University of Bucharest
Faculty of Mathematics and Computer Science
"Security and Applied Logic" MA Program

Cybersecurity

Presentation by
Ion-Gabriel IONESCU

Today's course topic:

Security Information and Event Management (SIEM)

Contents

>>> Brief cybersecurity knowledge refresh

>>> What is a SIEM and why is it important?

>>> The general functionality of a SIEM solution

>>> The benefits and capabilities of a SIEM

>>> Use cases

>>> Best practices when deploying a SIEM

>>> Question & Answer session (Q&A)

>>> Brief cybersecurity knowledge refresh

The main Cybersecurity domains and their subdomains:

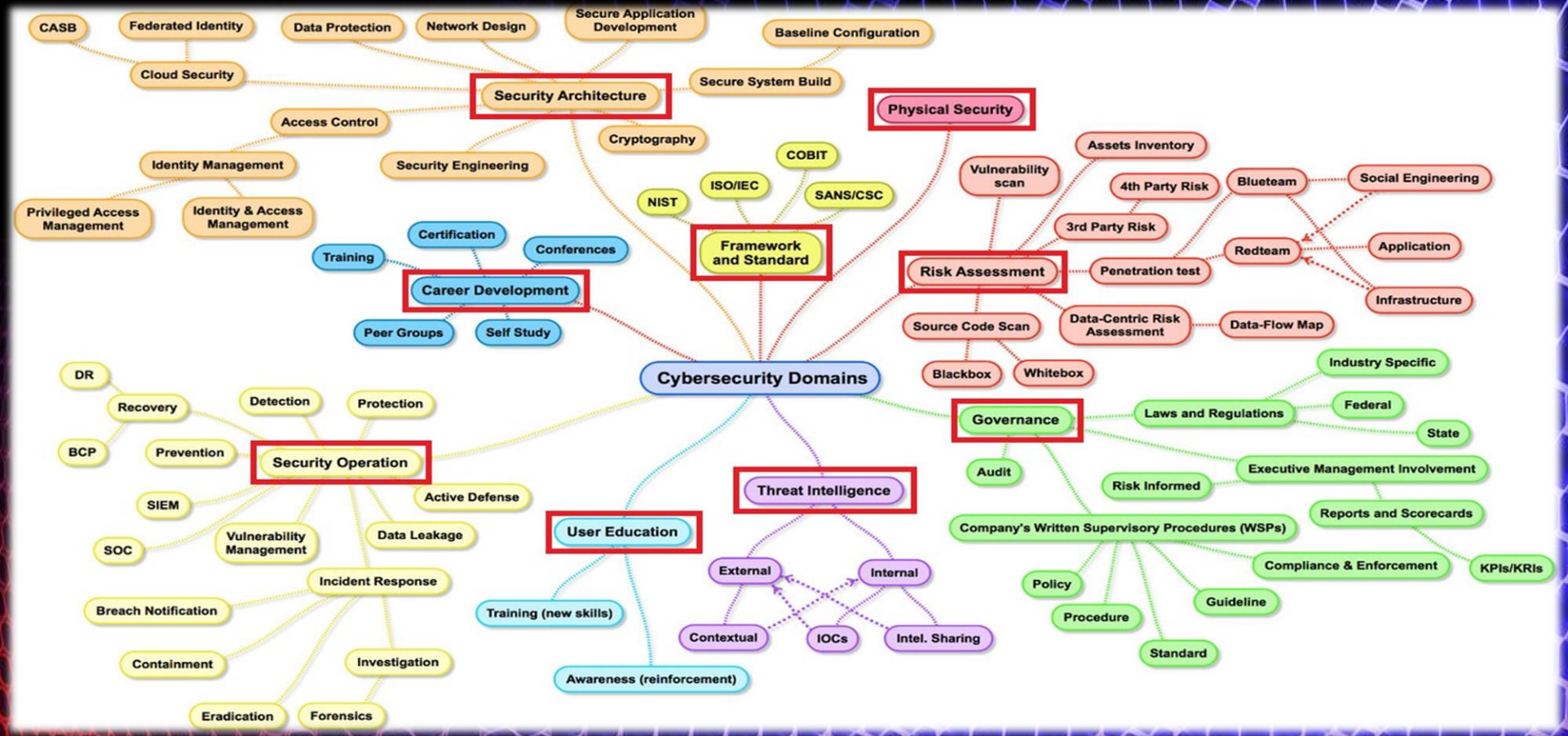

Image source: https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp

>>> Brief cybersecurity knowledge refresh

The Defense-In-Depth illustration:

Image source: https://www.researchgate.net/figure/The-Fan-illustrating-technology-and-process-defense-in-depth-architectural-pictorial_fig1_278676540

>>> Brief cybersecurity knowledge refresh

The cybersecurity definitions for: events, alerts and incidents.

- An event is an observed modification in the usual or normal behavior of an environment, workflow, system, process, and/or user.

- An alert is a notification that a particular event or a set of events has taken place.

- An incident is an event that can affect the confidentiality, integrity, and/or availability of an organization's assets. Incidents can have different levels of impact on the business, from low to critical.

>>> What is a SIEM and why is it important?

Defining a SIEM solution and its importance:

Security Information and Event Management, or SIEM for short, is a solution that allows organizations to monitor in real-time their IT environment, analyze events, as well as, track and log security data for compliance or auditing purposes.

Over the years, SIEMs have evolved so much that they have become more than just log management tools. Nowadays, SIEMs can even offer advanced user and entity behavior analytics (UEBA) thanks to AI and machine learning. UEBA plays a significant role in detecting modifications in the behavior of a user.

Security Information and Event Management (SIEM) is the result of merging Security Information Management (SIM) and Security Event Management (SEM) into one solution.

>>> The general functionality of a SIEM solution

Typical topology of an organization's IT infrastructure:

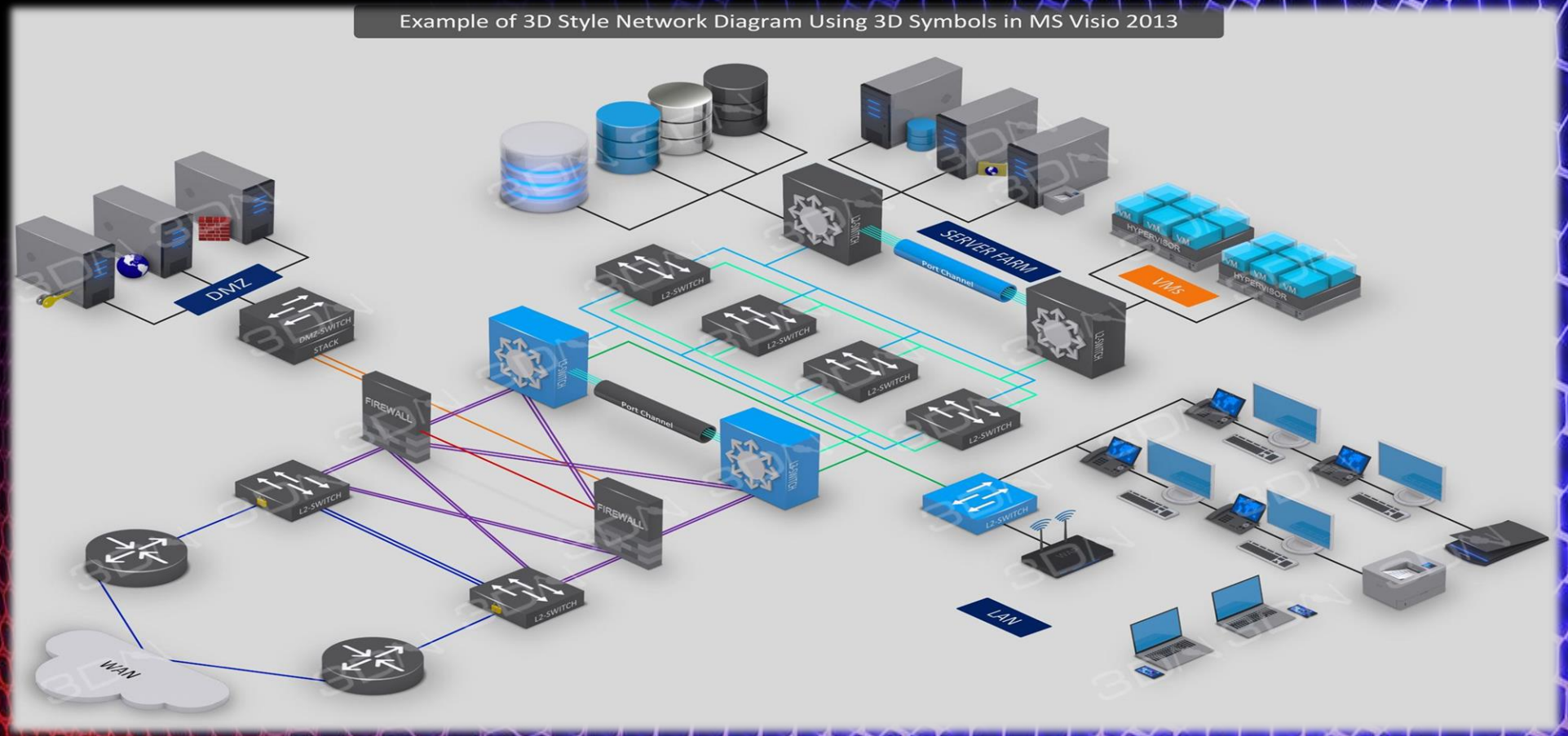

Image source: https://i.pinimg.com/originals/79/82/25/7982250dca5d1675a7f772410bbb4f9a.jpg

>>> The general functionality of a SIEM solution

Examples of devices from which the SIEM can collect logs:

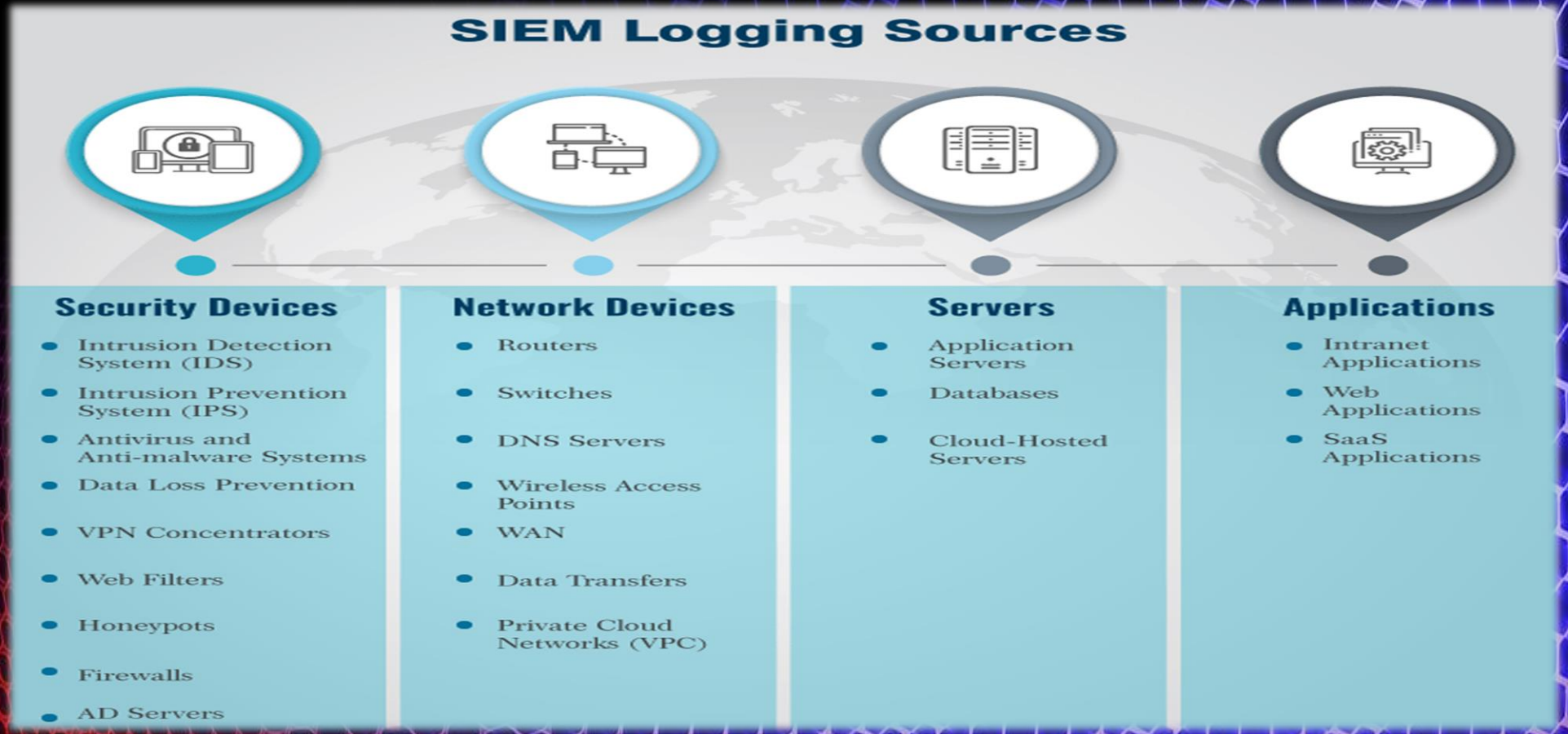

Image source: https://layots.com/security-information-and-event-management-siem-solution-its-importance/

>>> The general functionality of a SIEM solution

Basic functionality diagram of a SIEM solution:

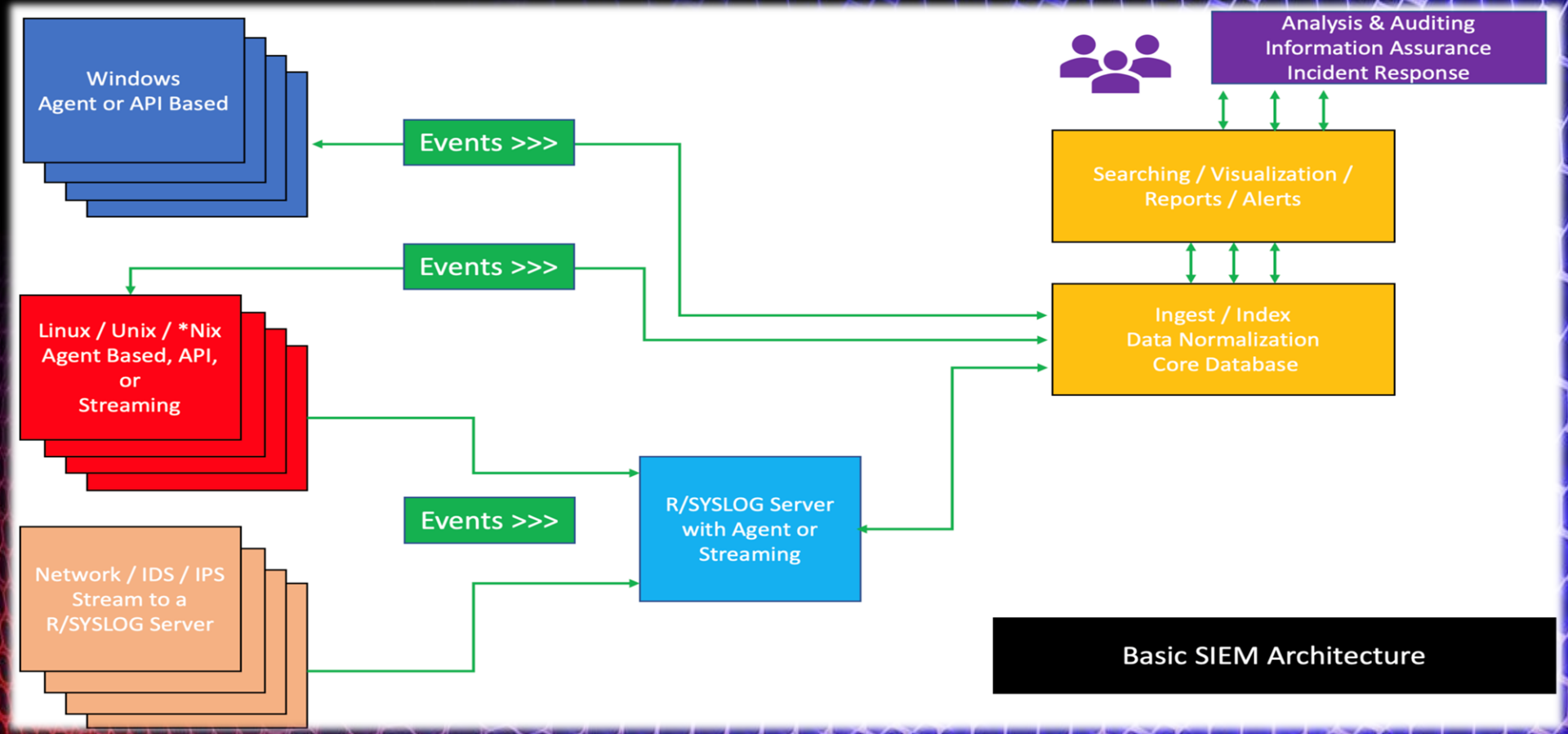

Image source: https://en.wikipedia.org/wiki/Security_information_and_event_management

>>> The benefits and capabilities of a SIEM

List of components and capabilities found in most SIEMs:

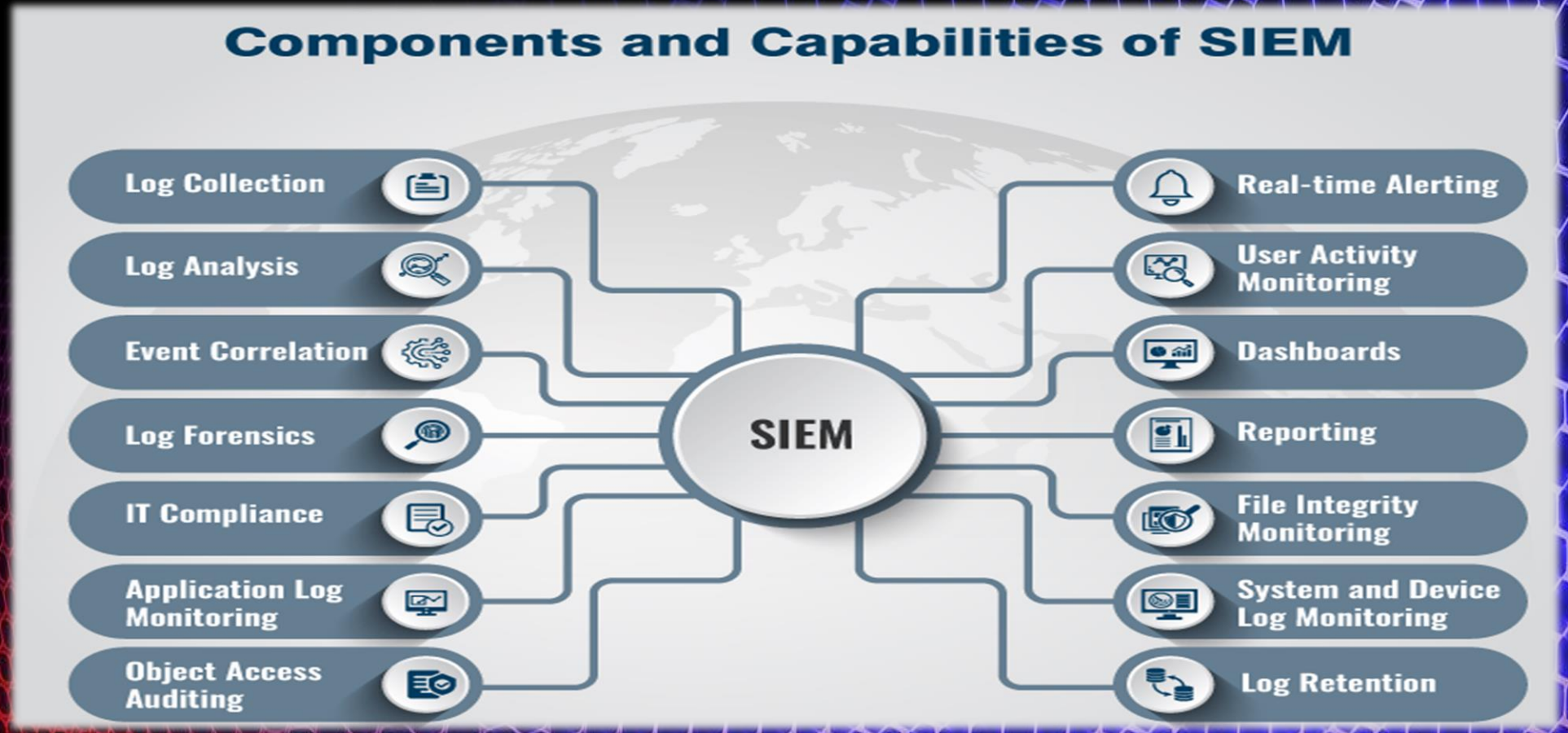

Image source: https://layots.com/security-information-and-event-management-siem-solution-its-importance/

>>> The benefits and capabilities of a SIEM

Log management:

Most SIEM solutions can collect event data from various internal sources, as well as from external ones (such as AWS servers). The data is collected, indexed (stored), and analyzed in real-time.

It is important to keep in mind that almost every equipment generates data, however, the generated data can be unstructured or structured in many ways.

For the indexed data to be easily searched, the SIEM is parsing it, giving it a structured form.

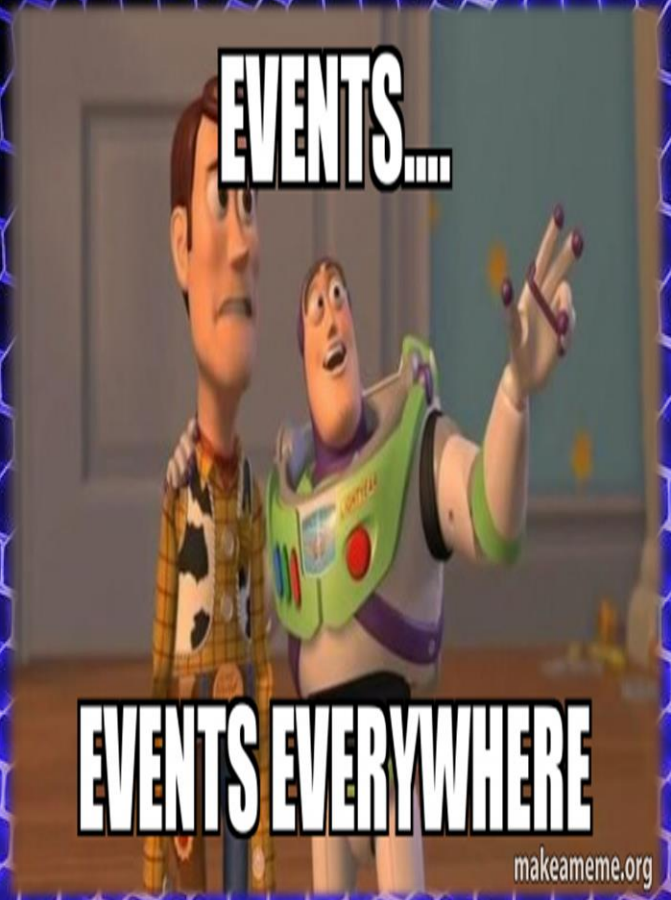

Image source: https://makeameme.org/meme/events-events-everywhere-5cc32b

>>> The benefits and capabilities of a SIEM

Parsing the logs: From unstructured to structured

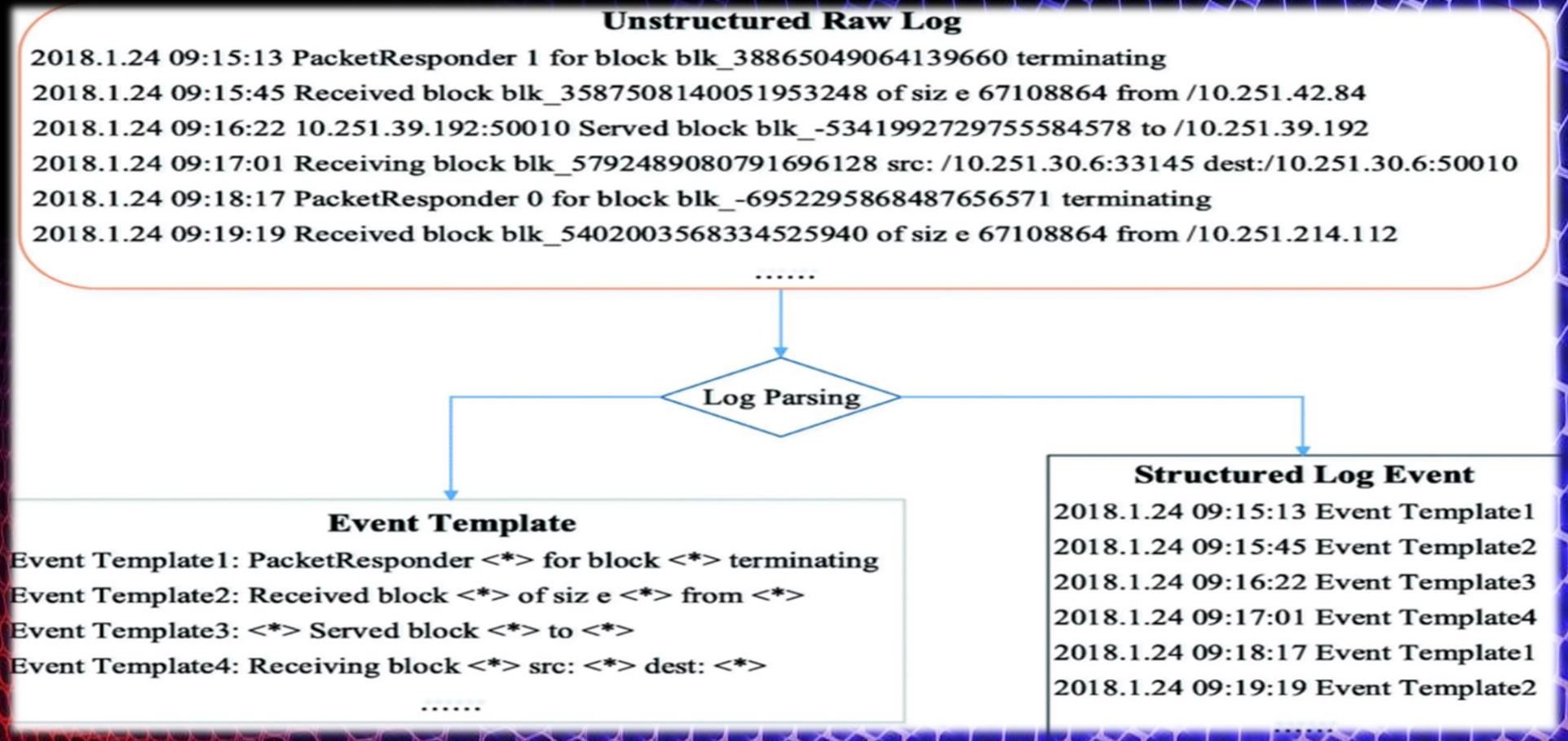

Image source: https://www.researchgate.net/figure/A-simple-example-of-log-parsing-Log-parsing-converts-unstructured-log-messages-into_fig1_338606640

>>> The benefits and capabilities of a SIEM

Parsing the logs: From unstructured to structured

Logging statement	logInfo("Found block *$blockId* locally") (From: spark/storage/BlockManager.scala)
Raw log (Unstructured)	17/06/09 20:11:11 INFO storage.BlockManager: Found block *rdd_42_20* locally
Parsed log (Structured)	**Timestamp**: 17/06/09 20:11:11; **Level**: INFO **Logger**: storage.BlockManager **Static template**: Found block <*> locally **Dynamic variable(s)**: *rdd_42_20*

Image source: https://deepai.org/publication/logram-efficient-log-parsing-using-n-gram-dictionaries

>>> The benefits and capabilities of a SIEM

Event correlation and analytics:

One of the main processes that an SIEM solution performs is called correlation. This process is performed by utilizing advanced analytics, which helps in identifying and understanding complex data patterns that would be otherwise extremely difficult to understand by just looking over numerous logs, events, and so on. In other words, the process of correlating aids in providing a clearer picture of what is going on within the environment and provides the opportunity to mitigate potential threats that could disrupt the business.

By utilizing a SIEM solution, the mean time to detect (MTTD), as well as, the mean time to respond (MTTR), are significantly shortened in the event of an IT incident.

>>> The benefits and capabilities of a SIEM

Incident monitoring and security alerts:

By utilizing predefined and custom correlation rules, SIEM administrators and authorized personnel can create, modify, or remove alerts for specific events that are taking place in the network.

Utilizing customizable, predefined correlation rules, the administrators and the authorized personnel can be alerted immediately so that they can take all the appropriate actions in order to mitigate the threat.

Image source: https://www.stormshield.com/news/security-alert-september-2021-stormshields-product-response/

>>> The benefits and capabilities of a SIEM

Compliance management and reporting:

Over time, SIEMs have become a popular choice among organizations due to the different forms of regulatory compliance with which they (the organizations) need to comply in order to conduct business. Therefore, because of the data gathering and analysis functions that it offers, a SIEM plays a vital role when it comes to collecting and verifying compliance data across the business environment.

SIEMs can generate compliance reports for various compliance standards, such as SOX, PCI-DSS, HIPPA, GDPR, and others.

Image source: https://ichillrefrigeration.co.nz/compliance/

>>> The benefits and capabilities of a SIEM

Benefits:

- ❑ Real-time threat recognition
- ❑ Detecting advanced & unknown threats
- ❑ Monitoring of users and applications
- ❑ Assessing and reporting on compliance
- ❑ Conducting forensic investigations
- ❑ Regulatory compliance auditing
- ❑ AI-driven automation

Image source: https://www.lifevisionkeys.com/yourlifepurpose/2019/01/12/5-life-changing-benefits-hidden-into-your-life-vision/

>>> Use cases

Examples of use cases:

1. SIEM visibility and anomaly detection could help detect zero-days or polymorphic code. This is primarily due to low rates of anti-virus detection against this type of rapidly changing malware.

2. Parsing, log normalization, and categorization can occur automatically, regardless of the type of computer or network device, as long as it can send a log.

3. Visualization with a SIEM using security events and log failures can aid in pattern detection.

Source: https://www.ibm.com/topics/siem

>>> Use cases

Examples of use cases (continue):

4. A SIEM uses pattern detection, alerting, baselines, and dashboards to identify anomalies that can indicate a misconfiguration or a security issue.

5. SIEMs can spot covert, malicious communications and encrypted channels.

6. Cyberwarfare can be detected by SIEMs with accuracy, discovering both attackers and victims.

Source: https://www.ibm.com/topics/siem

>>> Best practices when deploying a SIEM

Examples of best practices for when deploying a SIEM:

- Begin by fully understanding the scope of your implementation. Define how your business will best benefit from the deployment and set up the appropriate security use cases.

- Design and apply your predefined data correlation rules across all systems and networks, including any cloud deployments.

- Identify all of your business compliance requirements and ensure your SIEM solution is configured to audit and report on these standards in real-time so you can better understand your risk posture.

Source: https://www.ibm.com/topics/siem

>>> Best practices when deploying a SIEM

Examples of best practices for when deploying a SIEM (continue):

- Catalog and classify all digital assets across your organization's IT infrastructure. This will be essential when managing log data, detecting access abuses, and monitoring network activity.

- Establish BYOD (Bring Your Own Device) policies, IT configurations, and restrictions that can be monitored when integrating your SIEM solution.

- Regularly tune your SIEM configurations to ensure you're reducing false positives in your security alerts.

Source: https://www.ibm.com/topics/siem

>>> Question & Answer session (Q&A)

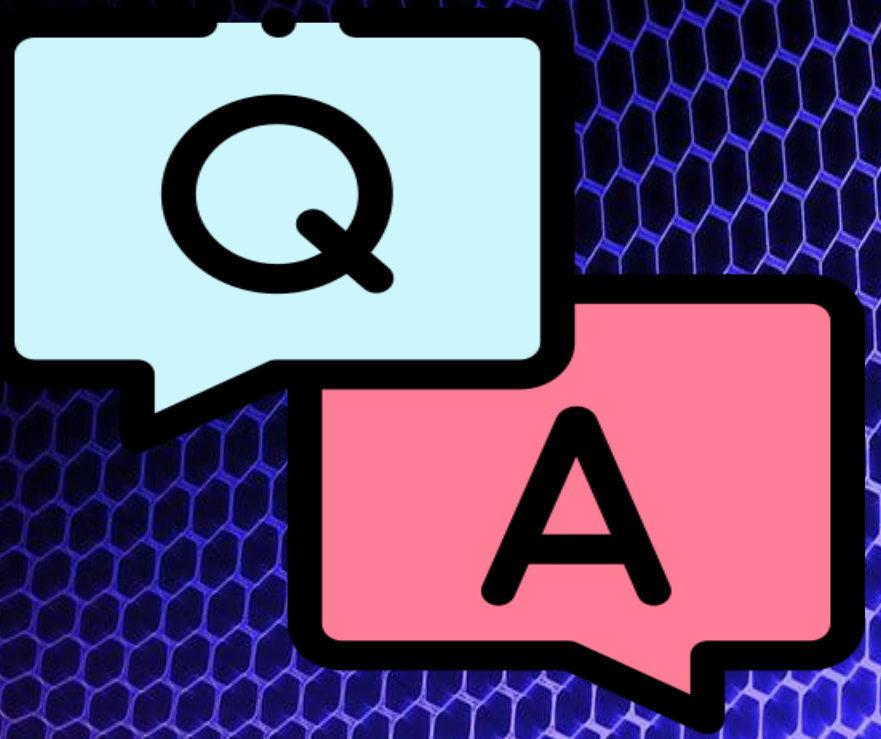

Image source: https://www.flaticon.com/free-icon/q-and-a_2274755

>>> References

For more details regarding SIEMs, please visit:

1. https://www.fireeye.com/products/helix/what-is-siem-and-how-does-it-work.html

2. https://www.coresecurity.com/siem#what-siem

3. https://www.ibm.com/topics/siem

4. https://static.helpsystems.com/core-security/pdfs/guides/cs-event-manager-customer-use-case-gd.pdf

5. https://www.varonis.com/blog/what-is-siem/

Thank you very much for your attendance and attention!