the aforementioned HIPS functionalities. The comparative analysis of these tools is based on comparison of system resource usage, i.e. CPU, RAM, and SWAP partition, with the HIPS being deployed on the appropriate Windows testing station.

ReHIPS

The first solution which was part of the comparative analysis of selected HIPS solutions is the ReHIPS product by ReCryptCompany, version 2.4.0. This is an innovative solution. The HIPS agents do not need to be deployed in a special way since they will be registered automatically as soon as the product installation has been completed. The user interface is very simple and intuitive, which contributes to the increased convenience of administration of the solution as a whole.

Figure 1 shows the ReHIPS user interface, where a camera or a microphone can be disabled as a part of AntiSpy protection. The intrusion prevention contains 5 modes, which are the Expert mode, the Standard more, the Permissive mode, the Learning mode and the Disabled mode. It is possible to display a log list in the advanced settings.



Protection Mode: Permissive

Permissive Mode - programs in ReHIPS database are processed according to their rules, other programs are allowed

□ Disable Camera

□ Disable Microphone

Fig. 1. ReHIPS console. Source: authors

The Expert mode offers maximum protection. Trusted Vendor list is not taken into account in this mode. It displays a large number of notifications. The Standard mode is similar to the Expert mode. The main difference is in the smaller number of displayed notifications. The Permissive mode allows running programs registered in an internal database, based on a set of defined rules. The Learning mode adapts rules to programs registered in the internal database. Programs running within the operating system that are not registered in the internal database can be enabled or disabled in Learning mode. Appropriate actions can be added to the list of registered programs in the internal database. The Disabled mode stops the complex HIPS protection within the device.

Comodo Internet Security

The second tested product with the HIPS functionality is Comodo Internet Security by Comodo. It is a program designed to increase security of the computer network and it has the HIPS technology integrated as one of the offered functionalities.

Functions offered by this product are divided into general functions, firewall functions, containment functions, and advanced functions. General functions include basic functions, which are also displayed in the initial environment. These are the following: the function of launching a scan, searching for updates for the program, protection while shopping online, unblocking applications blocked by security actions, and special online support by Comodo experts.

Firewall functions include, for instance, a function which allows a specific application to connect to the network, or blocks its connection to the network. In firewall functions it is possible to completely block the network traffic. Furthermore, there are functions such as displaying the list of applications which are currently connected to the public network, a function for the network management where it is possible to allow or block connection to an available computer network.

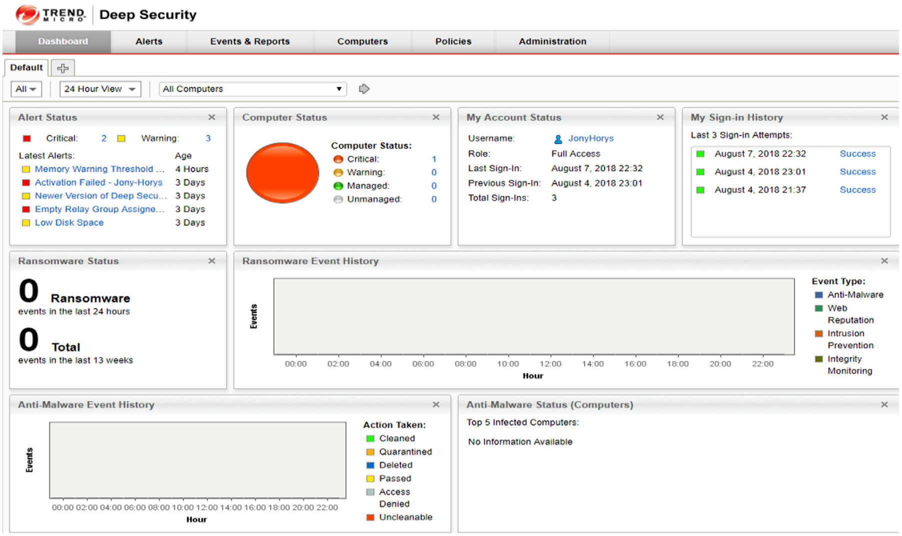
The next group consists of containment functions, where it is possible to launch a function for secured virtual desktop. It is also possible to display detailed information about active processes, launch functions for opening a shared space between classic and virtualized applications, and run applications by virtualization in sandbox.

The last group contains advanced functions which include creation of a rescue disc, displaying records, cleaning terminal points, quarantine, sending files, and task management for specific, currently running tasks.

DeepSecurity

The third solution tested in the comparative analysis is DeepSecurity 9.6. It is a multiplatform solution by Trend Micro. The key assets of DeepSecurity for the business world are security of virtual desktops, security of the cloud environment and, above all, security of physical, virtual and cloud servers. DeepSecurity is optimized for the VMware environment, Amazon Web Services and Microsoft Azure. DeepSecurity offers not only intrusion prevention, but also anti-malware, firewall, log scan and integrity monitoring functionalities.

The following figure depicts the dashboard of the DeepSecurity management server, which is accessible to the user via a web interface. The dashboard shows a status with critical messages and warnings about non-standard activities (Fig. 2).



Alert Status

🟥 Critical: 2 🟨 Warning: 3

Latest Alerts:	Age
🟨 Memory Warning Threshold ...	4 Hours
🟥 Activation Failed - Jony-Horys	3 Days
🟨 Newer Version of Deep Secu...	3 Days
🟥 Empty Relay Group Assigne...	3 Days
🟨 Low Disk Space	3 Days

Computer Status

Computer Status:

● Critical:	1
● Warning:	0
● Managed:	0
● Unmanaged:	0

My Account Status

Username:	JonyHorys
Role:	Full Access
Last Sign-In:	August 7, 2018 22:32
Previous Sign-In:	August 4, 2018 23:01
Total Sign-Ins:	3

My Sign-in History

Last 3 Sign-in Attempts:

🟩 August 7, 2018 22:32	Success
🟩 August 4, 2018 23:01	Success
🟩 August 4, 2018 21:37	Success

Ransomware Status

0 Ransomware
events in the last 24 hours

0 Total
events in the last 13 weeks

Ransomware Event History

Event Type:
- Anti-Malware
- Web Reputation
- Intrusion Prevention
- Integrity Monitoring

Anti-Malware Event History

Action Taken:
- Cleaned
- Quarantined
- Deleted
- Passed
- Access Denied
- Uncleanable

Anti-Malware Status (Computers)

Top 5 Infected Computers:

No Information Available

Fig. 2. DeepSecurity console. Source: authors

The dashboard shows the status of PC in which the solution is deployed. There is also history of specific events, e.g. anti-malware activity events as seen in the figure. It also shows activities of firewall, intrusion prevention system, web reputation, log scan and integrity monitoring.

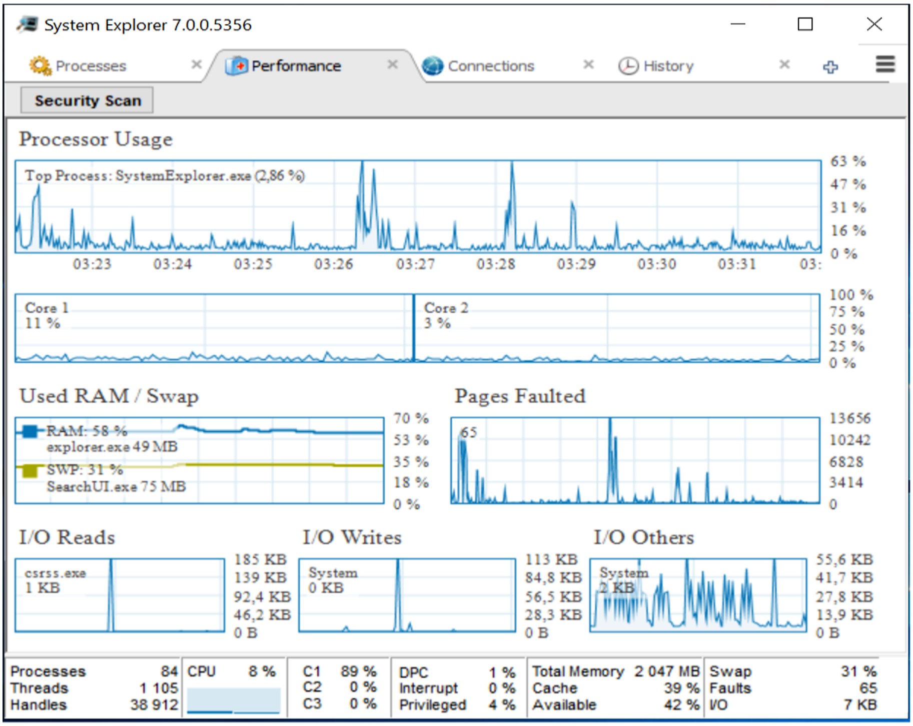
3 Comparative Analysis of Selected HIPS Solutions

For the purpose of conducting the comparative analysis, a personal computer was used as a single tool for analysing the use of system resources by the tested HIPS solutions. The hardware configuration of the personal computer is the following:

- OS: Windows 10 Pro 64 bit
- CPU: Intel Core 2 Duo E4600 2,4 GHz
- RAM: 2 GB
- GPU: NVIDIA GeForce GT 610 1GB DDR3 SDRAM
- HDD: 1 × HDD 500 GB
- Network adapter: Qualcomm/Atheros L1 Gigabit Ethernet Adapter

System Explorer was used for measuring the system resources. This surveillance tool enables recording information about usage of system resources, especially CPU, RAM, and SWAP partition of HDD. System Explorer includes display and management of tasks and processes along with evaluation of processes based on their security classification using an online database. In order to determine standard usage of system resources, performance of the device was first measured in the initial state without an activated HIPS solution. Subsequently, measurement of performance was conducted on the device with an activated HIPS solution. For this purpose, only the operating system and necessary services were launched: Antivirus program ESET Smart Security and System Explorer.

Figure 3 shows average usage of the device with the time period of 10 minutes in the initial state. Average processor (CPU) usage during the defined time period was 10%. Average usage of RAM during the defined time period was 58%. Average usage of SWAP partition (SWP) was 31%.

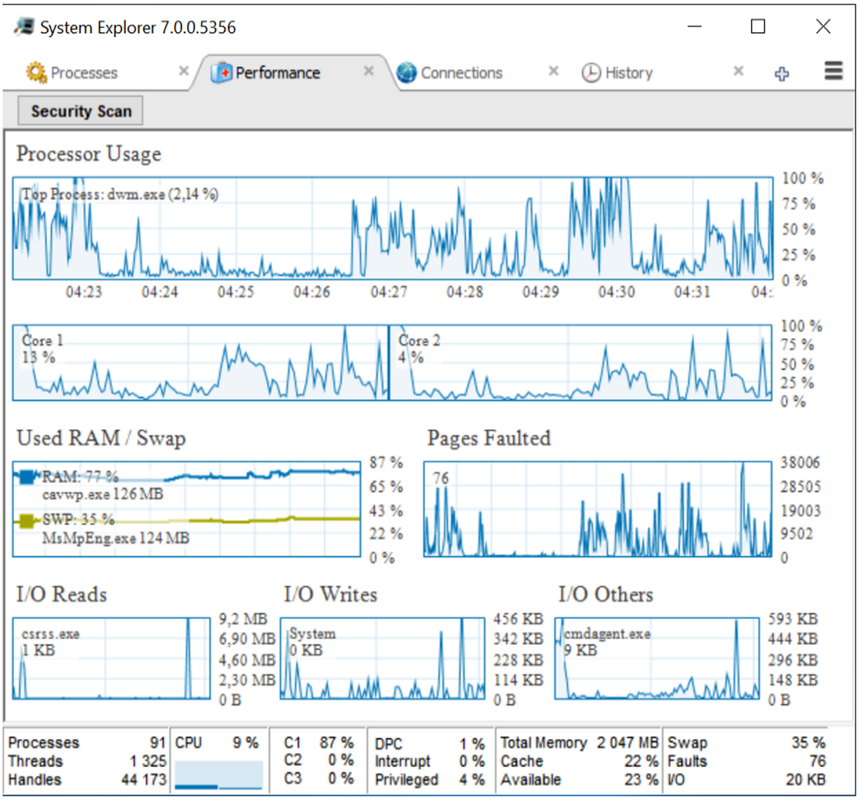


Processes	84	CPU	8 %	C1	89 %	DPC	1 %	Total Memory	2 047 MB	Swap	31 %
Threads	1 105			C2	0 %	Interrupt	0 %	Cache	39 %	Faults	65
Handles	38 912			C3	0 %	Privileged	4 %	Available	42 %	I/O	7 KB

Fig. 3. Standard usage of system resources. Source: authors

ReHIPS

Figure 4 shows average usage of the device during the defined time period of 10 minutes with ReHIPS solution being deployed. Average processor (CPU) usage during the defined time period was 60%. Average usage of RAM during the defined time period was 72%. Average usage of SWAP partition (SWP) was 35%.

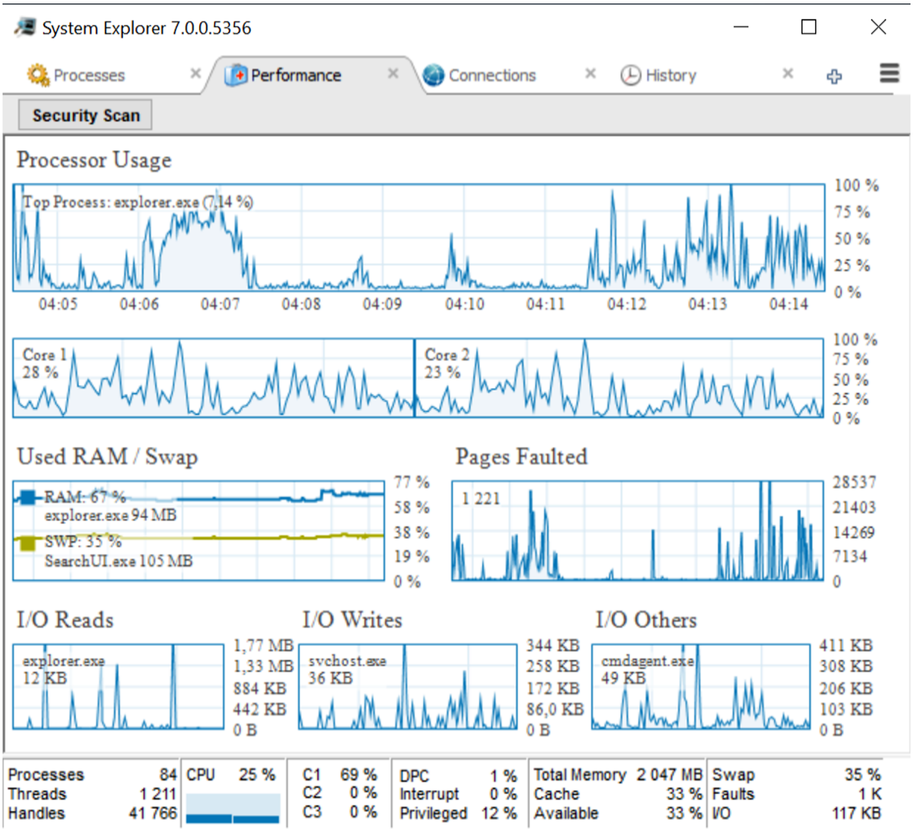


Processes	91	CPU	9 %	C1	87 %	DPC	1 %	Total Memory	2 047 MB	Swap	35 %
Threads	1 325			C2	0 %	Interrupt	0 %	Cache	22 %	Faults	76
Handles	44 173			C3	0 %	Privileged	4 %	Available	23 %	I/O	20 KB

Fig. 4. ReHIPS system resources. Source: authors

Comodo Internet Security

Figure 5 shows average usage of the device during the defined time period of 10 minutes with Comodo Internet Security Pro solution being deployed. Average processor (CPU) usage during the defined time period was 50%. The reason for such usage was fast launch of a device scan. Average usage of RAM during the defined time period was 77%. This means 19% increase of RAM usage in comparison with the initial state. Average usage of SWAP partition (SWP) was 35%.

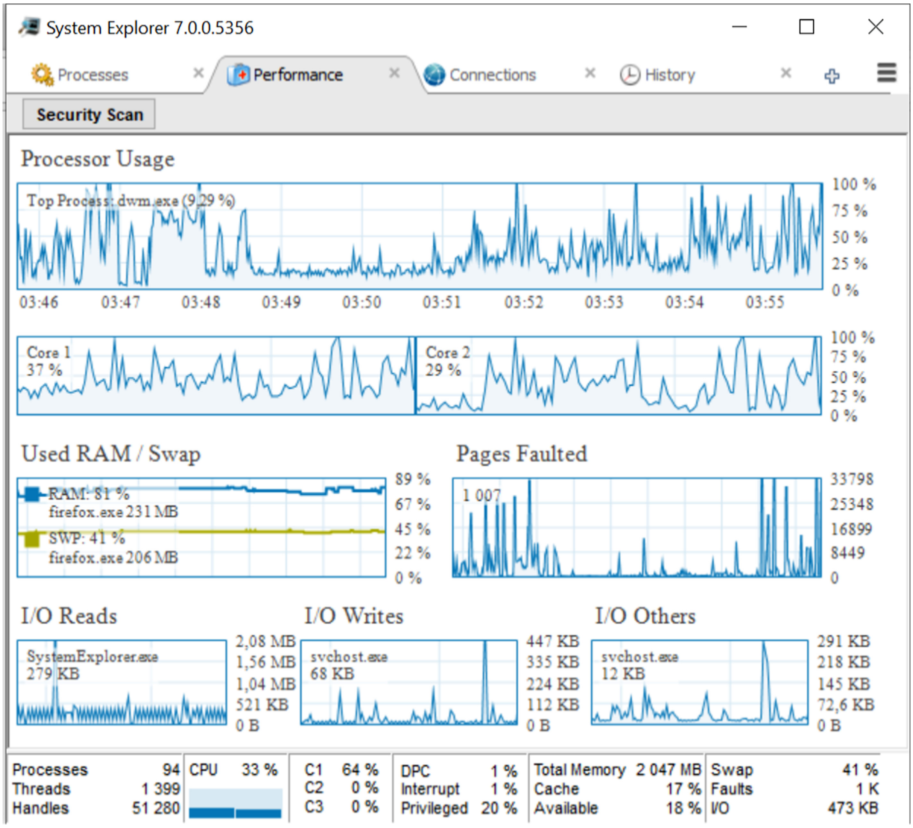


Processes 84
Threads 1 211
Handles 41 766
CPU 25 %
C1 69 %
C2 0 %
C3 0 %
DPC 1 %
Interrupt 0 %
Privileged 12 %
Total Memory 2 047 MB
Cache 33 %
Available 33 %
Swap 35 %
Faults 1 K
I/O 117 KB

Fig. 5. Comodo internet security pro system resources. Source: authors

DeepSecurity

Figure 6 shows average usage of the device during the defined time period of 10 minutes with DeepSecurity solution being deployed. Average processor (CPU) usage during the defined time period was 75%. This means 65% increase of CPU usage in comparison with the initial state. Average usage of RAM during the defined time period was 81%, which is a significant increase of usage in comparison with the initial state (58%), ReHIPS solution (72%) and Comodo Internet Security Pro solution (77%). Average usage of SWAP partition (SWP) was 44%.



Processes 94
Threads 1 399
Handles 51 280
CPU 33 %
C1 64 %
C2 0 %
C3 0 %
DPC 1 %
Interrupt 1 %
Privileged 20 %
Total Memory 2 047 MB
Cache 17 %
Available 18 %
Swap 41 %
Faults 1 K
I/O 473 KB

Fig. 6. DeepSecurity system resources. Source: authors

4 Conclusion

The aim of this paper was to conduct a comparative analysis of open-source HIPS solutions with an emphasis on their use within power systems and critical infrastructure protection. For the purpose of the analysis, three open-source HIPS products were selected. These were ReHIPS, Comodo Internet Security and DeepSecurity. The comparative analysis was based on system resources usage comparison, using System Explorer tool.

The results of the analysis clearly demonstrate that DeepSecurity is the most resource-demanding solution. This is partially due to the activated web interface of Deep security solution, which represented the user interface of the application. The fact that DeepSecurity offers a large number of functions and options of their management was identified as one of the main reasons for its high system resource requirements. According to the results of the comparative analysis, ReHIPS product achieved the best results in the testing, or more precisely, it caused the lowest usage of system resources. Other benefits of ReHIPS include automatic agent registration after the product has been installed. The interface used is simple and intuitive, which contributes to the increased convenience of administration of this solution as a whole. In further research, the comparative analysis can be extended to include commercial products and compare them with open-source solutions.

Acknowledgment. This work and the contribution were supported by a Specific Research Project, Faculty of Informatics and Management, University of Hradec Kralove, Czech Republic. We would like to thank Mrs. H. Svecova, a doctoral student, for the practical verification of the proposed solutions and close cooperation in the solution.

References

1. Baykara, M., Das, R.: A novel honeypot based security approach for real-time intrusion detection and prevention systems. J. Inf. Secur. Appl. (2018). https://doi.org/10.1016/j.jisa.2018.06.004.ISSN22142126
2. Vargas Martinez, C., Vogel-Heuser, B.: A host intrusion detection system architecture for embedded industrial devices. J. Franklin Inst. (2019). https://doi.org/10.1016/j.jfranklin.2019.03.037.ISSN00160032
3. Lee, R., Assante M. J., Conway, T.: Analysis of the cyber attack on the Ukrainian power Grid. NERC (2016). https://www.nerc.com/pa/ci/esisac/documents/e-isac_sans_ukraine_duc_18mar2016.pdf
4. Passeri, P.: 2016 Cyber Attacks Statistics. Hackmageddon (2017). https://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/
5. Ponemon institute: 2016 Cost of Cyber Crime Study & the Risk of Business Innovation. Ponemon Institute LLC (2016). https://go.cyphort.com/Ponemon-SIEM-Report-2017-Page.html
6. Birkinshaw, C, Rouka, E., Vassilakis, V.G.: Implementing an intrusion detection and prevention system using software-defined networking: defending against port-scanning and denial-of-service attacks (2019). https://doi.org/10.1016/j.jnca.2019.03.005, ISBN 1084-8045
7. Cook, A., Janicke, H., Smith, R., Maglaras, L.: The industrial control system cyber defence triage process. Comput. Secur. (2017). https://doi.org/10.1016/j.cose.2017.07.009, ISSN 01674048.
8. Radvanovsky, R., Brodsky, J.: Handbook of SCADA/Control Systems Security, 2nd ed. CRC Press, Taylor & Francis Group, Boca Raton (2016). ISBN 9781498717076.
9. Gregory-Brown, B.: Securing industrial control systems - 2017: A sans survey (2017). https://www.sans.org/reading-room/whitepapers/ICS/paper/3786.
10. Patel, A., Alhussian, H., Pedersen, J.M., Bounabat, B., Júnior J. C., Katsikas, S.: A nifty collaborative intrusion detection and prevention architecture for Smart Grid ecosystems (2017). https://doi.org/10.1016/j.cose.2016.07.002, ISSN 01674048.
11. Sawant, A.: A comparative study of different intrusion prevention systems. In: Fourth International Conference on Computing Communication Control and Automation (ICCUBEA) (2018). https://doi.org/10.1109/ICCUBEA.2018.8697500, ISBN 978-1-5386-5257-2, Dostupné z: https://ieeexplore.ieee.org/document/8697500/
12. Anilbhai, S. P., Parekh, C.: Intrusion detection and prevention system for IoT. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. **2**(6) (2017)