Bibliography

[1] *Apache Cassandra's website*. Mar. 2021. URL: https://cassandra.apache.org/.

[2] *Apache Kafka's website*. Mar. 2021. URL: https://kafka.apache.org/.

[3] *Apache Spark's website*. Mar. 2021. URL: https://spark.apache.org/.

[4] Armbrust, Michael, Das, Tathagata, Torres, Joseph, Yavuz, Burak, Zhu, Shixiong, Xin, Reynold, Ghodsi, Ali, Stoica, Ion, and Zaharia, Matei. "Structured streaming: A declarative API for real-time applications in apache spark". In: *Proceedings of the 2018 International Conference on Management of Data*. Houston TX USA, June 2018, pp. 601–613.

[5] Carcillo, Fabrizio, Dal Pozzolo, Andrea, Le Borgne, Yann-Aël, Caelen, Olivier, Mazzer, Yannis, and Bontempi, Gianluca. "Scarff: a scalable framework for streaming credit card fraud detection with spark". In: *Information fusion* 41 (May 2018), pp. 182–194.

[6] Casas, Pedro, Soro, Francesca, Vanerio, Juan, Settanni, Giuseppe, and D'Alconzo, Alessandro. "Network security and anomaly detection with Big-DAMA, a big data analytics framework". In: *2017 IEEE 6th international conference on cloud networking (CloudNet)*. Prague, Czech Republic, Sept. 2017, pp. 1–7.

[7] *Elastic Search's website*. Mar. 2021. URL: https://www.elastic.co/fr/.

[8] *EQL Search*. Mar. 2021. URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl.html.

[9] *Esper's website*. Mar. 2021. URL: https://www.espertech.com/esper/.

[10] Ficco, Massimo and Romano, Luigi. “A generic intrusion detection and diagnoser system based on complex event processing”. In: *2011 First International Conference on Data Compression, Communications and Processing*. IEEE. Palinuro, Italy, June 2011, pp. 275–284.

[11] *Flink’s website*. Mar. 2021. URL: https://flink.apache.org/.

[12] Hafsa, Mounir and Jemili, Farah. “Comparative study between big data analysis techniques in intrusion detection”. In: *Big Data and Cognitive Computing* 3.1–13 (Dec. 2018), p. 1.

[13] Husák, Martin, Čermák, Milan, Laštovička, Martin, and Vykopal, Jan. “Exchanging security events: Which and how many alerts can we aggregate?” In: *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. Lisbon, Portugal, May 2017, pp. 604–607.

[14] Husák, Martin and Kašpar, Jaroslav. “AIDA framework: Real-time correlation and prediction of intrusion detection alerts”. In: *Proceedings of the 14th International Conference on Availability, Reliability and Security*. Canterbury CA United Kingdom, Aug. 2019, pp. 1–8.

[15] *Ionos website: Apache Kafka*. Mar. 2021. URL: https://www.ionos.fr/digitalguide/serveur/know-how/apache-kafka/.

[16] Ivanov, Todor and Taaffe, Jason. “Exploratory analysis of spark structured streaming”. In: *Companion of the 2018 ACM/SPEC International Conference on Performance Engineering*. Berlin, Germany, Apr. 2018, pp. 141–146.

[17] *Kafka Documentation*. Mar. 2021. URL: http://kafka.apache.org/documentation.html#security.

[18] *Kafka-Proxy Documentation*. Mar. 2021. URL: https://github.com/grepplabs/kafka-proxy/tree/master.

[19] Kotenko, Igor, Kuleshov, Artem, and Ushakov, Igor. “Aggregation of elastic stack instruments for collecting, storing and processing of security information and events”. In: *2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. San Francisco, CA, USA, Aug. 2017, pp. 1–8.

[20] *Next generation SIEM*. Mar. 2021. URL: https://www.securonix.com/what-is-next-generation-siem/.

[21] Oasis. *STIX™ Version 2.0. Part 5: STIX Patterning*. Mar. 2021. URL: http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part5-stix-patterning.html.

[22] *OVHcloud's website*. Mar. 2021. URL: https://www.ovh.com/fr/.

[23] *Query DSL*. Mar. 2021. URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl.html.

[24] Ramaki, Ali Ahmadian, Amini, Morteza, and Atani, Reza Ebrahimi. "RTECA: Real time episode correlation algorithm for multi-step attack scenarios detection". In: *computers & security* 49 (Mar. 2015), pp. 206–219.

[25] *Security Information and Event Management*. Mar. 2021. URL: https://fr.wikipedia.org/wiki/Security_information_management_system.

[26] *Sigma Correlations*. Mar. 2021. URL: https://onedrive.live.com/view.aspx?resid=3454E59DF98D7D65!7485&ithint=file%5C%2cdocx&authkey=!ADb97TgRX9Fr4xQ.

[27] *Sigma github*. Mar. 2021. URL: https://github.com/Neo23x0/sigma.