Supporting Cyber Intelligence Analysts with Enterprise Security Modeling

Sung Kim, Kees Leune and Christopher Benson
Adelphi University, Garden City, NY, USA

sungkim@adelphi.edu
leune@adelphi.edu
cbenson@adelphi.edu

Abstract: To maximize the value of human defensive cybersecurity intelligence analysts, effective situational awareness and triage capabilities are critical success factors. We describe an approach to support analysts with developing and maintaining service-oriented models that describe the security-relevant aspects of an enterprise. We refer to these models as enterprise security models. Inspired by enterprise architecture approaches, our enterprise security models are described from three perspectives: a business perspective, an application perspective, and an implementation perspective. The business perspective provides the business context in which activities take place. The application perspective refines business processes and activities into services. The implementation perspective provides the technical implementation details. The enterprise security model can be combined, through automation, with cyber threat intelligence to prioritize threats facing the enterprise. Cyber threat intelligence is commonly viewed at three different levels: strategic, operational, and tactical intelligence. These levels of threat intelligence correspond to the three perspectives in our proposed enterprise security modeling approach. It is our assertion that the ability to organize the enterprise architecture with a security focus viewed from the business, application, and implementation perspectives allows an organization to process different levels of threat intelligence in their proper context and to respond appropriately. Human security analysts can focus on threats that are likely to manifest, in the way in which they have been observed to manifest. This paper presents work on the creation and maintenance of enterprise security models. By using a proof-of-concept scenario, we suggest that a service-based modeling approach is effective to describe cybersecurity-relevant data concerning enterprise information systems architecture. Given the complexity of current enterprise architectures and the rapidly changing threat landscape, it is necessary to develop a well-developed situational awareness that spans the full enterprise. Our proposed modeling approach can provide the proper context for automation efforts to support human analysts in developing and maintaining such awareness.

Keywords: Cybersecurity, Threat intelligence, Threat modeling, Enterprise architecture, Services

1. Introduction

To maximize the effectiveness of human defensive cybersecurity intelligence analysts, situational awareness and triage capabilities are critical success factors. Modern enterprise-defenders rely on cyber threat intelligence to accomplish this. Cyber Threat Intelligence (CTI) is commonly defined as threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes (Johnson et al., 2016). One can safely argue that it is almost infeasible for a human to appropriately deal with all these requirements (Nespoli et al., 2017) through manual processes. Approaches to cyber threat analysis supported by automation are frequently considered to be a critical success factor in cyber defense (Kaiser et al., 2022).

While many enterprises use CTI to implement blocklists containing IP addresses, email addresses, or domain names, these actions are commonly taken proactively and without directly relating the perceived threat to the actual defended environment. In other words, security engineers routinely implement large blocklists without evidence that these blocked entities pose direct threats. Aside from operationalizing CTI to implement blocklists, security research has yielded novel and innovative approaches to improve the usability of threat intelligence. For example, Li et al. (2023) propose an analysis method based on knowledge graphs which automatically extracts information from CTI and presents it to experts. However, experts will still need to make a manual determination concerning the risk posed by each specific threat. We investigate if cyber threat analysts who are supported with service-oriented models that describe the security-relevant aspects of an enterprise can more effectively triage threat intelligence and improve their situational awareness.

Threat modeling is an approach for identifying potential threats to a given system from the viewpoint of a hypothetical attacker (Jamil et al., 2021). While it has become a viable practice for secure software development (Xu et al., 2012), broader applications are rare. Traditional modeling methodologies are difficult to apply to an entire enterprise infrastructure, leaving organizations to adopt a risk-based prioritization approach and deploy protections with incomplete information on the likely threats that can impact the organization and where the gaps in the defense exist (Bokan and Santos, 2024).

Enterprise architecture sets out to optimize across the enterprise the often-fragmented legacy of processes into an integrated environment that is responsive to change and supportive of the delivery of the business strategy (TOGAF, n.d.).

We introduce the term *enterprise security modeling* to signify the creation of models that can be used to associate cyber threat intelligence to components in the enterprise architecture. In particular, in accordance with (Leune and Kim, 2021), we adopt a service-oriented perspective to create these models.

We state the hypothesis that a multi-layered service-based approach to creating enterprise security models is an effective way to capturing the relevant aspects of a security architecture. We postulate that these models better support human analysts, through automation, with triaging threat intelligence and improving situational awareness. We demonstrate that the framework is logically consistent and discuss the results of a proof-of-concept scenario in which we establish initial validation of our approach.

2. Related Work

2.1 Cyber Threat Intelligence

Cyber threat intelligence (CTI) is commonly viewed at three different levels: strategic, operational, and tactical (Intelligence and National Security Alliance Task Force, 2013). Strategic intelligence is high-level information consumed by those that control the strategy of an organization, typically executive teams or management (Borum et al., 2015; Amato et al., 2020). Operational intelligence deals with information related to tools, tactics, techniques and procedures (TTPs) employed by an actor. Tactical intelligence is focused on technical information, and it is provided in Indicators of Compromise (IoCs) and technical descriptions.

Technical or tactical CTI takes the form of IoCs, including information such as hash values of malware, IP address ranges, or domain names. At the other end of the spectrum, TTPs observed in attacks represent operational CTI (Leite et al., 2023). It is difficult to identify and process operational CTI, although the ability to detect threats based on TTPs is integral to an effective cyber defense (Bromander et al., 2021).

Literature has shifted to focus on the ability to process high-level CTI to generate hypotheses about attack patterns and create actionable targets for threat hunting. Karuna et al. (2021) propose using natural language processing to automate extraction of threats from human-language TTP write-ups. Gao et al. (2021) propose ThreatRaptor to extract knowledge about threat behaviors from unstructured CTI reports and use the extracted knowledge to facilitate threat hunting. Li et al. (2023) propose automatic analysis of CTI using a pre-trained model that can extract threat actions and use ATT&CK and D3fend knowledge graphs to provide actionable countermeasures. Kaiser et al. (2023) propose a multi-level threat knowledge base and an Attack Hypothesis Generator that infers attack technique hypotheses using graph analytics. With this shift to the generation and processing of high-level CTI and TTPs, it is increasingly vital to have an accurate and updated threat model.

2.2 Enterprise Architecture

The idea of enterprise architecture (EA) was developed in the late 1980s, motivated by the need to align business and information technology aspects of an organization (Gerber et al., 2020). The genesis of EA is broadly attributed to John Zachman (1987), who noted that the ability to distribute large amounts of computing facilities to remote locations required some sort of “architecture” because “decentralization without structure is chaos.” Today, EA is more broadly thought of as a “continuous practice of describing the essential elements of a sociotechnical organization, their relationships to each other and to the environment, in order to understand complexity and manage change (Gerber et al., 2020).” Several other EA frameworks have been proposed since the Zachman framework. While the original Zachman proposal did not encompass supporting a more strategic planning methodology to facilitate a business strategy (Zachman, 1987), other EA frameworks focus more on the alignment of strategic goals with the evolution of the enterprise (Dumitriu and Popescu, 2020). A key objective of EA is to create a consistent model of an enterprise’s structure and organization, including its goals and its processes (Grov, Mancini and Mestl, 2019).

One particular approach of note is The Open Group Architectural Framework (TOGAF), designed in 1995 and based on the United States Department of Defense’s Technical Architecture Framework for Information Management (TOGAF, n.d.). TOGAF is based on an iterative process model and features three levels of principles to help decision making throughout the enterprise (Dumitriu and Popescu, 2020). The three basic domains are identified as the business, information system, and technology architecture. Rohloff (2005)

reorganizes these domains into the Business Architecture, Application Architecture, and Infrastructure Architecture.

Viewing the enterprise architecture as being divided into three domains lends itself intuitively to the threat modeling process. The business architecture describes the requirements of the business based on business strategy and objectives. The application architecture gives an overview of the applications supporting the business processes. The infrastructure architecture includes the software, hardware, and network infrastructure required for the operation of the applications (Rohloff, 2005). These different layers can intuitively be mapped to threat modeling and cyber defense strategies.

2.3 Threat Modeling

Threat modeling is a structured process used to identify potential threats to the system (Shi et al., 2022). Threat modeling has several benefits, such as identifying business logic flaws and critical vulnerabilities; identifying, assessing, and prioritizing potential threats; and addressing issues early in the development process (Messe et al., 2020).

A modeling approach must account for the hardware, software, network, infrastructure, and human aspects of the current system, which is difficult to keep up-to-date, particularly for complex systems (Jamil et al., 2021). Because threat modeling places a heavy reliance on manual effort and requires a high level of expertise, continuous threat modeling or frequent iterations of threat analysis can be cost-prohibitive (van Landuyt et al., 2021).

Efforts have been made to incorporate security-related considerations into EA frameworks. The Sherwood Applied Business Security Architecture (SABSA) touts a "business-driven approach" that can be integrated with existing EA to derive security solutions (Burkett, 2012). Pleinevaux (2016) proposes a metamodel based on the SABSA framework that highlights the importance of the notions of business attributes, domains, and risk. McClintock et al. (2020) propose a security EA framework based on the ZFEA that applies the original six perspectives and interrogatives but with a security focus. Loft et al. (2022) propose an agile EA approach to managing security risks that uses a matrix with 40 performance markers across eight domains and five levels.

Various approaches have been introduced to add semantics to EA frameworks to facilitate security-related analysis. Grandry, Feltus and Dubois (2013) propose applying the Open Group's ArchiMate, a standard EA modeling language, to incorporate concepts of information system security risks management, focusing on asset-related and risk-related concepts. Kang et al. (2010) propose modeling EA with ontologies in three levels to define business terms, describe components of the EA, and describe the relationships among those components. Janulevičius et al. (2017) propose an ontology for cloud security management and an implementation to an EA modeling language. Välja et al. (2020) propose an ontology framework for an automated threat model creation process, albeit based on conceptual models that abstracts out implementation details. Komárková et al. (2018) propose CRUSOE, an extensible data model that features seven layers, each of which viewing the system from a different perspective. Husák et al. (2022) build on the earlier CRUSOE model to propose a toolset for supporting security analysis and incidence response. Ellerhold, Schnagl and Schreck (2023) propose using the Factor Analysis of Information Risk (FAIR) methodology in conjunction with MITRE ATT&CK to estimate the frequency of loss events based on attack scenarios.

Potential obstacles are present when attempting to model a complex enterprise for the purposes of security analysis. Grov, Mancini and Mestl (2019) identify two challenges they identified during their work on enterprise security architecture with the Norwegian Armed Forces: modeling at a suitable level of detail while keeping the complexity at an appropriate level for analysis; and the lack of support for automated tools to analyze the models as the scale and complexity rises. Jiang et al. (2024) examine efforts to incorporate security analysis in critical infrastructures and highlight the need to enhance the robustness and practical applicability of EA models in cybersecurity.

Efforts to automate the creation and processing of CTI further compels the drive towards facilitating automation in threat modeling. An automated hardware and software threat modeling approach can help find potential problems in the system—particularly in the design stage—and alleviate the high cost of threat modeling activities (Martins et al., 2015). However, the models must reflect the actual state of the enterprise, must be maintainable, and must have enough semantics to support security analysis.

3. A Framework for Enterprise Security Modeling

3.1 Philosophy

We propose an approach in which human analysts develop and maintain service-oriented models that describe the security-relevant aspects of an enterprise. These models, which we refer to as *enterprise security models*, are subsequently combined with threat intelligence data using automated processes to triage threats. By doing so, we shift the attention of the human analyst from threats that *might potentially* manifest, to threats that are *likely* to manifest.

We assert that the three levels of threat intelligence roughly correspond to the levels commonly distinguished in EA models. We accommodate for them by identifying three layers of abstraction in our approach: A business layer, an application layer, and an implementation layer. Like TOGAF (n.d.) we acknowledge that it is impossible to take one comprehensive perspective when engaging in enterprise security modeling. As a solution, we propose a service-centered approach that distinguishes these three core abstraction layers.

3.2 Proof-of-Concept Scenario

We applied our framework to an information technology infrastructure utilizing both on-premise and cloud-based applications. We established that a typical authentication exchange consists of users using both a username/password and a multi-factor authentication (MFA) step to access services. After logging in with the correct credentials, a push notification is sent to the user's registered device. If the user passes both authentication challenges, they will authenticate to the service they are attempting to access. This approach to MFA is in line with present-day industry best practices.

3.3 The Business Layer

The *Business Layer* aligns with the EA business architecture domain and focuses on strategy and objectives, and intersects with the concept of strategic threat intelligence. It describes business functions from a service-oriented perspective and introduces vocabulary items *business service* and *activity*. Semantically, *business services* enable *activities*, while activities may require business services.

In the scenario described above, the ability to determine the identity of an individual is captured in the form of a business service. The activity that requires validation of credentials is enabled by an authentication business service.

3.4 The Application Layer

The application layer extends and refines the business layer by providing constructs that map to specific TTPs. As such, it maps to operational cyber threat intelligence. In the application layer, we introduce *application services* as implementations of business services. Activities are further refined into two additional vocabulary elements: *events* and *event channels*.

Application services represent abstract representations of the products used to provide a business function. Events provide a representation of the messages exchanged between services, while channels provide an abstraction of the mechanism via which the events travel. Events and event channels refine the activity defined at the business layer.

In the proof-of-concept scenario, MFA is used to bolster the security of basic authentication methods like the use of pre-shared secrets in the form of passwords. Additional authentication factors may include a challenge based on something the user has in their possession (a push notification or a time-based token), or on a biometric factor.

A user attempting to log in would trigger an authentication event that is transmitted via a channel. Each component seen in Figure 1 will be examined further in the following subsections.

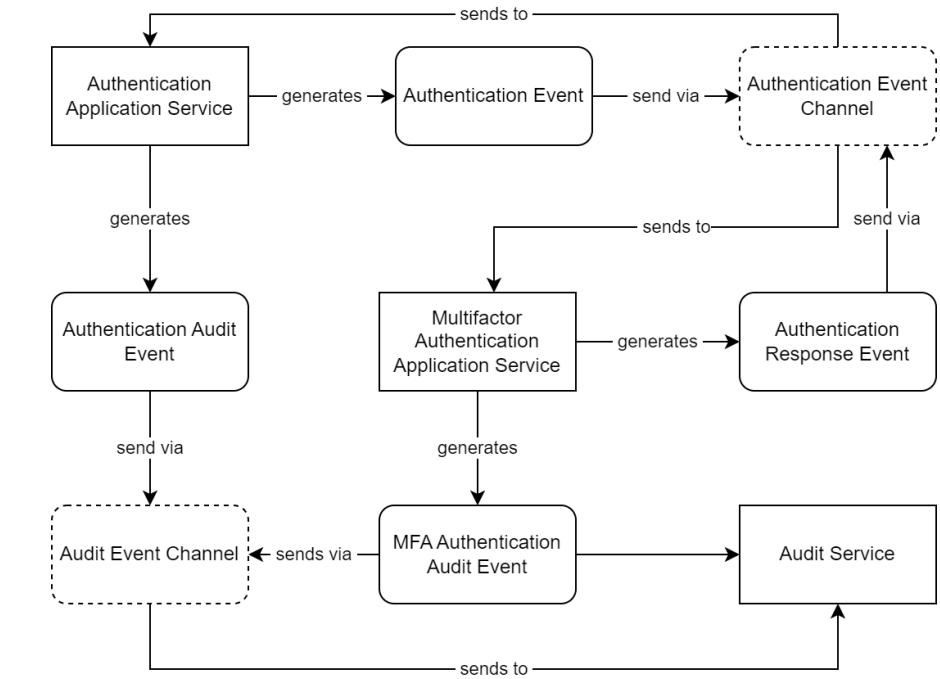

Figure 1: The Application Layer

On initial contact with a principal who wishes to validate their identity, the authentication service makes a determination if the user is attempting to authenticate from a previously known trusted device. If the device is not trusted, the authentication service triggers a secondary event to initiate multifactor authentication. The event is generated and transmitted to the multifactor authentication application service, which will make further attempts to validate the user's identity assertion. After the assertion is validated (or refused), a multifactor authentication response event is generated and transmitted back.

3.5 The Implementation Layer

The *implementation layer* represents how application services are implemented. It describes specific service implementations, interactions with users and other services, and specific technologies that are used to do so. Consequently, the implementation layer maps cleanly to traditional IoCs, such as email addresses, addresses of specific service implementations, or TLS certificates associated with channel implementations. Figure 2 shows that the implementation layer is the most extensive of our layers, since it contains the most granular information.

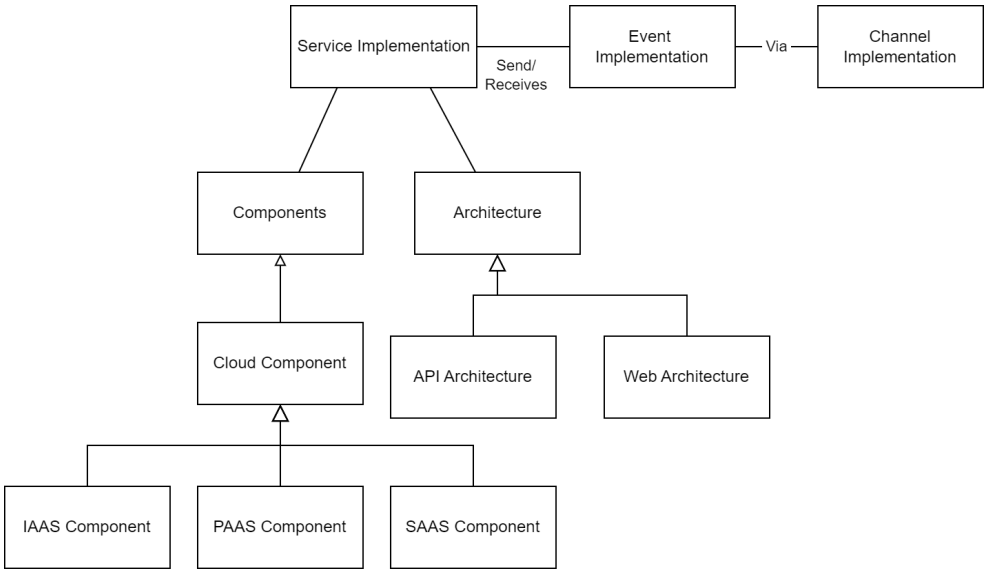

Figure 2: The Implementation Layer

The implementation layer describes specific technologies. The implementation layer intuitively maps to tactical threat intelligence. Traditional threat modeling also takes place at this layer.

At the implementation layer, application services are refined into *service implementations*, event channels into *event channel implementations* and events into event implementations.

A service implementation is an aggregate of a *component* and an *architecture*, which may be further refined. For example, components can be refined into cloud components, which, in turn, may be sub-categorized as infrastructure-as-a-service, platform-as-a-service, or software-as-a-service. Likewise, architectures could consist of stand-alone architectures, web architectures, API architectures, and so on.

While many commercially available authentication services are available in the marketplace or as custom-built solutions, the implementation layer refers to specific technologies.

In the proof-of-concept scenario, we established that (part of) the authentication infrastructure was hosted on-premise. This component was augmented by a commercially available MFA provider that provides push notifications, phone calls, text messaging, or security keys as a secondary factor. The audit service is based on commercially available software hosted on-premise.

We need to stress that these symbols are used here as placeholders to obfuscate details that are potentially security-sensitive. In actual modeling practice, real products, platforms and version numbers will be used. Associated with each platform will be details such as IP addresses, DNS names, and, if desired, any additional data that can be used to support a security team with effectively defending the infrastructure.

For example, we could describe one component as a server running Debian GNU/Linux version 12.7 on IP address 172.16.42.19. Another component could consist of an nginx 1.27.1 server operating on TCP port 443. Since a service implementation is an aggregate of components, these two implementations describe a Linux server running an nginx server. The information contained in the application services provides the context in which the implementation is used, while the business services and activities provide a description of the business value of use of the technology.

Continuing to draw on the scenario, we describe that multifactor authentication events include a username, a client IP address and TCP port, and the IP address and originating port of the server requesting providing basic authentication. This information is transmitted as a call to a RESTful API provided by the audit service implementation, traveling via a TLS 1.3 channel to the service's service IP address. The TLS channel information includes data concerning the X509 certificates used, such as supported and preferred cipher suites and public key materials.

This ability to provide context to a technical infrastructure is one of the strongest benefits of our approach.

4. Discussion

4.1 Applying Threat Intelligence to the Enterprise Security Model

Threat intelligence is often delivered as tactical IoCs. By developing enterprise security models and mapping IoCs to model elements through automation, we improve the ability to triage threat intelligence and improve situational awareness of enterprise defenders.

Operational threat intelligence in the form of TTPs is becoming more common. The organization of individual components and architectures into application-level services enables use of security models to process operational CTI. For example, reports of intercepting authentication challenges to bypass multifactor authentication or a spear-phishing campaign to steal credentials would allow the enterprise to analyze the application layer for potentially impacted services and focus their efforts into the relevant sectors.

Finally, the business layer view enables the organization to analyze strategic-level threat intelligence, review the organization's threat landscape, and direct its risk management activities. The ability to organize the enterprise architecture and map out and components with a security focus allows the organization to process different types of threat intelligence and respond appropriately.

4.2 Updating the Enterprise Security Model

The layered approach to enterprise security modeling presented here can also be updated and maintained layer-by-layer to accurately reflect the actual deployment of the enterprise architecture. By organizing the

enterprise according to business services and down to the related applications and implementation, the model can be viewed at the appropriate level.

The enterprise security model only needs to be updated according to the requisite level of detail. If an organization decides to change how MFA is implemented—for example, changing the SaaS MFA provider—only the *implementation layer* view of the MFA service needs to be updated. If an organization decides on a different approach for a service, the relevant *application layer* view of the application service will be reviewed, along with the related *implementation layer* components. A broader review or update of the model can be broken down by the business-level goals of the organization, with the *business layer* view providing an organizing framework to review and update the model.

Once the interrelations between modeling primitives across the layers are established, it is even possible to automate the update of the different views. This can help ameliorate some of the common challenges to security modeling at the enterprise level.

5. Conclusions and Future Work

Our research is driven by the recognition that effective cyber-defense requires a well-developed situational awareness that spans the full enterprise. Given the complexity of current enterprise architectures, and given the rapidly changing threat landscape, automation must support human analysts in developing and maintaining such awareness.

While threat modeling techniques have been developed to understand threats to software or to business processes, very little work has been done in using threat models to capture the threats to an entire enterprise.

We propose an approach in which human analysts are supported by technology to develop and maintain service-oriented models that describe the enterprise. These enterprise security models are subsequently combined with threat intelligence data to triage threats and to enhance situational awareness.

We investigated the hypothesis that a multi-layered service-based approach to creating such enterprise security models is an effective way to capturing the relevant aspects of a security architecture. A proof-of-concept scenario indicates that a service-based modeling approach consisting of an implementation layer, an application layer, and a business layer is an effective approach to capturing cybersecurity-relevant data concerning enterprise information systems architecture.

By choosing the abstraction layers as described in this paper, we are able to closely align these models with cyber threat intelligence at three commonly distinguished levels: strategic threat intelligence, operational threat intelligence, and tactical threat intelligence.

By doing so, we gain several benefits:

- By mapping static indicators of compromise to model elements described at the implementation layer, we can fully appreciate the value of these indicators in the context of the applications they support and the business functions they enable. This leads to improved situational awareness.
- By separating the enterprise security model from the threat intelligence, we maintain them independently, facilitating improved maintenance and enabling automated support.
- The layered approach allows the enterprise security model to be analyzed and updated at the appropriate level of detail.
- The process of intentionally and carefully mapping out the security-relevant aspects of an enterprise architecture facilitates close alignment of security goals and business goals.

AI Declaration: The authors affirm that artificial intelligence tools were not used in the creation of this paper.

Ethics Declaration: The authors affirm that ethical clearance was not required for this research.

References

Amato, G. et al. (2020) A service architecture for an enhanced Cyber Threat Intelligence capability and its value for the cyber resilience of Financial Market Infrastructures, Bank of Italy, Rome.

Bokan, B.S. and Santos, J.R. (2024) “Threat Modeling for Optimal Enterprise Protections Against Known Cybersecurity Threats”, in ASEE Mid-Atlantic Section Spring Conference.

Borum, R. et al. (2015) “Strategic cyber intelligence”, Information and Computer Security, 23(3), pp 317–332.

Bromander, S. et al. (2021) “Investigating Sharing of Cyber Threat Intelligence and Proposing A New Data Model for Enabling Automation in Knowledge Representation and Exchange”, Digital Threats, 3(1). Available at: https://doi.org/10.1145/3458027.

Burkett, J.S. (2012) “Business Security Architecture: Weaving Information Security into Your Organization’s Enterprise Architecture through SABSA®”, Information Security Journal: A Global Perspective, 21(1), pp 47–54. Available at: https://doi.org/10.1080/19393555.2011.629341.

Dumitriu, D. and Popescu, M. (2020) “Enterprise Architecture Framework Design in IT Management”, Procedia Manufacturing, 46, pp 932–940. Available at: https://doi.org/10.1016/j.promfg.2020.05.011.

Ellerhold, C., Schnagl, J. and Schreck, T. (2023) “Enterprise Cyber Threat Modeling and Simulation of Loss Events for Cyber Risk Quantification”, in Proceedings of the 2023 on Cloud Computing Security Workshop, New York, NY, USA: Association for Computing Machinery (CCSW ’23), pp 17–29. Available at: https://doi.org/10.1145/3605763.3625244.

Gao, P. et al. (2021) “Enabling Efficient Cyber Threat Hunting with Cyber Threat Intelligence”, in IEEE 37th International Conference on Data Engineering (ICDE), pp 193–204. Available at: https://doi.org/10.1109/ICDE51399.2021.00024.

Gerber, A. et al. (2020) “The Zachman Framework for Enterprise Architecture: An Explanatory IS Theory”, in Responsible Design, Implementation and Use of Information and Communication Technology, pp 383–396. Available at: https://doi.org/10.1007/978-3-030-44999-5_32.

Grandry, E., Feltus, C. and Dubois, E. (2013) “Conceptual Integration of Enterprise Architecture Management and Security Risk Management”, in 2013 17th IEEE International Enterprise Distributed Object Computing Conference Workshops, pp 114–123. Available at: https://doi.org/10.1109/EDOCW.2013.19.

Grov, G., Mancini, F. and Mestl, E. (2019) “Challenges for Risk and Security Modelling in Enterprise Architecture”, in 12th IFIP Working Conference on The Practice of Enterprise Modeling (PoEM), Luxembourg, Luxembourg: Springer International Publishing (The Practice of Enterprise Modeling), pp 215–225. Available at: https://doi.org/10.1007/978-3-030-35151-9_14.

Husák, M. et al. (2022) “CRUSOE: A toolset for cyber situational awareness and decision support in incident handling”, Computers & Security, 115, p 102609. Available at: https://doi.org/10.1016/j.cose.2022.102609.

Intelligence and National Security Alliance Task Force (2013) Operational Levels of Cyber Intelligence, Available at: https://www.nist.gov/system/files/documents/2017/06/08/20131213_charles_alsup_insa_part3.pdf.

Jamil, A.-M. et al. (2021) “Towards Automated Threat Modeling of Cyber-Physical Systems”, in 2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM), pp 614–619.

Janulevičius, J. et al. (2017) “Enterprise architecture modeling based on cloud computing security ontology as a reference model”, in 2017 Open Conference of Electrical, Electronic and Information Sciences (eStream), pp 1–6. Available at: https://doi.org/10.1109/eStream.2017.7950320.

Jiang, Y. et al. (2024) “Enterprise architecture modeling for cybersecurity analysis in critical infrastructures - A systematic literature review”, International Journal of Critical Infrastructure Protection, 46, p 100700. Available at: https://doi.org/10.1016/j.ijcip.2024.100700.

Johnson, C. et al. (2016) Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150, NIST.

Kaiser, F., et al. (2022) “Cyber threat intelligence enabled automated attack incident response”, in 2022 3rd International Conference on Next Generation Computing Applications (NextComp), pp 1–6.

Kaiser, F. et al. (2023) “Attack Hypotheses Generation Based on Threat Intelligence Knowledge Graph”, IEEE Transactions on Dependable and Secure Computing, pp 4793–4809. Available at: https://doi.org/10.1109/TDSC.2022.3233703.

Kang, D. et al. (2010) “An ontology-based Enterprise Architecture”, Expert Systems with Applications, 37(2), pp 1456–1464. Available at: https://doi.org/10.1016/j.eswa.2009.06.073.

Karuna, P. et al. (2021) “Automating Cyber Threat Hunting Using NLP, Automated Query Generation, and Genetic Perturbation”, [online], ArXiv, Available at: https://api.semanticscholar.org/CorpusID:233388123 (Accessed 9 July 2024).

Komárková, J. et al. (2018) “CRUSOE: Data Model for Cyber Situational Awareness”, in ARES2018: International Conference on Availability, Reliability and Security, pp 1–10. Available at: https://doi.org/10.1145/3230833.3232798.

van Landuyt, D. et al. (2021) “Threat modeling at run time: the case for reflective and adaptive threat management (NIER track)”, in 2021 International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS), pp 203–209. Available at: https://doi.org/10.1109/SEAMS51251.2021.00034.

Leite, C. et al. (2023) “Automated Cyber Threat Intelligence Generation on Multi-Host Network Incidents”, in 2023 IEEE International Conference on Big Data, pp 2999–3008. Available at: https://doi.org/10.1109/BigData59044.2023.10386324.

Leune, K. and Kim, S. (2021) “Supporting Cyber Threat Analysis with Service-Oriented Enterprise Modeling’, in Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT 2021), pp 385–394.

Li, Z.-X. et al. (2023) “K-CTIAA: automatic analysis of cyber threat intelligence based on a knowledge graph”, Symmetry, 15(2), p 337.

Loft, P. et al. (2022) “CAESAR8: An agile enterprise architecture approach to managing information security risks”, Computers & Security, 122, p 102877. Available at: https://doi.org/10.1016/j.cose.2022.102877.

Martins, G. et al. (2015) “Towards a systematic threat modeling approach for cyber-physical systems”, in 2015 Resilience Week (RWS), pp 1–6. Available at: https://doi.org/10.1109/RWEEK.2015.7287428.

McClintock, M. et al. (2020) “Enterprise Security Architecture: Mythology or Methodology?”, in Proceedings of the 22nd International Conference on Enterprise Information Systems (ICEIS 2020), pp 679–689. Available at: https://doi.org/10.5220/0009404406790689.

Messe, N. et al. (2020) “Asset-Oriented Threat Modeling”, in 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp 491–501. Available at: https://doi.org/10.1109/TrustCom50675.2020.00073.

Nespoli, P. et al. (2017) “Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks”, IEEE Communications Surveys & Tutorials, 20(2), pp 1361–1396.

Pleinevaux, P. (2016) “Towards a Metamodel for SABSA Conceptual Architecture Descriptions”, in 2016 11th International Conference on Availability, Reliability and Security (ARES), pp 187–194. Available at: https://doi.org/10.1109/ARES.2016.87.

Rohloff, M. (2005) “Enterprise Architecture - Framework and Methodology for the Design of Architectures in the Large.”, in Proceedings of the 13th European Conference on Information Systems, Information Systems in a Rapidly Changing Economy, ECIS 2005, pp 1659–1672.

Shi, Z. et al. (2022) “Threat Modeling Tools: A Taxonomy”, IEEE Security & Privacy, 20, pp 29–39.

TOGAF (n.d.) The TOGAF® Standard, 10th Edition. The Open Group, [online], Available at: https://www.opengroup.org/togaf (Accessed: 9 July 2024).

Välja, M. et al. (2020) “Automating threat modeling using an ontology framework”, Cybersecurity, 3(19).

Xu, D. et al. (2012) “Automated Security Test Generation with Format Threat Models”, IEEE Transactions on Dependable and Secure Computing, 9(4), pp 525–539.

Zachman, J. (1987) “Zachman, J.: A Framework for Information Systems Architecture”, IBM Systems Journal, 38, pp 276–292. Available at: https://doi.org/10.1147/sj.263.0276.