2023

Guide to Designing an Information Security Operations Center for a Big Data Environment

UNWE, SOFIA

INTRODUCTION

The growing digitization of processes, objects, and activities in our daily lives is a modern trend driven by technological advances over the last decades. One of the significant outcomes of this digital transformation is the exponential increase in the volume of data generated from various diverse sources. As digital transformation permeates nearly every sphere of human activity, data has become a primary asset for gaining a competitive edge in business. This phenomenon is universal, impacting all sectors, from healthcare, finance, logistics, transportation to ecology and sports.

The continuous accumulation of vast amounts of data and information is an integral part of these activities. Big data repositories provide valuable information that, when analyzed, can bring substantial benefits to businesses. The process of extracting knowledge from data collection and analysis has the capacity to optimize operations, leading to greater business efficiency or improvements in specific sectors. The knowledge derived from data empowers companies to identify what matters most to them, paving the way for additional or alternative actions that can help them achieve their ultimate goals and succeed. Information security emerges as a critical component in safeguarding data within organizations. This encompasses protecting data related to clients, financial records, intellectual property, and others that may be vulnerable to cybersecurity threats such as malicious software, phishing attacks, and social engineering techniques. Information security constitutes a multifaceted process aimed at preventing unauthorized access, mitigating various threats, ensuring confidentiality, and reducing the risk of data destruction or modification.

Effective information security management necessitates the identification, assessment, and management of risks associated with an organization's information assets. With the increasing volume of data, risks related to security breaches during data storage, processing, and analysis, unauthorized access, and data quality issues also rise. This requires a comprehensive and integrated approach to security, including the implementation of established policies, international standards, procedures, and technical controls to protect against potential threats. Therefore, the presence of an operational center for managing information security, capable of monitoring and responding to security threats, is of paramount importance in safeguarding digital information and ensuring an adequate level of security for businesses.

OPERATIONAL CENTER FOR INFORMATION SECURITY FOR BIG DATA SYSTEMS

An Information Security Operational Center (ISOC) is a centralized facility responsible for monitoring and managing an organization's security. It houses a team of security analysts and experts tasked with real-time detection, analysis, and response to security incidents. The ISOC facilitates data collection, storage, and normalization, providing a higher level of security focus on situational awareness and incident response.

The primary goal of an ISOC is to create a collaborative platform for scalable security analysis tools while offering additional capabilities for identifying security issues. Automation and analysis play a crucial role in OSC operations, enabling the detection and response to security threats through processes such as log analysis, incident sorting, and threat intelligence gathering.

DESIGNING AN ISOC

To design and build an ISOC, established principles and methods must be followed. Principles provide decision-making frameworks, while methods focus on specific techniques and processes aimed at achieving objectives. To create a functional ISOC project, it is crucial to understand all the requirements, risks, and goals of our organization. Therefore, the following principles and methods for designing an ISOC provide a framework for understanding an organization's requirements, risks, and goals.

- Principles of Designing and Building an ISOC

- Observation: Effective monitoring is of paramount importance for detecting and responding to security threats, including malicious attacks and activities from both internal and external entities.

- Real-time Analysis: Real-time data analysis is crucial for identifying and responding to security threats as they emerge.

- Incident Response: A well-defined incident response plan is exceptionally valuable for addressing security-related incidents, regardless of whether they originate from within or outside.

- Breach Detection and Response: Response plans are necessary to effectively manage security incidents, including steps for containment, investigation, and recovery.

- Audit of Log Files: Analyzing log files (logs) from various devices and correlating events is of vital importance for compliance tracking and documenting security incident responses.

- Regular Testing and Evaluation: Continuous testing and evaluation help identify vulnerabilities and ensure the effectiveness of security measures.

- Scalability: The ISOC must be designed to scale horizontally or vertically to accommodate the increasing size and speed of big data.

- Data Confidentiality: Implement encryption and access control methods to protect data from internal and external threats.

- Automation: Automation helps rapidly identify security-related events and provides timely responses, reducing the risk of errors caused by employees.

These principles provide a framework for designing a robust ISOC for large-scale environments with big data, such as Hadoop. To fully understand the steps involved in designing such a system, various methods that can be used need to be explored.

- Methods for Designing and Building an ISOC

- Risk Assessment: Conducting a comprehensive risk assessment is of paramount importance. This helps in identifying potential risks and vulnerabilities associated with the data, infrastructure, and applications that will be monitored by the ISOC.

- Security Information and Event Management (SIEM) Tools: Deploying SIEM tools is essential for collecting, analyzing, and summarizing real-time security event data.

- Access Control: Ensuring strict access control to limit individuals who have access to sensitive information, data, and systems.

- Encryption: Using mechanisms to encrypt data at rest and in transit to protect sensitive data from unauthorized access.

- Network Segmentation: Segmenting the network by creating separate zones for different types of data and user roles, helping to prevent unauthorized access and limit potential damage from security breaches.

- Compliance: The ISOC must comply with all applicable regulations and standards, such as GDPR and PCI DSS, to ensure the protection of big data.

- Training and Awareness: Implementing training programs and raising staff awareness about the importance of information security and how to identify and report potential threats.

- Continuous Improvement: Implementing a continuous improvement program for regular review and updating of the ISOC to ensure it remains effective and up to date.

Designing an ISOC for big data systems can be a complex and challenging process, but it is essential to ensure that sensitive data is protected, and security incidents are detected and responded to promptly.

For this reason, in the process of building an ISOC, some of the controls from the ISO 27001 standard related to big data security are incorporated.

- ISO 27001 Controls in the ISOC Design Process

Implementing ISO 27001 controls not only ensures the protection of sensitive information but also guarantees a rapid response to security incidents within the ISOC.

- Information Security Policies (A.5): Creating and maintaining information security management policies is vital. These policies guide ISOC teams in their responsibilities and incident response procedures.

- Physical Security (A.7): Implementing physical security measures protects information assets, processing facilities, and critical resources from threats such as theft or unauthorized access.

- Information Classification (A.8): Classifying information assets based on sensitivity levels allows for focused efforts on critical assets and ensures the application of appropriate security controls.

- Access Control (A.9): Restricting access to authorized users is essential. ISOC teams require access to sensitive data and systems, but it must be carefully controlled to prevent unauthorized access or data breaches.

- Incident Management (A.16): Establishing an incident management process for detecting, reporting, and responding to security incidents is crucial. ISOC teams are responsible for monitoring security events and incident response.

By integrating these ISO 27001 controls into the ISOC design framework, data confidentiality, integrity, and availability are improved. This approach not only protects the data processed and stored within the security center but also safeguards the entire ISOC infrastructure against potential security threats.

Levels of Management of the Operational Center for Information Security for Big Data Systems

The Information security operation center (ISOC) for big data has a primary goal of addressing the evolving security needs of businesses in the face of increasing cyber threats from various threat actors. This security center implements adaptive security measures and utilizes dynamic vulnerability corrections through AI-managed responses to security incidents, depending on assessments of the existing threat landscape. The architecture of ISOC (Figure below) aims to enhance protection against cyberattacks by using increased automation, primarily managed by artificial intelligence, to collect various types of data from heterogeneous sources.

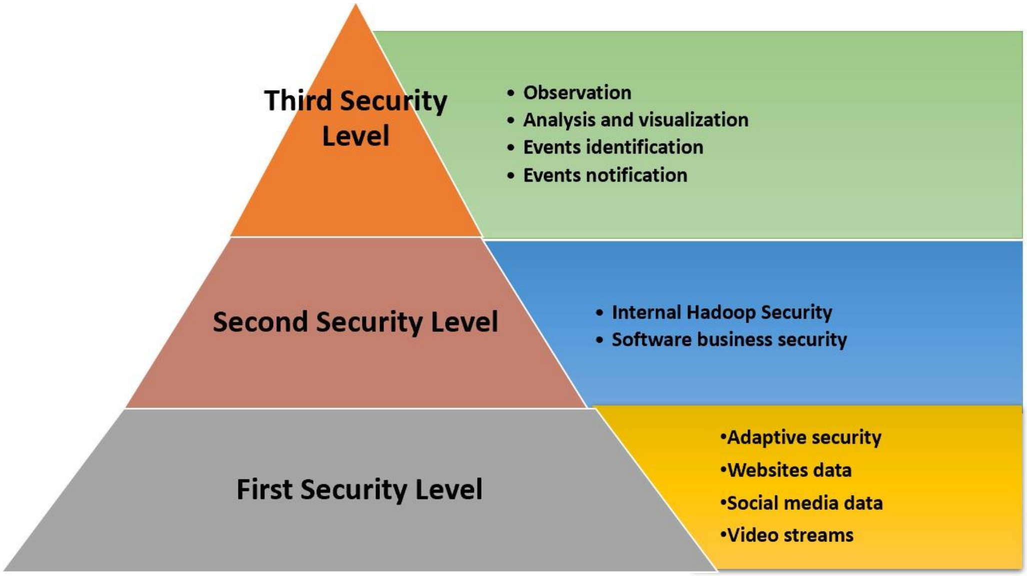


Figure 1. Security Operations Center Functional Architecture.

This architecture is structured into three distinct levels, with the first level referred to as "Intelligent Security Management." The primary goal of this level is real-time threat detection and response, using artificial intelligence and adaptive security mechanisms. The system collects data from various sources, including video streams, social media data, and other sources. Cognitive search, image recognition, knowledge discovery, and data analysis are facilitated through artificial intelligence, machine learning, and deep learning techniques. Data collected from social media and online platforms can be used to identify individuals or groups representing security threats, as well as to recognize stolen vehicles. Additionally, facial recognition technology aids in identifying individuals who may pose security risks. This security center incorporates adaptive security and offers dynamic vulnerability correction using AI when processing security incidents that impact the security level based on existing threats. Adaptive Security (AS) is a cybersecurity approach that continuously analyzes network behavior and events, ready to adapt to threats by investigating and analyzing them before they occur. An organization can continuously assess risk and ensure the appropriate implementation of protective mechanisms and approaches using adaptive security.

The second level of this architecture is based on Hadoop-based internal security and software business security. Its role is to protect the confidentiality, integrity, and availability of data. Approaches at this level include centralized user authentication, establishing user access rights to large system clusters for management, and segmenting big data.

The highest level, the third level, focuses on the analysis and visualization of the obtained results. Its goal is to provide suitable data visualizations collected from the previous levels, enabling real-time threat detection. This level monitors events occurring within the center, such as creating and analyzing log files, for proactive identification and detection of potential threats in real-time.

This architecture is adaptive and can be personalized to meet the specific requirements of organizations, regardless of their size or industry.

The proposed architecture offers a multi-layered approach to security management, providing comprehensive protection for big data systems as well as the data itself, integrating technologies to achieve the set goals. By implementing the proposed method for designing an ISOC with the presented solutions, organizations can enhance their information security. Different technologies offered by various companies can be used to implement each of the levels, but the main challenge lies in integrating them into a unified system and fostering collaboration among them. To address this, this guide outlines technologies that have been verified to work together and not impede the processes that an ISOC needs to perform. Some of the selected technological solutions are presented in more detail because they have specific implementation nuances, demonstrating that the same solutions can be applied to the proposed operational information security center.

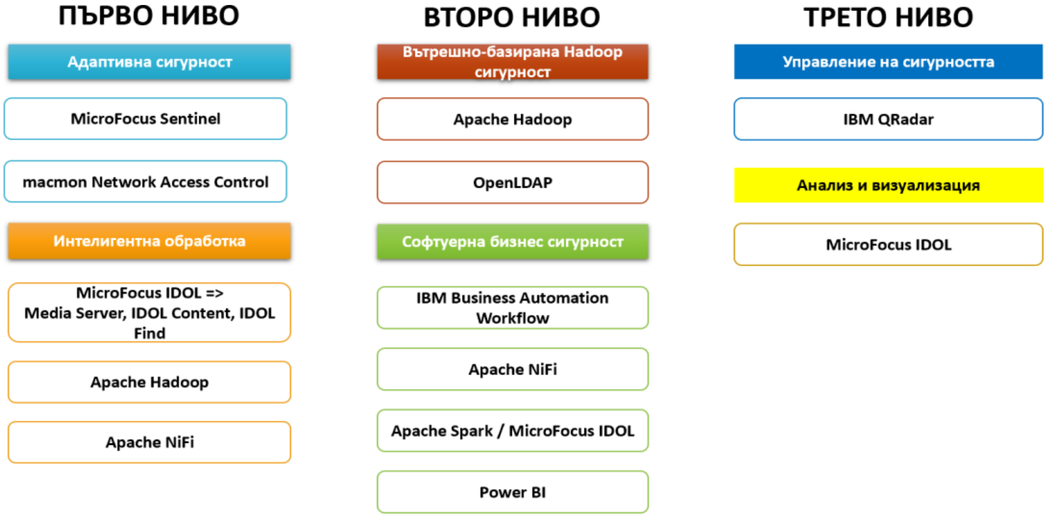

ПЪРВО НИВО
Адаптивна сигурност
MicroFocus Sentinel
macmon Network Access Control
Интелигентна обработка
MicroFocus IDOL => Media Server, IDOL Content, IDOL Find
Apache Hadoop
Apache NiFi
ВТОРО НИВО
Вътрешно-базирана Hadoop сигурност
Apache Hadoop
OpenLDAP
Софтуерна бизнес сигурност
IBM Business Automation Workflow
Apache NiFi
Apache Spark / MicroFocus IDOL
Power BI
ТРЕТО НИВО
Управление на сигурността
IBM QRadar
Анализ и визуализация
MicroFocus IDOL

Figure 2. Technologies used at the different levels of ISOC.

Figure 2 provides an overview of the capabilities of the technologies used at each of the levels, achieving the set goals at each of them.

Next is an introduction to the workflow of the levels and the technological solutions for each of them.

- First Level of ISOC - Adaptive Security

The proposed comprehensive approach to designing a system for information security operation center (ISOC) for big data, which focuses on ensuring data confidentiality, integrity, and availability. The architecture, illustrated in Figure 3, presents the components of adaptive security for big data systems, which is part of the first level of the ISOC architecture.

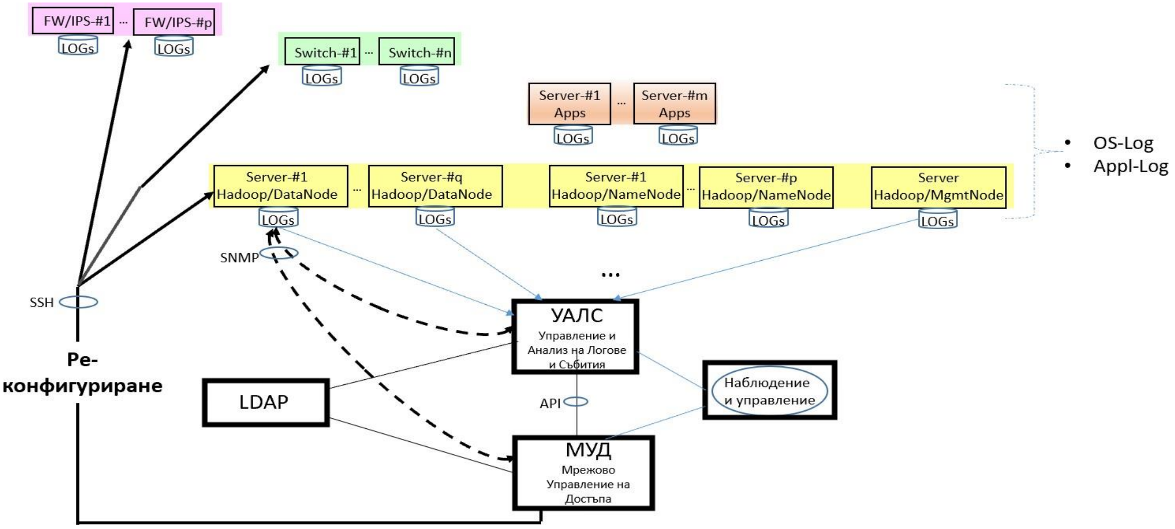


Figure 3. Adaptive Security Components for Big Data Systems.

- Firewalls and switches: These components are responsible for protecting big data and application servers. They play a key role in data security and isolating potential threats.

- Hadoop Distributed File System (HDFS) servers: This is where data blocks are stored and managed, ensuring data availability even in the event of node compromise. HDFS servers are responsible for storing and managing big data.

- Devices and connections: These components connect all elements of the system and facilitate communication between them. They also provide real-time network status, reducing potential security risks.

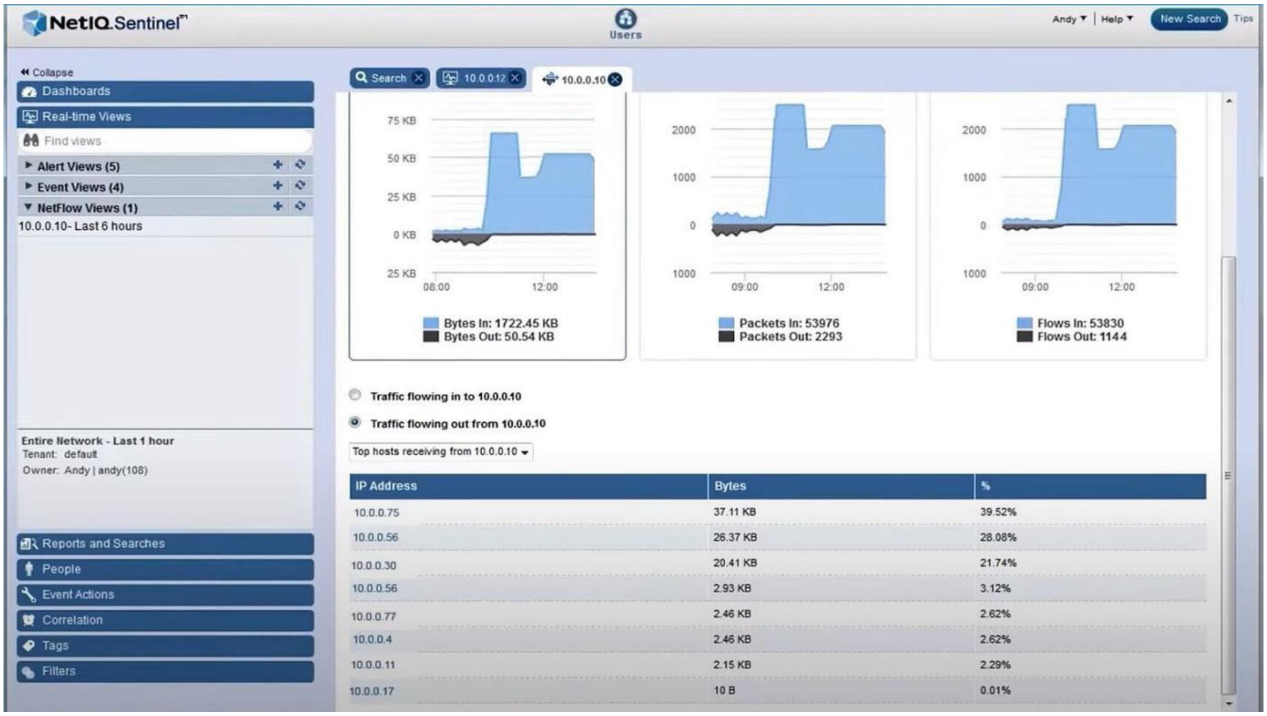
- NameNode, DataNode, and ManagementNode: This set of components forms the core of the Hadoop environment and handles file system name management, data storage, and management services. Their logging capabilities allow adaptive security systems to monitor network status in real-time.

- Data replication: To ensure data availability in case of incidents, the system uses data replication, which provides copies of data in different parts of the system.

- Log and Event Management System (LEMS): This component collects and analyzes security-related data from various sources. It plays a key role in event monitoring and immediate threat detection.

- Network Access Management System (NAMS): This component manages and analyzes log files and events, ensuring proper network access and analyzing security events.

The proposed adaptive security solution for the ISOC system includes the use of Micro Focus Sentinel for LEMS and macmon Network Access Control for NAMS. Sentinel collects and analyzes security-related data from various sources, while macmon provides network access and device/user control. Integrating these two systems allows for greater network visibility and rapid response to security incidents. Data sharing through APIs enables event correlation and security alerts, facilitating the identification of potential threats and immediate mitigation actions. This approach allows the ISOC team to stay informed about the current state of the system and take timely security measures.



10.0.0.10- Last 6 hours

Entire Network - Last 1 hour
Tenant: default
Owner: Andy | andy(108)

Bytes In: 1722.45 KB
Bytes Out: 50.54 KB

Packets In: 53976
Packets Out: 2293

Flows In: 53830
Flows Out: 1144

○ Traffic flowing in to 10.0.0.10

● Traffic flowing out from 10.0.0.10

Top hosts receiving from 10.0.0.10 ▾

IP Address	Bytes	%
10.0.0.75	37.11 KB	39.52%
10.0.0.56	26.37 KB	28.08%
10.0.0.30	20.41 KB	21.74%
10.0.0.56	2.93 KB	3.12%
10.0.0.77	2.46 KB	2.62%
10.0.0.4	2.46 KB	2.62%
10.0.0.11	2.15 KB	2.29%
10.0.0.17	10 B	0.01%

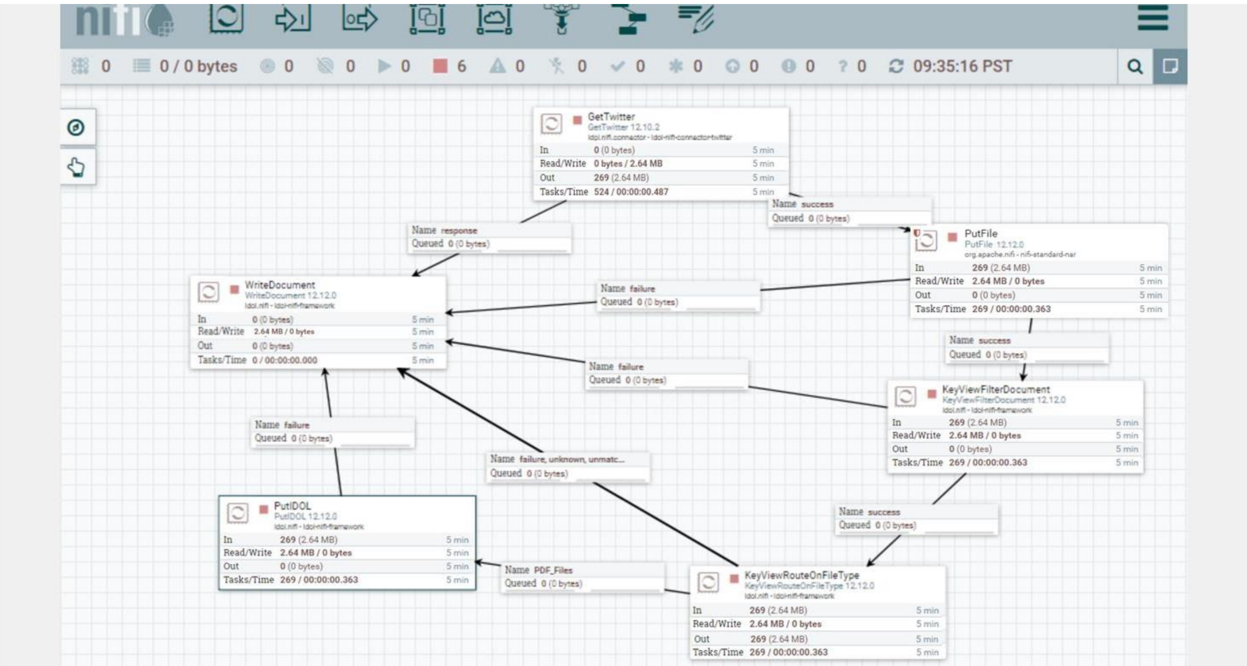
Figure 4. Sentinel dashboard.

Figure 4 shows the dashboard for continuous monitoring by Sentinel, displaying network load on the monitored devices in the proposed ISOC.

- First Level of ISOC - Intelligent Data Processing

Intelligent data processing refers to a security system or approach that utilizes intelligent or automated technologies, with artificial intelligence playing a key role. This level of security primarily focuses on collecting and analyzing data from various sources in a secure manner. Automation of data analysis through machine learning algorithms and other artificial intelligence techniques simplifies the detection and response to potential threats by identifying patterns in large datasets. Artificial intelligence is used to monitor social media and websites for suspicious activity and detect unusual behavior through cameras placed inside or outside facilities. This technology can identify potential threats such as the spread of false information, unauthorized access, or suspicious activity in restricted areas. At this level, we use the products Micro Focus IDOL, Apache Hadoop, and Apache NiFi, and the selected social media platforms are Facebook and Twitter.

The process of handling unstructured social data involves installing and configuring the IDOL server and its components, creating a database to store the extracted data, defining access roles, and utilizing built-in AI functionalities. Next, Apache NiFi is installed and configured for data extraction and storage. The subsequent installation is Hadoop, which is configured for data storage. Connectors are installed and configured to extract data from social media platforms such as Twitter and Facebook by creating applications in the developer environment and using client keys and tokens to connect to the API. Then, the NiFi system is used to define connectors for social media to extract desired content.



GetTwitter
GetTwitter 12.10.2
idol.nifi.connector - idol-nifi-connector-twitter

In	0 (0 bytes)	5 min
Read/Write	0 bytes / 2.64 MB	5 min
Out	269 (2.64 MB)	5 min
Tasks/Time	524 / 00:00:00.487	5 min

PutFile
PutFile 12.12.0
org.apache.nifi - nifi-standard-nar

In	269 (2.64 MB)	5 min
Read/Write	2.64 MB / 0 bytes	5 min
Out	0 (0 bytes)	5 min
Tasks/Time	269 / 00:00:00.363	5 min

WriteDocument
WriteDocument 12.12.0
idol.nifi - idol-nifi-framework

In	0 (0 bytes)	5 min
Read/Write	2.64 MB / 0 bytes	5 min
Out	0 (0 bytes)	5 min
Tasks/Time	0 / 00:00:00.000	5 min

KeyViewFilterDocument
KeyViewFilterDocument 12.12.0
idol.nifi - idol-nifi-framework

In	269 (2.64 MB)	5 min
Read/Write	2.64 MB / 0 bytes	5 min
Out	0 (0 bytes)	5 min
Tasks/Time	269 / 00:00:00.363	5 min

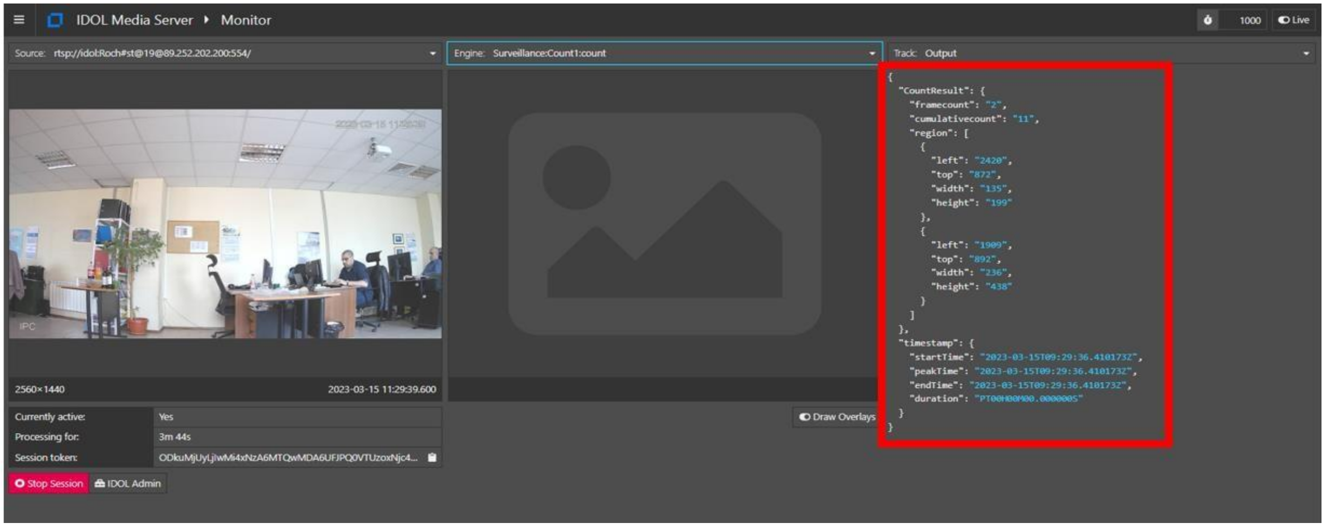
PutIDOL
PutIDOL 12.12.0
idol.nifi - idol-nifi-framework

In	269 (2.64 MB)	5 min
Read/Write	2.64 MB / 0 bytes	5 min
Out	0 (0 bytes)	5 min
Tasks/Time	269 / 00:00:00.363	5 min

KeyViewRouteOnFileType
KeyViewRouteOnFileType 12.12.0
idol.nifi - idol-nifi-framework

In	269 (2.64 MB)	5 min
Read/Write	2.64 MB / 0 bytes	5 min
Out	269 (2.64 MB)	5 min
Tasks/Time	269 / 00:00:00.363	5 min

Furthermore, the use of video streams can help detect unusual behavior such as unauthorized access or suspicious activity around restricted areas. By employing advanced machine learning techniques,



Source: rtsp://idol:Roch#st@19@89.252.202.200:554/

Engine: Surveillance:Count1:count

Track: Output

2560×1440 2023-03-15 11:29:39.600

Currently active:	Yes
Processing for:	3m 44s
Session token:	ODkuMjUyLjIwMi4xNzA6MTQwMDA6UFJPQ0VTUzoxNjc4...

```
{
  "CountResult": {
    "framecount": "2",
    "cumulativecount": "11",
    "region": [
      {
        "left": "2420",
        "top": "872",
        "width": "135",
        "height": "199"
      },
      {
        "left": "1909",
        "top": "892",
        "width": "236",
        "height": "438"
      }
    ]
  },
  "timestamp": {
    "startTime": "2023-03-15T09:29:36.410173Z",
    "peakTime": "2023-03-15T09:29:36.410173Z",
    "endTime": "2023-03-15T09:29:36.410173Z",
    "duration": "PT00H00M00.000000S"
  }
}
```

algorithms can be trained to count people entering and exiting a given location in real-time, providing security teams with valuable information about human traffic and occupancy levels. Object detection and tracking techniques, including deep neural networks, can be utilized to avoid double counting and artificially inflating the object count within the frame. AI can also be trained to recognize specific faces based on images of "flagged" individuals, enabling quick identification and response to potential threats. This technology can be particularly useful in high-security environments such as airports, train stations, and stadiums. Recognizing license plate numbers from images or video streams involves using algorithms that utilize Optical Character Recognition (OCR) to identify and read license plate numbers. OCR technology has various applications such as traffic control, parking management, and law enforcement. The proposed architecture for extracting data from video streams includes recording or capturing the video, followed by data processing using artificial intelligence embedded in the IDOL Media Server. The latter analyzes the video stream to detect faces and objects and has the capability to convert speech to text for monitoring audio emissions. The AI algorithms in the Media Server can also count people from the video stream, achieving one of the goals of the proposed architecture. The people count output includes data such as the number of people per frame, cumulative count, and also specifies the duration, start time, and end time of the video stream. The proposed architecture for extracting data from video streams includes recording or capturing the video, followed by data processing using AI algorithms within the IDOL Media Server. The latter analyzes the video stream to detect faces and objects and can convert speech to text for audio monitoring. The AI algorithms in the Media Server can also count people from the video stream, achieving one of the objectives of the proposed architecture. Figure 7 shows real-time visualization of the video stream and the output generated by the Media Server.

On the other hand, cognitive analysis can be used to analyze unstructured data such as text, images, and video clips from websites and blogs. This allows the system to understand the context of website content, detect negative sentiments or tones, and identify visual elements that contribute to the user experience. Web scraping or crawling tools like BeautifulSoup, Scrapy, and Selenium can be used to extract website content, which is then indexed in a big data system. Another approach for fetching web content is by using a Content Management System (CMS), which separates content creation and management from the presentation layer. A CMS may provide an API for Hadoop to access content stored in the CMS, or data can be transferred from the CMS to HDFS using a customized script or NiFi. Analyzing web data with artificial intelligence enables businesses to gain valuable insights into user behavior, market trends, and other key business metrics. AI-powered search engines can recognize and analyze a wide variety of data types, including structured, unstructured, and semi-structured data, providing a more comprehensive understanding of the data.

- The second level of the CISOC - Internal Hadoop Security

Internal security for big data systems is an approach that emphasizes the inclusion of security measures directly into the big data infrastructure. This approach aims to prevent malicious actors from gaining unauthorized access or compromising the system. Traditional data security relies on perimeter-based security measures such as firewalls and intrusion detection systems. Internal security, however, focuses on integrating security functions within the big data infrastructure.

The proposed method for internal security in big data systems utilizes the Hadoop data platform, which includes several built-in security features. These features are designed to address key areas of security, such as authentication and authorization, encryption, and auditing.

Centralized user authentication is a fundamental security approach for Hadoop clusters. This can be achieved through LDAP (Lightweight Directory Access Protocol) and/or Kerberos mechanisms to ensure proper authentication and permission control for multiple users who have access to the cluster. One-time passwords add an additional layer of security by requiring a unique password that can only be used once and is valid for a limited period.

The first step is to install and configure the OpenLDAP LDAP server. This involves creating an LDAP directory, defining users and groups, and configuring authentication and authorization rules. The OpenLDAP system uses an LDAP Data Interchange Format (LDIF) file, which is created using a text editor. Users and groups can be added to the OpenLDAP database using the ldapadd command.

Authentication and authorization policies can be configured using the OpenLDAP Access Control Language (ACL).

```
access to * by dn=“cn=admin,dc=example,dc=com“ write by * read
```

LDAP authentication for Hadoop can be enabled by editing the core-site.xml configuration file of Hadoop. Multi-factor authentication (MFA) can be applied with LDAP to require two or more authentication factors to verify the user's identity. To control access to DataNode servers based on user accounts and groups, you can implement the System Security Services Daemon (SSSD). SSSD serves as an identity and authentication provider that allows integration of various authentication mechanisms and maintains data segmentation for access control to DataNode servers.

Access control to HDFS directories and files can be managed by assigning permissions to users and groups through the Unix-style permission model and the "setfacl" command from the Hadoop CLI.

```
Dn:

cn=ivelkova,ou=users,dc=e

xample,dc=com

objectClass: top

objectClass: person

objectClass:

organizationa

lPerson
```

Another security approach involves creating a centralized Hadoop Access Control List (ACL) managed through the HDFS command-line interface (CLI) or the graphical user interface (GUI) tool. This mechanism enables administrators to add or remove users or groups from the ACL and modify access rules for specific files or directories.

Additionally, establishing a comprehensive audit mechanism is crucial to ensure data access traceability and user activity tracking, helping prevent data loss and maintaining compliance. Data lineage tracking involves recording metadata about the origin of data, its history, and transformations within the infrastructure. User activity tracking includes logging metadata about actions taken by users within the infrastructure.

- Second level of security - Software Business Security

Software Business Security (SBS) is a vital aspect of protecting sensitive data collected by business organizations from various cyber threats, including malicious software, hacker attacks, and phishing. This level includes various security measures such as access control, data encryption, secure software practices, vulnerability assessments, penetration testing, security monitoring, and incident response. To achieve a higher level of security, statistical methods can be combined with other security measures to analyze data and detect anomalies, trends, and patterns that may indicate security threats. For example, correlation analysis can be used to identify potential threats and take appropriate measures to address them. Business Process Management (BPM) can also be integrated into security efforts by identifying potential risks and vulnerabilities in business processes and taking appropriate security measures to mitigate these risks.

Integrating business software security into the Lambda architecture used for big data processing ensures the protection of the data being worked with. The extended Lambda architecture introduces additional layers, such as a data collection layer, a data storage layer, and a data processing layer, which enhances system performance, scalability, and robustness. This integration allows data to be securely collected, stored, and processed in accordance with security requirements.

The extended Lambda architecture intelligently combines data management with big data processing and visualization tools, enabling business organizations to analyze and visualize data, understand trends, and detect anomalies. This approach also includes the use of statistical methods and artificial intelligence to enhance data analysis capabilities while ensuring data security.

Such an approach represents a comprehensive security strategy that includes real-time monitoring, threat detection and mitigation, and ensures data consistency and accuracy throughout the processing and analysis process.

- Third level of security

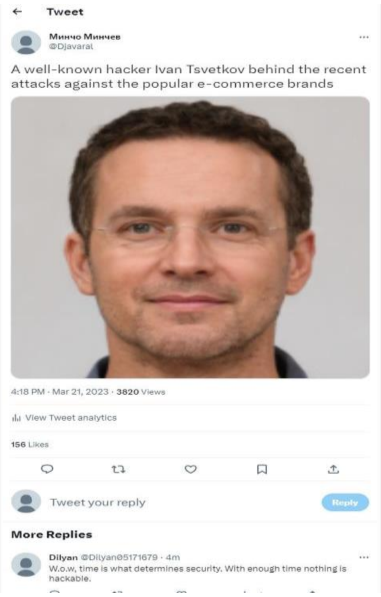
The third level of Information Security Assessment and Management (ISAM) focuses on security management and data analysis from various sources, including log files, video streams, and social media. Effective analysis and visualization of these data play a crucial role in implementing comprehensive security measures and vulnerability prevention strategies.

For this purpose, Security Information and Event Management (SIEM) systems like QRadar and MicroFocus IDOL are integrated into ISAM. These systems provide real-time monitoring, analysis, and incident response capabilities. QRadar uses correlation mechanisms to detect patterns and anomalies in security data, while IDOL specializes in analyzing and visualizing unstructured data from various sources. The integration of QRadar with IDOL offers significant advantages, such as a better understanding of security status, identification of potential threats and vulnerabilities that other security tools may miss. This integration provides enhanced visualization capabilities and allows businesses to explore their security data in new and more effective ways.

VERIFICATION OF THE PROPOSED APPROACH FOR DESIGNING AND BUILDING ISAM USING ARCHITECTURAL SOLUTIONS FOR POTENTIAL THREAT NOTIFICATION

The proposed Information Security Operations Center (ISOC) utilizes various software tools for monitoring and safeguarding networks and data. An illustrative scenario showcasing the system's effectiveness is presented.

The first process involves extracting a publication from a social media platform, analyzing the data, and storing the results in the Hadoop repository.



Минчо Минчев
@Djavaral

A well-known hacker Ivan Tsvetkov behind the recent attacks against the popular e-commerce brands

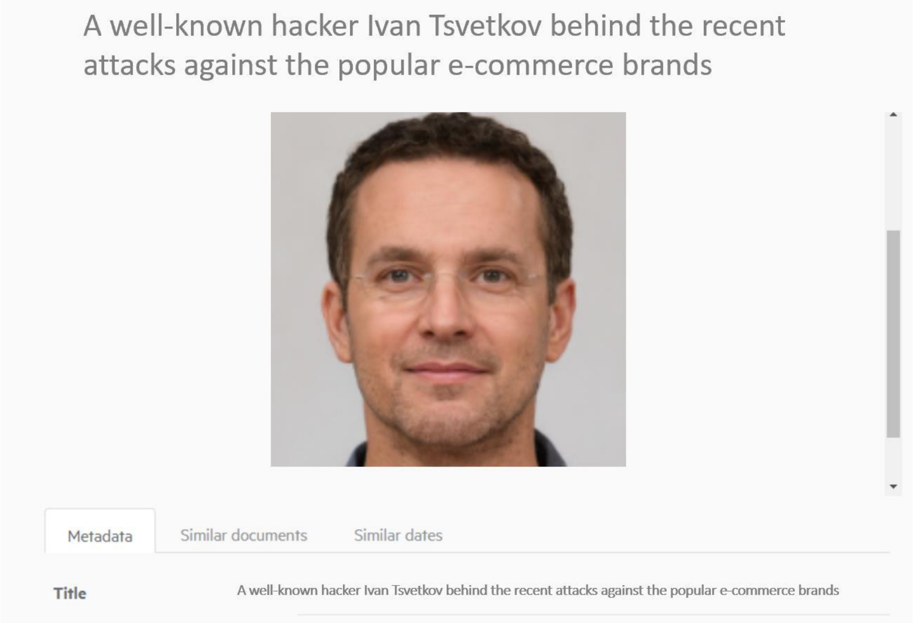
4:18 PM · Mar 21, 2023 · 3820 Views

156 Likes

More Replies

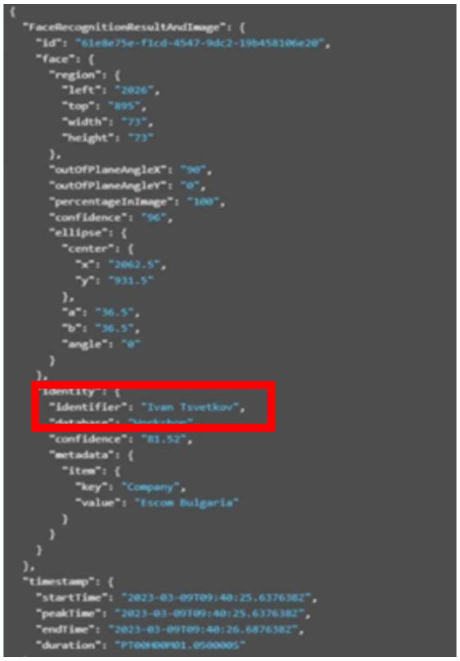
Dilyan @Dilyan05171679 · 4m
W.o.w, time is what determines security. With enough time nothing is hackable.

The second process involves extracting data from a video stream from a camera, performing analysis by the Media Server, and face recognition.



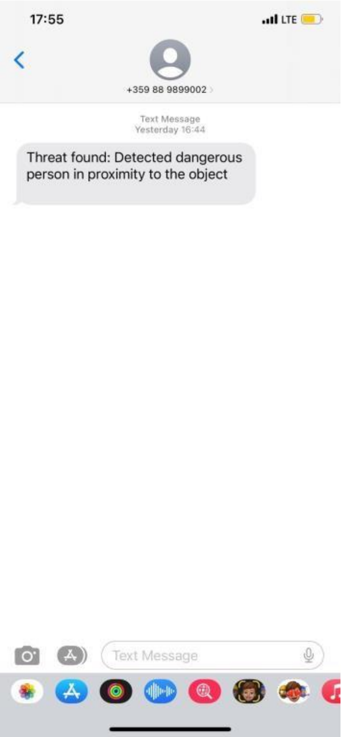
A well-known hacker Ivan Tsvetkov behind the recent attacks against the popular e-commerce brands

Title A well-known hacker Ivan Tsvetkov behind the recent attacks against the popular e-commerce brands



```
{
  "FaceRecognitionResultAndImage": {
    "id": "61e8e75e-f1cd-4547-9dc2-19b458106e20",
    "face": {
      "region": {
        "left": "2026",
        "top": "895",
        "width": "73",
        "height": "73"
      },
      "outOfPlaneAngleX": "90",
      "outOfPlaneAngleY": "0",
      "percentageInImage": "100",
      "confidence": "96",
      "ellipse": {
        "center": {
          "x": "2062.5",
          "y": "931.5"
        },
        "a": "36.5",
        "b": "36.5",
        "angle": "0"
      }
    },
    "identity": {
      "identifier": "Ivan Tsvetkov",
      "database": "Workshop",
      "confidence": "81.52",
      "metadata": {
        "item": {
          "key": "Company",
          "value": "Escom Bulgaria"
        }
      }
    }
  },
  "timestamp": {
    "startTime": "2023-03-09T09:40:25.6376382",
    "peakTime": "2023-03-09T09:40:25.6376382",
    "endTime": "2023-03-09T09:40:26.6876382",
    "duration": "PT00H00M01.0500005"
```

Then the multimedia server matches the identified face with the data stored in Hadoop, and if there is a match, QRadar generates an SMS alert to the SOC team. Working together, these software tools provide organizations with a more efficient and effective way to monitor and protect their networks and data.



17:55

+359 88 9899002

Text Message
Yesterday 16:44

Threat found: Detected dangerous person in proximity to the object

The collaboration of these software tools can lead to a greater scope and effective resolution of IT and cybersecurity-related issues, enabling organizations to better monitor, analyze, and protect their networks and data.

A validation of the proposed architecture for ISCM in a big data system has been performed, demonstrating the benefits of the synergy between software solutions. Micro Focus Sentinel and macmon Network Access Control are used for first-level management, collecting secure data from devices and systems and monitoring security threats. Micro Focus IDOL and NiFi are employed for secure data extraction and storage in a big data environment, while LDAP and multi-factor authentication with OpenLDAP secure system access. BPM and the extended Lambda architecture are used as a single process with NiFi, IDOL, and PowerBI for generating graphs and diagrams for business insights. IDOL is used for visualizing log file analysis, and QRadar is utilized for real-time notifications and log file analysis.

References

“How to Build a Security Operations Center (SOC): Peoples, Processes, and Technologies,” Digital Guardian. https://www.digitalguardian.com/blog/how-build-security-operations- center-soc-peoples-processes-and-technologies (accessed Mar. 29, 2023).

“The Evolution of Security Operations and Strategies for Building an Effective SOC,” ISACA. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution- of-security-operations-and-strategies-for-building-an-effective-soc (accessed Mar. 29, 2023).

A. T. A. J. Kienzle, “What Is a SOC? Top Security Operations Center Challenges,” IIoT World, Jan. 28, 2022. https://www.iiot-world.com/ics-security/cybersecurity/top-challenges- soc-are-facing/ (accessed Mar. 29, 2023).

“5G/SOC: SOC Generations -HP ESP Security Intelligence and Operations Consulting Services - Business white paper”.

E. R. https://www.emergenresearch.com, “SOC as a Service Market Size, Share | Industry Forecast by 2030.” https://www.emergenresearch.com/industry-report/security-operations- center-as-a-service-market (accessed Apr. 17, 2023).

“Atos opens new global next-gen Security Operations Center in Bulgaria and strengthens its sovereign security offering in Europe,” Atos, Mar. 22, 2022. https://atos.net/en/2022/press-release_2022_03_22/new-global-security-operations-center-in-bulgaria (accessed Apr. 17, 2022).

“Next Gen CR - PROCYB srl,” Oct. 06, 2021. https://procyb.io/en/next-generation-soc-en/ (accessed Apr. 17, 2023).

“ISO 27001 Annex A.5 - Information Security Policies,” https://www.isms.online/. https://www.isms.online/iso-27001/annex-a-5-information-security-policies/ (accessed Apr. 23, 2023

D. Kosutic,“What are the 11 new securitycontrols in ISO 27001:2022?” https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/ (accessed Apr. 23, 2023).

“ISO 27001 Annex A.9 Access Control - Your Step-by-Step Guide,” https://www.isms.online/. https://www.isms.online/iso-27001/annex-a-9-access-control/ (accessed Apr. 24, 2023).

“ISO 27001 Annex A.16 - Information Security Incident Management,” https://www.isms.online/. https://www.isms.online/iso-27001/annex-a-16-information- security-incident-management/ (accessed Apr. 24, 2023).

“Adaptive architecture: Key to True Cybersecurity | Kaspersky official blog.” https://www.kaspersky.com/blog/asa-key-to-true-cybersecurity/6678/ (accessed Dec. 10, 2022).

“Designing an Adaptive Security Architecture for Protection From Advanced Attacks,”

Gartner. https://www.gartner.com/en/documents/2665515 (accessed Mar. 28, 2023).

“Set Up Containerize and Test a Single Hadoop Cluster using Docker and Docker compose,” Engineering Education (EngEd) Program | Section. https://www.section.io/engineering- education/set-up-containerize-and-test-a-single-hadoop-cluster-using-docker-and-docker- compose/ (accessed Mar. 29, 2023).

K. Miao, J. Li, W. Hong, and M. Chen, “A Microservice-Based Big Data Analysis Platform for Online Educational Applications,” Scientific Programming, vol. 2020, p. e6929750, Jun. 2020, doi: 10.1155/2020/6929750.

“Enterprise Business Intelligence | Sentinel.” https://www.microfocus.com/en-us/cyberres/secops/sentinel (accessed Mar. 29, 2023).

“Zero Trust Network Access.” https://www.macmon.eu/en/ (accessed Mar. 29, 2022).

Y. Duan, J. S. Edwards, and Y. K. Dwivedi, “Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda,” International Journal of Information Management, vol. 48, pp. 63–71, Oct. 2019, doi: 10.1016/j.ijinfomgt.2019.01.021.

[1] “Big data Hadoop and MapReduce solutions for CMS content management problems,” TheServerSide.com. https://www.theserverside.com/tutorial/How-big-data-solved-the- content-management-CMS-problem (accessed Mar. 02, 2023).

KARDEN, “Authentication in Hadoop cluster: MIT Kerberos and Active Directory – DekarLab,” May 23, 2020. https://dekarlab.de/wp/?p=883 (accessed Mar. 29, 2022).

“Set up Okta Verify (MFA) | eSolutions.” https://www.monash.edu/esolutions/phones/change-device-multi-factor-authentication (accessed Mar. 29, 2023).

“Best Practices Guide for Systems Security Services Daemon Configuration and Installation

- Part 1 - Cloudera Blog.” https://blog.cloudera.com/best-practices-guide-for-systems- security-services-daemon-configuration-and-installation-part-1/ (accessed Mar. 29, 2022).

A. Luntovskyy and D. Gütter, “From Big Data to Smart Data: Best Practices for Data Analytics,” in Highly-Distributed Systems: IoT, Robotics, Mobile Apps, Energy Efficiency , Security, A. Luntovskyy and D. Gütter, Eds., Cham: Springer International Publishing, 2022, pp. 79–96. doi: 10.1007/978-3-030-92829-2_4.

P. P. Sharma, “Securing Big Data Hadoop : A Review of Security Issues , Threats and Solution,” 2014. https://www.semanticscholar.org/paper/Securing-Big-Data-Hadoop-%3A-