International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I10P104

Volume 72 Issue 10, 15-21, October 2024

Original Article

Empowering Intelligent Enterprises: Leveraging SAP's SIEM Intelligence for Proactive Cybersecurity

Puneet Aggarwal[1], Amit Aggarwal[2]

[1]*Department of Information & Technology, Deloitte LLP, Texas, United States of America.*
[2] *Department of Information & Technology, TCS, Michigan, United States of America*

[1]*Corresponding Author : erpuneetaggarwal@gmail.com*

Received: 19 August 2024 Revised: 23 September 2024 Accepted: 08 October 2024 Published: 22 October 2024

Abstract *- This article highlights the critical importance of cybersecurity in SAP environments. It demonstrates how SAP Enterprise Threat Detection (SAP ETD) acts as a crucial tool for safeguarding sensitive data and maintaining the operational integrity of intelligent enterprises. By utilizing SAP ETD, organizations can proactively detect and respond to digital threats, thereby enhancing their cybersecurity resilience. The study explores SAP ETD's ability to provide real-time threat detection, aiding businesses in mitigating risks associated with evolving cyber threats. The findings suggest that the effective implementation of SAP ETD significantly strengthens an organization's cybersecurity framework, ensuring continuous protection in dynamic digital landscapes.*

Keywords *- ERP compliance, SAP cybersecurity, SAP enterprise threat detection, SAP ETD, Threat detection.*

1. Introduction

We will explore the role of SAP Enterprise Threat Detection (SAP ETD) in safeguarding intelligent ERP enterprises from cyber threats. This analysis will cover the importance of cybersecurity, relevant statistics, common SAP vulnerabilities, SAP ETD's role in mitigating these threats, its architecture and components, integration capabilities, effectiveness in addressing critical CVEs, and its contribution to resilience and intelligence within intelligent ERP enterprises. In today's interconnected digital landscape, cybersecurity is paramount for protecting networks, devices, applications, systems, and data from cyber threats. The goal is to fend off attacks aimed at accessing, destroying, extorting, or disrupting data and business operations, whether these attacks originate from within or outside the organization.

1.1. Importance of Cybersecurity

The past year has seen a dramatic increase in the volume and complexity of cyberattacks. Cybercriminals are continuously evolving their tactics, often exploiting new opportunities. According to the FBI, cybercrime incidents surged by as much as 300% early in the pandemic in 2020, driven by hackers targeting remote workforces and pandemic-related vulnerabilities. This is reflected in the 358% increase in malware attacks in 2020 and the $3.92 million average cost of a data breach to an enterprise, data from CSO [5]. The Unit 42 Cloud Threat Report highlighted that as remote work grew from 20% to 71% early in the pandemic, cloud migration accelerated, and there was a notable increase in cloud security incidents. In the second quarter of 2020 alone, cloud security incidents surged, with DDoS attacks seeing a 15% increase and nearly 4.83 million attacks recorded. Cyberattacks often target data stored in the cloud, on personal devices, IoT devices, and private networks. With data growth accelerating and predicted to reach 200 zettabytes by 2025, the importance of cybersecurity cannot be overstated. Safeguarding data is a top priority for businesses and governments worldwide. Different types of cyberattacks like Social Engineering Attacks, Malware Attacks, IoT Attacks, Advanced Persistent Threats, Denial-of-Service (DoS) Attacks, etc.

1.2. Why We Need Threat Detection Tools

Cybersecurity in SAP environments requires constant vigilance due to the critical nature of the data and processes involved. In 2024, several high-profile vulnerabilities have been identified, emphasizing the importance of proactive threat detection:

- CVE-2024-41730: Missing Authentication Check in SAP BusinessObjects BI Platform.
- CVE-2024-29415: Server-Side Request Forgery in SAP Build Apps.
- CVE-2024-33006: File Upload Vulnerability in SAP NetWeaver AS ABAP.
- [Multiple CVEs]: Escalation of Privileges in SAP Edge Integration Cell.

Check here for more vulnerabilities.

In today's interconnected digital landscape, cybersecurity is paramount for protecting sensitive data and ensuring the operational integrity of organizations worldwide. This is especially critical for enterprise systems like SAP, which manage vast amounts of sensitive information across various industries. As cyber threats become more sophisticated, the need for robust security measures has never been greater. A key component of maintaining SAP security is the regular update of software patches and corrections. SAP conducts a Security Patch Day on the second Tuesday of every month, aligning with the Security Patch Day schedules of other major software vendors.

These days, SAP releases software corrections in the form of SAP Security Notes, which are specifically focused on addressing security vulnerabilities to protect against potential weaknesses or attacks. Organizations can access SAP Security Notes via SAP for Me by selecting "All Security Notes" to view the complete list. SAP recommends prioritizing the implementation of these corrections to maintain optimal security. To facilitate this process, several tools are available to help identify, select, and implement the necessary security corrections effectively. The United States' regulatory environment, including acts like Sarbanes-Oxley (SOX), HIPAA, and the California Consumer Privacy Act (CCPA), mandates stringent controls over data and systems, making cybersecurity an indispensable aspect of compliance. Globally, organizations such as the United Nations and major corporations like Apple, Google, and Shell rely on SAP systems to manage critical business processes, underscoring the need for advanced cybersecurity measures.

1.3. What Is SAP Enterprise Threat Detection Tool?

SAP Enterprise Threat Detection (SAP ETD) is a security monitoring and forensic tool powered by SAP HANA, designed to detect and analyze cyber threats in real time. It enables organizations to monitor their SAP landscapes continuously, identify suspicious activities, and respond to potential threats before they cause significant damage. For the latest version and compatibility matrix.

1.3.1. Key Highlights

Powered by HANA

SAP ETD leverages the high-performance in-memory computing capabilities of SAP HANA to process and analyze large volumes of security data in real time.

Comply with Data Protection and Audit Regulations

SAP Enterprise Threat Detection provides critical Security Information and Event Management (SIEM) capabilities that utilize real-time intelligence to enforce data governance.

This helps organizations comply with data protection regulations and effectively detect both external and internal cybersecurity threats.

Deployment Flexibility

SAP ETD can be deployed on-premise or in the cloud, offering flexibility to meet the specific needs of your organization. It is also available as a managed service, providing 24x7 monitoring and support.

Preconfigured and Customizable Functionality

The solution comes with preconfigured functionality that allows for rapid deployment and immediate use. It also offers customizable features, enabling organizations to tailor the system according to their unique security requirements.

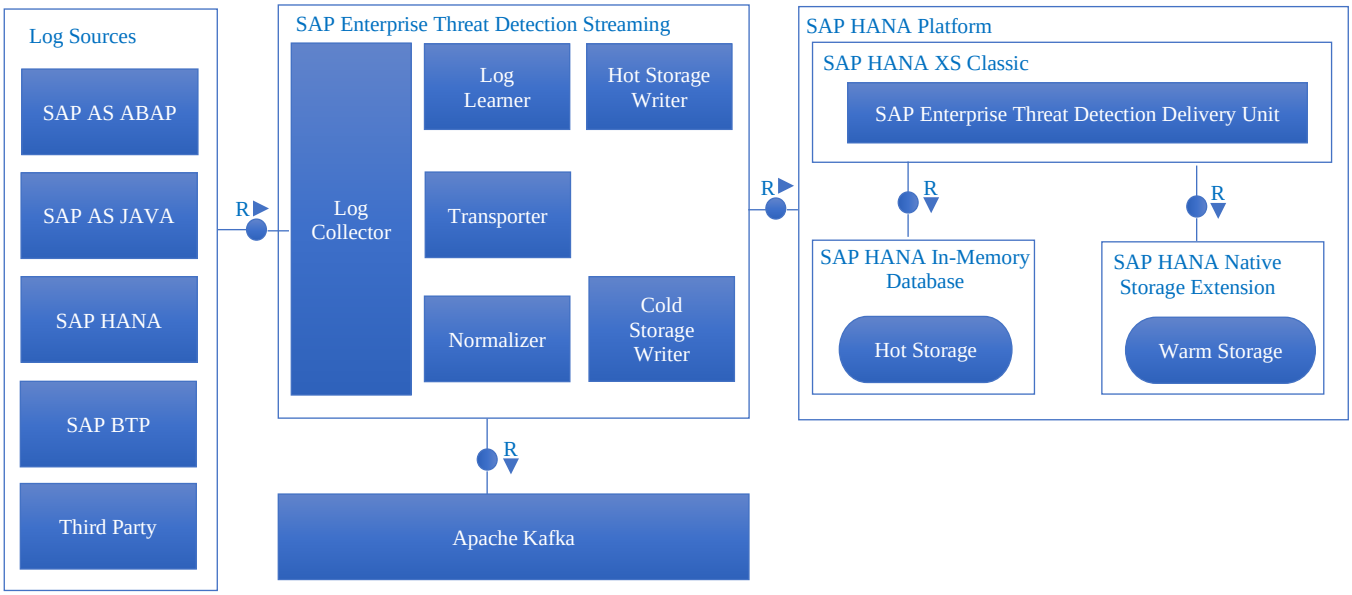

Fig. 1 SAP threat detection tool

Risk-Based and Prioritized Alerting

SAP ETD prioritizes alerts based on the risk they pose, ensuring that security teams focus on the most critical threats first. This risk-based approach helps to efficiently allocate resources and respond to incidents promptly.

Forensic Investigations, Threat Hunting, and Anomaly Detection

SAP ETD provides tools for conducting detailed forensic investigations, enabling organizations to dig deep into security incidents. It also supports proactive threat hunting and anomaly detection, allowing for the identification of potential threats before they can escalate.

Components

- *Event Stream Processor*: Analyzes real-time log data.
- *Alerting Framework*: Generates alerts for suspicious activities.
- *Forensic Lab*: Provides tools for in-depth investigation of security incidents.
- *Dashboard*: Offers a consolidated view of security status and alerts.

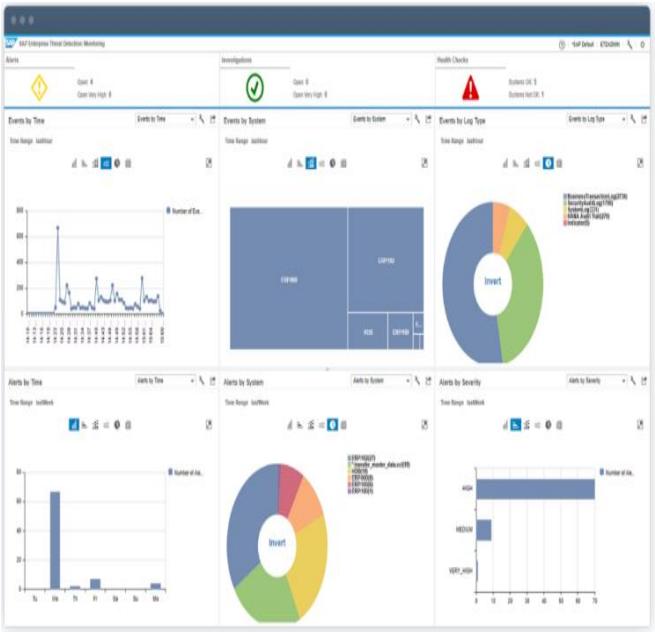

Fig. 2 SAP Enterprise Threat Detection Streaming view[4]

1.4. Licensing

While SAP Enterprise Threat Detection itself does not require a separate license, it runs on SAP HANA, which does require a license. Licensing is based on the number of monitored users identified within logs, measured over a 90-day period.

1.5. Integration with Third-Party SIEM Solutions

SAP Enterprise Threat Detection can be integrated with several third-party Security Information and Event Management (SIEM) solutions, enhancing the overall security posture by centralizing threat detection across the entire IT environment:

- IBM QRadar DSM
- McAfee Enterprise Security Manager
- Hewlett Packard Enterprise ArcSight
- Splunk

2. Monitoring Integration and Logs

All SAP Enterprise Threat Detection Streaming applications provide an HTTP endpoint that exports certain metrics that Prometheus or any other compatible monitoring tools can consume.

Prometheus is an open-source system monitoring and alerting toolkit that is easy to use, has a wide range of support and is capable of generating alerts. Grafana or other observability tools can be used to visualize and aggregate data from various sources and provide monitoring of your log infrastructure.

2.1. Log Source Setup

SAP Enterprise Threat Detection can receive and process logs from the following sources[:

• SAP NetWeaver Application Server for ABAP -
To transfer logs from SAP NetWeaver Application Server for ABAP to SAP Enterprise Threat Detection, you can use either ABAP Log Extraction or immediate log transfer (only one)

We can use the new ABAP Log Extractor if your ABAP systems are based on SAP BASIS 7.40 or higher. If your ABAP systems are on an SAP BASIS release lower than this, you can still use Immediate Log Transfer for some log types, but for the rest, you would need to stick to the ABAP Log Extractor (Legacy).

• SAP NetWeaver Application Server for Java
• SAP HANA
• Cloud Connector logs
• SAProuter logs
• Audit logs of SAP BTP, Cloud Foundry environment
• Identity Authentication logs
• SAP Cloud Integration logs
• SAP Authorization and Trust Management service logs
• User Account and Authentication logs
• SAP BTP, Neo environment (audit logs only)
• SAP S/4HANA Cloud (Security Audit Log)
• Operating system (syslog)
• SAP Commerce
• SAP Sales Cloud and SAP Service Cloud
• Other systems

2.2. Level of Analysis & Method Summary

2.2.1. Logs of SAP NetWeaver Application Server for ABAP

Log Type	Insights	Transfer method	Available as of Basis release	Lower release
Business Transaction Log	ABAP statistics records, this is a log of system activities. Every dialog step is logged and recorded with technical information, such as response time, transaction code, or CPU time. Business Transaction Analysis data is logged by default Parameter - stat/level = 1 • Main statistic records • HTTP server records • HTTP client records • RFC server records • RFC client records • Passport records • Web service records	ABAP Log Extractor (New)	7.40 SP10	ABAP Log Extractor (Legacy)
Change Document Log	Records change to business objects, recommended provide the data for the object SECURITY_POLICY to SAP changes to ABAP profile parameters with security relevance	ABAP Log Extractor (New)	7.40 SP10	ABAP Log Extractor (Legacy)
Gateway Log	Monitors the activities of the gateway. SAP Gateway carries out RFC services within the SAP world, which are based on TCP/IP. gw/logging=ACTION=SPX LOGFILE=gw_log_$(SAPSYSTEMNAME)_$(SAPLOCALHOST)-%y&m%d SWITCHTF=day Reads actions performed during SAP systems and external programs to communicate with one another.	ABAP Log Extractor (New)	7.40 SP10	ABAP Log Extractor (Legacy)
HTTP Client Log	Logs HTTP requests from SAP NetWeaver AS for ABAP icm/HTTP/logging_client_<xx> inbound and outbound requests	Immediate Log Transfer	7.55 SP0	Not supported
HTTP Server Log	Logs HTTP requests to or from SAP NetWeaver AS for ABAP. The HTTP Server Log is not enabled by default icm/HTTP/logging_<xx> • %a (IP address of the remote host) • %b (length of the response in bytes) • %h, %h0 and %h1 (name of the remote host) • %j (HTTP or HTTPS) • %l (remote log name) • %L (duration of a request in milliseconds) (optionally surrounded by square brackets) • %r, %r0, %r1 and %r2 (first line of an HTTP request) (optionally surrounded by quotation marks) • %s (HTTP response code) • %t (time in CLF format)	Immediate Log Transfer	7.55 SP0	ABAP Log Extractor (Legacy)
Message Server Log	Logs whenever a message server is started or an application server logs on or logs off.	ABAP Log Extractor (New)	7.40 SP10	Not supported
Read	Logs read access to data that has been categorized as sensitive by	Immediate	7.53 SP0	ABAP

Access Log	legal requirements, external company policy, or internal company policy.	Log Transfer		Log Extractor (Legacy)
Security Audit Log	Transaction SM19 or RSAU_CONFIG Logs security-related events on SAP NetWeaver AS for ABAP. The system records events such as unsuccessful logon attempts, the starting of transactions or reports, or changes to user master records for your analysis. rsau/enable = on Recommend to send all event code messages from the Security Audit Log to SAP Enterprise Threat Detection	ABAP Log Extractor (New)	7.40 SP10	ABAP Log Extractor (Legacy)
SOAP Web Service Log	Logs all incoming and outgoing SOAP Web Service calls in an SAP ABAP system. The log contains information about the consumer proxy, service definition, endpoint, logical port, URLs and users involved in the web service Communication. For outgoing calls, the semantic event Executable, WebService, Call is used. For incoming requests, the semantic event Executable, WebService, Run is used	Immediate Log Transfer	7.55 SP0	Not supported
System Log	Logs all system errors, warnings, user locks due to failed logon attempts by known users, and process messages	Immediate Log Transfer	7.53 SP0	ABAP Log Extractor (Legacy)
UI Data Protection Log	Logs data entered and displayed by users in SAP systems based on the following UI channels: • SAP GUI for Windows • SAP Gateway • Web Dynpro for ABAP • Web Client UI • SAP NetWeaver BW • RFC and Web Services	Immediate Log Transfer	7.40 SP24	ABAP Log Extractor (Legacy)
User Change Log	Logs all changes made directly to the authorizations or profiles of users, as well as changes to the user password, the user type, the user group, the validity period, and the account number.	ABAP Log Extractor (New)	7.40 SP10	ABAP Log Extractor (Legacy)
Web Dispatcher Log	Logs HTTP requests to SAP Web Dispatcher icm/HTTP/logging_client_<xx> icm/HTTP/logging_<xx>	Immediate Log Transfer	7.55 SP0 (not applicable for standalone Web Dispatcher)	Not supported

Master Data Type	**Detail**	**Fallback Transfer Method**	**Transfer Method for Lower Releases**	**Available as of SAP_BASIS Release**
Configuration Checks	Contains information about standard users and profile parameters, perform user-related and profile parameter-related checks	ABAP Log Extractor (New)	ABAP Log Extractor (Legacy)	7.00 (latest SP)
Implementation Status of Security Notes	Contains information from SAP Notes, including their version, implementation status and processing status, only need to transfer the implementation status if you want to monitor the distribution of security notes.	ABAP Log Extractor (New)	ABAP Log Extractor (Legacy)	7.40 SP10

Object Directory	Contains information from the directory of repository objects like object type, object name, package, transport layer, software Component or application component, ETD performs analysis on • Service, Application Component • Service, Software Component	ABAP Log Extractor (New)	ABAP Log Extractor (Legacy)	7.40 SP10
User Contexts (Strongly recommended)	Contains user information like alias, validity, user group or user type. In addition, the personal details of the users like names, locations, functions, departments and email addresses are transferred as well.	ABAP Log Extractor (New)	ABAP Log Extractor (Legacy)	7.40 SP24
System Contexts (Strongly recommended)	Contains system information like the role, operating system or database information. It also contains information about installed components, active components, installed software products, installed software features, including software features installed Technical usages. In addition, also application server information like IP address, kernel version or operation System is transferred as well	ABAP Log Extractor (New)	ABAP Log Extractor (Legacy)	7.40 SP24

2.2.2. Logs of SAP NetWeaver Application Server for Java & Other Platforms

Log Type	Log Description
Security Log	Contains entries from security-related services, including authentication, destination service, user management, virus scanner interface, and Web services. Includes both successful and failed user logons and logouts.
Security Audit Log	Contains security events such as successful and failed user logons and the creation or modification of users, groups, and roles.
HTTP Access Log	Records client-side HTTP/HTTPS request access on the AS Java. The log extractor is disabled by default and can be written in Common Log File (CLF) or SAP format. SAP Enterprise Threat Detection recommends using CLF format for detailed user access information.
SAP HANA	Configure UDP, TCP, or TLS port for receiving syslogs. Configure SAP HANA to write its audit trail to syslog. Configure the host operating system of SAP HANA to forward its syslog to the UDP, TCP or TLS port ofthe log collector. or provide logs from SAP HANA via database subscriber by creating a view and
Logs from SAProuter	SAProuter needs to be started with parameter -G <logfile>. Enable the log collector to access the log directory where the SAP router logs are stored. To do so, install the log collector locally on the SAProuter system, reading files from the local directory. Configure a directory reader for the SAProuter logs.
Cloud Connector	Set Audit log and install log collector locally on the Cloud Connector system, reading audit log files from the local directory, Configure a directory reader for the _crossaccount folder and each subaccount folder.
Logs from SAP Cloud Solutions	can consume audit logs from the SAP Business Technology Platform (SAP BTP, Cloud Foundry environment). To connect to the SAP Business Technology Platform, you must manually create access tokens in your subaccounts and make these tokens available to the log collector.
SAP Commerce	SAP Commerce Generic Audit tracks changes in specific database tables according to the SAP Commerce audit configuration and writes them to separate database tables as change logs following the <deploymentName><numericTypeCode>sn naming convention.
SAP Sales Cloud and SAP Service Cloud	SAP Enterprise Threat Detection can consume the following logs from SAP Sales Cloud and SAP Service Cloud: User Activation and Deactivation Log (RPCCAB02_Q001) and User Logon Activity (RPCOD_USER_LOGON_ANA_Q0001).

Security Audit Logs from SAP S/4HANA Cloud	can consume Security Audit Logs from SAP S/4HANA Cloud. To enable this, you must configure the SAP Enterprise Threat Detection log collector to fetch data via the OData Subscriber.
Syslog from the Operating System	can consume operating system logs in syslog format.
Windows Event Logs from Operating Systems	can consume raw Windows Event XML Logs from the connected systems.

2.3. Log Learning and Observability

SAP Enterprise Threat Detection to monitor external systems whose logs cannot be processed by SAP Enterprise Threat Detection by default, you can teach SAP Enterprise Threat Detection to convert these logs into semantic events[1].

It allows you to analyze events in a forensic lab. To enable the analysis and correlations across log sources, incoming logs must be normalized to the semantic data model of SAP Enterprise Threat Detection with its semantic events and attributes. For more information about semantic attributes and events

2.3.1. Log Layouts Supported

Structured logs have a regular structure with a fixed number of elements of a log entry, separated by a fixed separator. Logs with Key-Value Lists with a header (for example, a timestamp), followed by a list of key-value pairs. Free-text logs are a mixture of fixed text, variables, and the key-value list; JSON logs are also considered Free-text logs. For more details, check here.

2.4. SAP Enterprise Threat Detection Integration with Splunk

This integration allows us to forward alerts from SAP Enterprise Threat Detection to Splunk as high-value log events in order to allow further investigation of threats found in SAP systems on the infrastructure level.

It is also possible to forward Splunk alerts to SAP Enterprise Threat Detection as high-value log events in order to allow further investigation and correlation of threats detected on the infrastructure level with logs of your SAP system landscape.

2.4.1. SAP Enterprise Threat Detection to Splunk

Alerts are forwarded from SAP Enterprise Threat Detection to Splunk via Splunk's HTTP Event Collector. To find the forwarded alerts within Splunk, search for the source type sapetd_alert.

2.4.2. Splunk to SAP Enterprise Threat Detection

Alerts are forwarded from Splunk to SAP Enterprise Threat Detection via the HTTP Listener of the log collector. They are forwarded via the same HTTP(S) endpoint as, for example, SAP AS ABAP logs. We deliver the necessary log learning rules so that you can easily find your Splunk alerts in the forensic lab by searching for either the event log type SplunkAlert or the semantic event Alert, Splunk. You have to download, install and configure the SAP Enterprise Threat Detection for Splunk app from SplunkBase. For the configuration, you must provide the Splunk administrator with the hostname, port, protocol (http or https), username and password of the HTTP endpoint of the log collector.

3. Conclusion

SAP Enterprise Threat Detection is a critical component in the cybersecurity toolkit of any organization leveraging SAP systems. By providing real-time threat detection, comprehensive monitoring, and seamless integration with third-party tools, SAP ETD helps protect against the ever-evolving landscape of cyber threats. Organizations that adopt SAP ETD can enhance their resilience, ensuring their intelligent enterprise remains secure and compliant in a challenging digital environment. There are other 3rd party tools by companies like onapsis, which excelled in SAP cybersecurity Security assessments and vulnerability scanning, Change control and compliance management, Security automation and orchestration.

References

[1] Susanmarie Thomas, Introduction to Semantic Events and Attributes, SAP Community, 2016. [Online]. Available: community.sap.com/t5/application-development-blog-posts/introduction-to-semantic-events-and-attributes/ba-p/13199830

[2] SAP Security Notes and News, Sap Support, 2019. [Online]. Available: support.sap.com/en/my-support/knowledge-base/security-notes-news.html

[3] SAP Help Portal, Sap.com, 2024. [Online]. Available: https://help.sap.com/docs/

[4] SAP Enterprise Threat Detection, SIEM and Cybersecurity, SAP, 2017. [Online]. Available: https://www.sap.com/products/financial-management/enterprise-threat-detection.html

[5] Brian Carlson, Top Cybersecurity Statistics, Trends, and Facts, CSO Online, 2021. [Online]. Available: www.csoonline.com/article/571367/top-cybersecurity-statistics-trends-and-facts.html