

**The value proposition when shifting cyber security technologies from on-prem to the cloud or a hybrid cloud: Case study of active defense cyber security**

**PhD Coordinator: Prof. Adriana Zait**

**Submitted By: Guy Waizel**

**Preliminary research proposal for the degree of**

**Doctor of Philosophy (PhD) in** [**Economics and Business Administration**](http://doctorat.feaa.uaic.ro/international)

**At the University of UAIC**

**March -2022**

Contents

[Short Bio 3](#_Toc100519597)

[Introduction 4](#_Toc100519598)

[Research Motivation 7](#_Toc100519599)

[Literature review 9](#_Toc100519600)

[Primary Research Question (PRQ) 13](#_Toc100519601)

[Secondary Research Questions (SRQ) 13](#_Toc100519602)

[Methodology 14](#_Toc100519603)

[Problem Statement and Importance of the Research 16](#_Toc100519604)

[Access to Data 18](#_Toc100519605)

[Preliminary References 19](#_Toc100519606)

[Papers written by the candidate Guy Waizel 26](#_Toc100519607)

**Research disciplines**: organizational change, business management, value proposition, ROI, Cyber Security budget management, cloud security, cloud computing, active cyber defense, information security, backup contingency plan, disaster recovery plan, deception technology, honeypots, cyber risk management

# Short Bio

Guy Waizel has 25 years of operations experience. Today he fulfills the role of Director of Business Operations and Israel Site Operations at Metallic Security Services, a Commvault company. Before that, he worked at TrapX Security as the COO of the company. He led all TrapX Security Operations departments, including R&D, Product, H.R., I.T. Support, TAM, and Operations. Before joining TrapX in 2014, Guy was the Professional Services and Support Manager at Synerion Systems, a global leader in H.R. He established and managed a global multidisciplinary support organization at AeroScout, a Stanley Healthcare company. Guy also created and managed the 3rd tier support center for the EMEA and APAC regions at Blue Pumpkin Software – a Verint company. Earlier career experience includes serving as CIO & CSO for SecuTech, a global healthcare solutions company. Guy holds an MBA from Netanya Academic College Israel (2007) and a B.Sc in Technology Management from the Holon Institute of Technology in Israel (2002). He has also completed technical certifications in Cybersecurity, penetration testing, ethical hacking, reverse engineering & exploit development.

Guy is a Cyber security expert in Cyber deception technology. Over the last 8 years, Guy has been providing training and lectures to Fortune 500 customers, leading enterprise organizations, governments, financial institutions, and cyber experts from all business sectors around the globe, training their security operations teams and cyber security leaders about Deception technology and cyber active defense strategy, mentoring organizations to defend against the most challenging and sophisticated cyber-attacks.

Guy created many publications, which are available on the TrapX Security website: https://www.trapx.com/blog/

# Introduction

Over the last decade, organizations have started moving some of their business applications from on-premises to the cloud. Boillat and Legner pointed out the impact of cloud computing on enterprise software vendors’ business models when moving from on-premises software to cloud services (Boillat & Legner, 2013). Many software enterprise vendors identified the opportunity to reduce costs (Walther et al., 2012) for existing or new customers by working in SAAS mode and started developing SAAS and hybrid cloud applications mainly in the fields of CRM, ERP, HCM, time and attendance, HR, recruitment, marketing, R&D, QA, DevOps, finance, BI, IT, and other business-related areas. For example, Elmonem et al. (2021) researched how prioritizing organizational factors impact cloud ERP adoption and the critical issues related to security, usability, and vendors, and Gai (2014) researched how to leverage private cloud computing in financial services. One of the main areas of concern for organizations before deciding to move to the cloud has always been the security concern (Dimitrakos, 2014). Many cybersecurity frameworks, certifications, and methodologies exist to assist vendors in developing their solutions securely in an SAAS model.

Such frameworks and certifications significantly increase organizations’ confidence to shift their data to the cloud. For example, ISO 27001 (Disterer, 2013), SOC2, OWASP, CSA STAR, ISO 22301, NIST, and others are mentioned in the literature review section. During the last few years, more security software enterprise vendors have decided that it is time to shift some of their solutions to the cloud in a hybrid model or a native SAAS mode, extending their offering to their customers. Some new security vendors even create solutions just for the cloud or SAAS environment. Rane researched a cloud security perspective for application providers in 2010 (Rane, 2010).

Enterprise security vendors who sell software solutions are now at a stage with their existing customers where the solution is on-premises. In some situations, they require their client to move the central management of the system to the cloud, which is not an easy task. Some of the security community is very conservative and accustomed to traditional security, which has always been based on-premises. Behl pointed out some emerging security challenges in cloud computing in 2011 (Behl, 2011). In addition, many security vendors operate their solutions exclusively on-site, so integration with such security tools would not be feasible in some circumstances in the cloud.

In most cases, organizations can quickly customize on-premises solutions to meet their needs using professional services. SAAS or hybrid cloud solutions should be simple and fit SMB and mid-market customers. There are some limitations for large enterprise markets adapting SAAS solutions. Tawfique and Vejseli researched the decision to migrate to the cloud, focusing on the security aspects from the consumer perspective (Tawfique & Vejseli, 2018). Because of the additional risk of moving business applications and security to the cloud, some organizations hesitate and prefer to keep their existing security tools on-site.

Enterprise security software vendors should prepare a detailed value proposition plan that can assist in convincing and conveying the right message. Many security vendors have already started adjusting their features to cloud computing. Rajesh described how Fortinet tightens its partnership with Google Cloud to provide advanced cloud security and accelerate the cloud on-ramp (Rajesh Maurya, 2019), and IBM has utilized open technology to speed up response to cyber threats across cloud networks (Computer, E. 2019).

When preparing a value proposition plan, we need to answer questions such as: What value do we deliver to the customer? Which of our customers’ problems are we helping to solve? What bundles of products and services are we offering to each customer segment? Which customer needs are we satisfying? (Boillat & Legner, 2013).

This research focuses on active cyber defense technology, specifically deception, as a case study. With this research, we construct a detailed value proposition plan for potential vendors who wish to transition existing customers who initially deployed the solution on-premises and who now wish to move their customers to a hybrid or native cloud environment.

Organizations who deploy active cyber defense technology on-premises get value from the technology including ease of deployment, reducing the organization’s risk, getting high fidelity alerts, less IT maintenance, early detection, and many more offerings. Guy Waizel discussed this on the TrapX Security blogs (Waizel, 2021).

Sun Tzu, the military strategist of the sixth century BC, was the first to introduce the deception technique as an active defense strategy to win a war and was the author of the book *The Art of War*, stating that “all warfare is based on deception” (Sun Tzu, Capstone Publishing, 2010). Stevens researched how active cyber defense reduces our exposure to cyber incidents, protects our most precious assets, and allows us to operate successfully and prosperously in cyberspace (Stevens et al., 2019). Ferguson-Walter conducted an empirical assessment of the effectiveness of deception for cyber defense (Ferguson-Walter, 2020) based on the Tularosa study *(*Ferguson-Walter et al., 2018)

As soon as deception technology is deployed as an active defense strategy, we reduce risk by reducing threat event frequency (Jones, 2016). Moreover, with the move to the cloud, there are new opportunities to adjust deception features to the cloud, for example, decoys for Office 365, decoys for SAAS applications such as Salesforce and Microsoft Dynamics, and decoy VPNs for remote workers. In addition, there is an opportunity to increase ROI, reduce the cost of potential loss for customers, and move the infrastructure security responsibility to the vendor, ensuring a high level of service and dramatically reducing downtime due to infrastructure issues. We discuss these issues and more with this research.

# Research Motivation

This research intends to present a value proposition plan and recommendations for enterprise software security vendors who wish to shift their customers from on-premises deployment to a SAAS or hybrid cloud deployment. Such a value proposition plan should include budget, ROI, security, and value-added product features in a cloud environment to convince customers to move to the cloud.

A good example is the case study of active cyber defense technology. Organizations usually deploy such technology products on-premises. Some security vendors wish to move the solution to the cloud and shift their clients’ deployment to hybrid or full SAAS models. With such a deception solution, organizations can reduce their cyber security risks and improve overall security by applying practical active defense strategies and techniques in the cloud, SAAS applications, and local networks.

I have been working with the high-tech industry for 25 years, and for TrapX Security, a world leader in cyber security deception technology, for the last 8 years. Recently TrapX Security was acquired by Metallic, a Commvault venture. Metallic is one of the rapidly growing SAAS companies for cloud backup and data management.

These days we plan the roadmap of our product and plan to make it hybrid cloud and eventually native cloud. One of our challenges is shifting more than 200 customers from on-premises deployment to SAAS or hybrid cloud models. Such a value proposition plan could greatly help my organization and any other organization looking to shift their customers’ deployment from on-premises to hybrid cloud or native SAAS.

Another interesting topic is the value-added combination between active cyber defense solutions, business contingency plans (BCPs), and disaster recovery plans (DRPs), for example, the early detection of the infected endpoint and then rapid restore of the endpoint by a backup and subsequent recovery of the system.

Furthermore, a new cloud attack landscape is here; organizations do not have much time to prepare. Security vendors need to prepare their clients and potential clients for the worst-case scenarios by adjusting their products and technologies to the cloud. Improving organizations’ overall security by managing and reducing cyber threat risks and potential loss becomes a crucial topic now and for the coming years as cybercriminals leverage both the COVID-19 pandemic and the massive increase of new vulnerabilities to carry out their criminal intents.

# Literature review

Current literature on related items to the research topic mainly includes topics that focus on cloud computing in general. Value proposition focuses mainly on general SAAS models and not specifically on cyber security vendors. For example, these researches:

* Research about the impact of vendors' business models when moving from on-premise to the cloud (Boillat and Legner, 2013).

In this research Boillat and Legner, analyzed four cloud offerings in ERP and CRM and two of their on-premise counterparts. Using the business model canvas of Osterwalder and Pigneur (Osterwalder and Pigneur, 2010) .They derive two distinct business model configurations – SaaS and SaaS+PaaS (Platform-as-a-Service).

Their study reveals that the move from on-premise software to cloud services impacts all nine business model elements and synthesizes the specificities of enterprise software vendors' business models. They complement Osterwalder and Pigneur's business model canvas which analyzes 9 business models: Customer segment, Customer relationships AppExchange, Channels, Value proposition, Revenue streams, Key Resources, Key Activities, Key Partners, and Cost Structure. They found that software vendors provide a development platform (PaaS) to compensate for the lack of in-depth customization resulting from the multitenant model. PaaS platform allows developers to develop and deploy add-ons through online stores and address two customer segments – users and developers – with different value propositions. The analysis of Boillat et al. does not cover enterprise security vendors. It doesn't refer to value proposition and success factors that can be achieved when moving enterprise security vendors to SAAS or hybrid cloud. Also, it doesn't discuss PAAS options for the enterprise cyber security market. Moreover, the research doesn't discuss situations wherein some conditions; a hybrid cloud is a must need as a crucial component of their product reside still on-prem, for example, agents installed on endpoints or related requirements with local network segmentations.

* Research about success factors and value propositions of software as a service provider (Walther et al., 2012).

In this research, the authors based on an abstraction of several papers, discussed success factors that were aggregated into 13 different factors: performance, security, individualization, privacy, availability, compliance, flexibility, interoperability, ease of implementation, legal policies, charging, alternative costs of in-house IT systems and social aspects. These success factors were counted by the number of articles they were mentioned in, and they checked which Success factors were highly discussed and which factors were not.

They also aggregated the value propositions into 19 different propositions: cost savings, financing, concentration on core competencies, functionality, cost flexibility, installation, planning, strategic flexibility, innovation ability, helpdesk quality, ease of use, availability, mobility, data security, higher investment security, replacement of old infrastructure, energy savings and accounting benefits

They found that the essential value proposition of SaaS is cost saving. This is congruent with understanding a context activity, where the highest benefits for the company concerning a context activity can be gained by reducing costs. The value proposition "concentration on core competencies" further highlights the role of SaaS as a context activity.

Enterprise security vendors are not discussed in this research. Also, this market's value proposition and success factors are not mentioned. Many of the security vendors have crucial components of their systems on-prem; thus, a possible stage one solution for them could be to move to a hybrid cloud solution, but this is not discussed in this research.

* Research about South African Vendors' cloud computing value proposition to small, medium, and micro enterprises (Gumbi et al., 2015).

In this research, Gumbi et al. analyzed the main concerns in Adopting Cloud Computing, Concerns as Recovery of Data, Connectivity Issues, Data Privacy and Security, Application Performance, Integration Issues with other Applications, Complex Pricing/Charging Models, Lock-in Terms and Contracts, Poor Service Level Agreements, Customization of the Product, Unclear Scheme in Pay Per Use Model.

They conclude that Cloud computing is changing the entire ICT environment. It presents opportunities for SMMEs to reduce their ICT infrastructure costs by adopting high-end information and communication systems.

They also conclude that the value proposition of cloud computing as offered not only by cloud services vendors but also by industry experts, consultants, and researchers is not clearly or adequately perceived by SMMEs in South Africa.

The research focuses more on African SMMEs, and also, this research doesn't focus on enterprise security vendors and options for them to move to the cloud or hybrid cloud model.

Further research found in relation to this proposal includes:

* Value propositions and current performance in leveraging private cloud computing in financial services (Gai, 2014)
* Research on cloud security challenges and guidelines (Dimitrakos, 2014)
* Research on cloud security for SMBs (Scott, 2010)
* Research on cloud SAAS security issues and challenges (Fehér & Sándor, 2019)
* Research on new trust models for cloud security (Sato et al., 2010)
* Offerings of on-premises security vendors of new cloud features to protect against cloud threats (Computer, E. 2019; Fortinet, 2019; TrapX Security, 2021) support for containers
* Cyber security risk management methods, and active defense and attack scenarios are covered very well, and there are many literature discussions about these, for example, ISO/IEC 27000 and ISO/IEC 27001 (Disterer, 2013; Heron, 2019), NIST (NIST, 2018; Saleh, Refai & Mashhour, 2011; Shen, 2014), COBIT (Garsoux, 2013), CIS controls (formerly known as critical security controls) (Laing, 2012), NERC CIP (Newburn, 2015; Laing, 2012; Peacock, 2020), FAIR (Freund & Jones, 2015), MITRE ATT&CK and MITRE D3FEND (Barnum, 2012; Pennington, 2019), and HITRUST CSF (Pandey & Sharma, 2017).

**Gaps identified in knowledge and literature:**

Little or no literature about the value proposition when shifting customers from on-premises to SAAS or hybrid cloud for security enterprise vendors, and specifically for active cyber defense technology, could be found.

The literature on cloud security lacks information about offering action plans for existing customers running on-premises solutions and planning to move to the cloud.

The literature lacks information about value proposition plans and opportunities for security vendors to secure the cloud better with their move to the cloud, for example, by securing cloud assets with the solution.

The literature does not discuss the challenges of integrating ecosystem on-premises security systems with cloud or hybrid cloud environments.

Research about active defense and honeypots exists but mainly covers academic research and does not provide explicit business best practices for reducing risk as to the value offered compared to the potential loss risk.

There is a lack of relevant literature about deception security deployment in native or hybrid cloud environments.

# Primary Research Question (PRQ)

PRQ: What components and considerations may comprise a value proposition plan for security software vendors offering their customers to move from traditional classical on-prem security solutions to the cloud or a hybrid cloud as a case study of active defense technology?

# Secondary Research Questions (SRQ)

SRQ1: How can organizations reduce APT (Advanced Persistent Threats), ransomware, supply chain risks, and other cyber threats?

SRQ2: How can organizations improve their overall DRP (Disaster Recovery Plan) and BCP (Business Continuity Plan) by utilizing cyber security active defense on cloud or hybrid cloud technology for early threats detection and cloud backup solutions for immediate remediation?

SRQ3: How are I.T. organizations' budgets and ROI affected by moving traditional and advanced on-prem security tools to the cloud?

# Methodology

The research method combines a mix of qualitative and quantitative research methods

We start with semi-structured qualitative research with Security leaders, questions related to SRQ1, SRQ2, and SRQ3, then deduce from that the top main questions for the closed-ended questionnaire for a sample side of 200 to answer the PRQ and then validate the results over a Delphi focused group discussion.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Method | Objective | Research Question | Research tool | Sample Size | Data Analysis method |
| Qualitative research | 1. To examine how customers can reduce APT & ransomware threat risks by deploying a deception solution in a hybrid cloud model or native cloud environment  2. How can organizations improve their DRP (Disaster Recovery Plan) and BCP (Business Continuity Plan) by utilizing cyber security active defense on cloud or hybrid cloud technology for early threats detection and cloud backup solutions for immediate remediation?  3. To examine how I.T. organizations' budgets and ROI are affected by moving traditional and advanced on-prem security tools to the cloud? | SRQ1  SRQ2  SRQ3 | Semi-structured Interviews | 15 cyber security managers: I.T., Security specialist, SOC Analysts & CISO | Content analysis |
| Quantitative Analysis | To examine if the target sample group were convinced by the value proposition plan to move to a hybrid cloud or native SAAS | PRQ | Closed-ended questionnaire based on the qualitative part | 200 participants | SPSS for data analysis  Survey monkey for creating and distributing an electronic survey  Consider using social networks or one of the online survey participants' tools such as:  positely.com  cloud research  respondent.io  poll-pool.com |
| Qualitative | To examine What components and considerations may comprise a value proposition plan for security software vendors offering their customers to move from traditional classical on-prem security solutions to the cloud or a hybrid cloud | PRQ | A delphi focus group discussion | 8  Cyber security\IT managers | Content analysis |

# Problem Statement and Importance of the Research

Many enterprise security vendors initially developed their solutions for the on-premises environment. Some are network-based solutions that rely on local networking requirements, with security mainly for endpoints, and vendors did not design them to operate in cloud or hybrid cloud environments.

With more organizations moving their business applications to the cloud, there is an opportunity to better secure the cloud applications. Enterprise security vendors should adopt new approaches to their solutions to adjust them to the new reality. Many are developing additional functionality and features for hybrid cloud and SAAS to support the rapid change and need for such adaptation.

One of the main questions between various enterprise security vendors is what to do with existing customers who have worked on a legacy on-premises solution for a few years and are who are now being asked to move to a hybrid cloud model or a SAAS environment. That is not an easy task. Some of these organizations are government facilities, financial institutions, and other organizations with very conservative mindsets who wish to keep most of their security solutions on-site. This is mainly for security reasons and ecosystem integration with another on-premises environment.

Another important aspect of this research is finding a way for enterprise security vendors to educate their existing customers about ROI and IT budget improvement due to moving from on-premises deployment to a hybrid cloud or native cloud solution. Specifically, the case study of a deception security solution emphasizes the added value ROI in favor of the potential loss risk.

To support this rapid change, this research seeks to establish a detailed value proposition plan to effectively share with the enterprise security community how to convince their customers to move to a hybrid cloud or SAAS environment. Success is essential both on the business and technical side. With this transition, vendors are also providing new adjusted added value for their customers.

A good case study for moving from an on-premises solution to a hybrid cloud or SAAS solution is active defense security technology, such as deception technology. In many cases, organizations deploy such solutions on-premises to cover their network segmentation. However, with changes over recent years, enterprise security vendors have decided to move their customers from an on-premises environment to a hybrid cloud or fully SAAS environment.

Reducing costs is not the only offering for such customers. For example, there are new ways to protect themselves in the cloud to reduce risks by deploying more cloud decoys and many other offerings. For example, TrapX Security recently developed more cloud functionality and support for container decoys. This was the first step in adding more value for their customers in the cloud (TrapX Security 2021; TrapX extends attack surface coverage to containers with DeceptionGrid 7.2, PRNewswire, viewed January 16 2022, <https://www.prnewswire.com/news-releases/trapx-extends-attack-surface-coverage-to-containers-with-deceptiongrid-7-2--301342840.html>).

For many years, my experience as a cyber security leader and in managing daily business operations has taught me that cybercriminals do not rest for a moment in today’s world. We constantly hear about significant cyber-attacks on businesses and governmental facilities, ransomware attacks, and APT and supply chain attacks.

A strong value proposition plan can benefit security vendors greatly. In addition, security experts at all levels, CSOs, CISOs, IT managers, SOC analysts, security consultants, and security operation teams in small, medium, and large organizations can benefit from such a shift to a hybrid cloud or native SAAS solution to address cyber security risks better and remediate threats accordingly.

# Access to Data

As part of my role as a CyberSecurity leader, I currently work closely with partners and customers in the field of Cyber Security. I firmly believe this fact can assist me in collecting valuable data from the field.

As part of my new role as Director of Business Operations at one of the fastest-growing SAAS backup and data management companies, I am involved with the business processes and roadmap plans to shift existing TrapX customers to hybrid cloud and, in the future, to a native SAAS cloud environment.

The following are examples of some online research databases that I plan to use in this research:

<https://scholar.google.com>

<https://www.openathens.net>

[CORE – Aggregating the world's open access research papers](https://core.ac.uk/)

[ScienceOpen](https://www.scienceopen.com/)

[arXiv.org e-Print archive](https://arxiv.org/)<https://www.base-search.net/>

<https://ethos.bl.uk/>

# Preliminary References

Assante MJ, Lee RM (2015) The Industrial Control System Cyber Kill Chain. Available at <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-systemcyber-kill-chain-3629>

Bodeau D, Graubart R (2011) Cyber Resiliency Engineering Framework, Version 1.0. <https://www.mitre.org/sites/default/files/pdf/11_4436.pd>

Bodeau D, Graubart R (2016) Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Preparedness. (The MITRE Corporation, Bedford, MA), MITRE Technical Report MTR-150264.Available at [https://www.mitre.org/sites/default/files/publications/15-0797-cyber-prep-2- motivating-organizational-cyber-strategies.pd](https://www.mitre.org/sites/default/files/publications/15-0797-cyber-prep-2-%20motivating-organizational-cyber-strategies.pd)

Bodeau D, Graubart R (2016) Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Preparedness. (The MITRE Corporation, Bedford, MA), MITRE Technical Report MTR-150264. Available at [https://www.mitre.org/sites/default/files/publications/15-0797-cyber-prep-2- motivating-organizational-cyber-strategies.pd](https://www.mitre.org/sites/default/files/publications/15-0797-cyber-prep-2-%20motivating-organizational-cyber-strategies.pd)

Bodeau D, Graubart R (2017) Cyber Resiliency Design Principles: Selective Use Throughout the Life Cycle and in Conjunction with Related Disciplines. (The MITRE Corporation, Bedford, MA), MITRE Technical Report MTR170001. Available at <https://www.mitre.org/sites/default/files/publications/PR%20170103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf>

Bodeau D, Graubart R, Heinbockel W, Laderman E (2015) Cyber Resiliency Engineering Aid – The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques. (The MITRE Corporation, Bedford, MA), MITRE Technical Report MTR-140499R1. Available at <http://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliencyengineering-aid-framework-update.pdf>

Bodeau D, Graubart R, McQuaid R, Woodill J (2018) Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods. (The MITRE Corporation, Bedford, MA), MITRE Technical Report MTR-180314. Available at <https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyberresiliency-metrics-measures-of-effectiveness-and-scoring.pdf>

Boillat, T., & Legner, C. (2013). From on-premise software to cloud services: THE IMPACT OF CLOUD computing on enterprise software vendors' business models. Journal of Theoretical and Applied Electronic Commerce Research, 8(3), 7–8. https://doi.org/10.4067/s0718-18762013000300004

Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (S.P.) 800-161. <https://doi.org/10.6028/NIST.SP.800-161>Ross RS, Dempsey KL, Viscuso P, Riddle M, Guissanie G (2016) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (S.P.) 800-171, Rev. 1, Includes updates as of June 7, 2018. <https://doi.org/10.6028/NIST.SP.800-171r1>

Chandramouli R (2016) Secure Virtual Network Configuration for Virtual Machine (V.M.) Protection. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (S.P.) 800-125B. <https://doi.org/10.6028/NIST.SP.800-125B>

Dewar, R.S., 'The "triptych of cyber security": a classification of active cyber defense,' in P. Brangetto, M. Maybaum and J. Stinissen (eds.), 2014 6th International Conference on Cyber Conflict: Proceedings, Tallinn, NATO CCD COE Publications, 2014, pp. 7-21.

Dimitrakos, T., 2014, August. Cloud Security Challenges and Guidelines. In EIT ICT Labs Symposium on Trusted Cloud and Future Enterprises.

Disterer, G. ISO/IEC 27000, 27001 and 27002 for information security management". 2013.

Fagan M, Megas KN, Scarfone KA, Smith M (2019) Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (I.R.) 8259. <https://doi.org/10.6028/NIST.IR.8259-draf>

Ferguson-Walter, K., Shade, T., Rogers, A., Trumbo, M.C.S., Nauer, K.S., Divis, K.M., Jones, A., Combs, A. and Abbott, R.G., 2018. *The Tularosa Study: An Experimental Design and Implementation to Quantify the Effectiveness of Cyber Deception* (No. SAND2018-5870C). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

Ferguson-Walter, K.J., 2020. An empirical assessment of the effectiveness of deception for cyber defense.

Gai, K., 2014. A review of leveraging private cloud computing in financial service institutions: Value propositions and current performances. Int. J. Comput. Appl., 95(3), pp.40-44.

Gumbi, L.N. and Mnkandla, E., 2015. Investigating South African Vendors' cloud computing value proposition to small, medium and micro enterprises: a case of the City of Tshwane Metropolitan Municipality. The African Journal of Information Systems, 7(4), p.1.

H.M. Government, National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom, Cm 9161, London, The Stationery Office, November 2015. https://www.gov.uk/government/publications/ national-security-strategy-and-strategic-defence-and-security-review-2015

International Organization for Standardization (ISO) Guide 73:2009, Risk management – Vocabulary, November 2009. <https://www.iso.org/standard/44651.html>

Jasper, S., Strategic Cyber Deterrence: The Active Cyber Defense Option, Lanham, MD, Rowman, and Littlefield, 2017

Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (S.P.) 800-37 Rev. 2. <https://doi.org/10.6028/NIST.SP.800-37r2>

Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD). NIST Special Publication (S.P.) 800-39. <https://doi.org/10.6028/NIST.SP.800-39>

Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (S.P.) 800-53, Rev. 4, Includes updates as of January 22, 2015. <https://doi.org/10.6028/NIST.SP.800-53r4>

Laing, C. ed., Securing critical infrastructures and critical control systems: Approaches for threat protection: Approaches for threat protection"IGI Global, 2012. Bodeau DJ, McCollum CD, Fox DB (2018) Cyber Threat Modeling: Survey, Assessment, and Representative Framework. (The MITRE Corporation, McLean, VA), PR 18-1174. Available at <https://www.mitre.org/sites/default/files/publications/pr_18-1174-ngci-cyberthreat-modeling.pdf>

Levy, I., Active Cyber Defence – One Year On, London, National Cyber Security Centre, February 5 2018. https://www.ncsc.gov.uk/information/active-cyberdefence-one

Levy, I., 'Active Cyber Defence – tackling cyber attacks on the U.K.,' blog post, November 1 2016. https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tacklingcyber-attacks-uk

Muñoz-González, L. and E.C. Lupu, ‘The secret of machine learning’, April 2018. <https://www.bcs.org/content/conWebDoc/59383>

National Audit Office, Cyber Security, and Information Risk Guidance for Audit Committees, September 2017. https://www.nao.org.uk/report/cyber-security-andinformation-risk-guidance/

National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. <https://doi.org/10.6028/NIST.FIPS.199>

National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). <https://doi.org/10.6028/NIST.CSWP.04162018>

National Institute of Standards and Technology (2019) NIST Privacy Risk Assessment Methodology (PRAM). (National Institute of Standards and Technology, Gaithersburg, MD). <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources>

National Security Agency (2018) NSA/CSS Technical Cyber Threat Framework v2. (National Security Agency, Fort George G. Meade, MD), National Security Agency Cybersecurity Report. Available at <https://www.nsa.gov/Portals/70/documents/what-wedo/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threatframework.pdf>

Newburn, B.C., """""Implementing national electrical reliability corporation/critical infrastructure protection standards (NERC/CIP) in the real world utility industry""""", ProQuest Dissertations Publishing, 2015.

Rose S, Borchert O, Mitchell S, Connelly S (2019) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (S.P.) 800-207. <https://doi.org/10.6028/NIST.SP.800-207-draft>

Ross RS, Oren JC, McEvilley M (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (S.P.) 800-160, Vol. 1, Includes updates as of March 21, 2018. <https://doi.org/10.6028/NIST.SP.800-160v1>

Salih, S., Hamdan, M., Abdelmaboud, A., Abdelaziz, A., Abdelsalam, S., Althobaiti, M.M., Cheikhrouhou, O., Hamam, H. & Alotaibi, F. 2021, "Prioritising Organisational Factors Impacting Cloud ERP Adoption and the Critical Issues Related to Security, Usability, and Vendors: A Systematic Literature Review", *Sensors,*vol. 21, no. 24, pp. 8391.

Saunders, J., 'Tackling cybercrime – the U.K. response', Journal of Cyber Policy, 2, 1 (2017), pp. 4-15.

Sexton, M., 'U.K. cybersecurity strategy and active cyber defense – issues and risks,' Journal of Cyber Policy, 1, 2 (2016), pp. 222-242

Singhal A, Winograd T, Scarfone KA (2007) Guide to Secure Web Services. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (S.P.) 800-95. <https://doi.org/10.6028/NIST.SP.800-95>

Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (S.P.) 800-82, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-82r2>

Strom BE, Battaglia JA, Kemmerer MS, Kupersanin W, Miller DP, Wampler C, Whitley SM, Wolf RD (2017) Finding Cyber Threats with ATT&CK-Based Analytics. (The MITRE Corporation, Annapolis Junction, MD), MITRE Technical Report MTR-170202. Available at <https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyberthreats%20with%20att%26ck-based-analytics.pdf>

Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (S.P.) 800-18, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-18r1>

Tawfique, K. and Vejseli, A. (2018) *Decision to migrate to the Cloud : A focus on security from the consumer perspective*, *DIVA*. Available at: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1192599&dswid=5851 (Accessed: 24 March 2022).

The Smart Grid Interoperability Panel—Smart Grid Cybersecurity Committee (2014) Guidelines for Smart Grid Cybersecurity: Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (I.R.) 7628, Rev. 1, Vol. 1. <https://doi.org/10.6028/NIST.IR.7628r1>

Tzu, Sun. The Art of War. Capstone Publishing, 2010

Walther, S., Plank, A., Eymann, T., Singh, N. and Phadke, G., 2012. Success factors and value propositions of software as a service providers–a literature review and classification.

Yeluri, R. and Castro-Leon, E., 2014. Building the Infrastructure for Cloud Security: A Solutions View (p. 244). Springer Nature.

# Papers written by the candidate Guy Waizel

Waizel, G., 2021. Attacks on healthcare organizations: Was the writing on the wall? *TrapX Security*. Available at: https://www.trapx.com/attacks-on-healthcare-organizations-was-the-writing-on-the-wall/ [Accessed April 10, 2022].

Waizel, G., 2021. Deception – a shield between vulnerability disclosure and patch deployment: The case of CVE-2021-22005. *TrapX Security*. Available at: https://www.trapx.com/deception-a-shield-between-vulnerability-disclosure-and-patch-deployment-the-case-of-cve-2021-22005/ [Accessed April 10, 2022].

Waizel, G., 2021. Defending against cisco authentication bypass vulnerability exploits. *TrapX Security*. Available at: https://www.trapx.com/defending-against-cisco-authentication-bypass-vulnerability-exploits/ [Accessed April 10, 2022].

Waizel, G., 2021. Defending crown jewel assets such as Active Directory Domain Controllers from breaches. *TrapX Security*. Available at: https://www.trapx.com/defending-crown-jewel-assets-such-as-active-directory-domain-controllers-from-breaches/ [Accessed April 10, 2022].

Waizel, G., 2021. How trapx can help you defend against RMM Supply Chain attacks like Kaseya. *TrapX Security*. Available at: https://www.trapx.com/how-trapx-can-help-you-defend-against-rmm-supply-chain-attacks-like-kaseya/ [Accessed April 10, 2022].

Waizel, G., 2021. Protecting operational technology environments from today's cyberthreats. *TrapX Security*. Available at: https://www.trapx.com/protecting-operational-technology-environments-from-todays-cyberthreats/ [Accessed April 10, 2022].

Waizel, G., 2021. TrapX DeceptionGrid deceives and traps attackers exploiting latest vulnerabilities. *TrapX Security*. Available at: https://www.trapx.com/trapx-deceptiongrid-deceives-and-traps-attackers-exploiting-latest-vulnerabilities/ [Accessed April 10, 2022].

Waizel, G., 2021. Using DeceptionGrid to detect and defeat exploits of Log4j Remote Code Execution (RCE) vulnerability. *TrapX Security*. Available at: https://www.trapx.com/using-deceptiongrid-to-detect-and-defeat-exploits-of-log4j-remote-code-execution-rce-vulnerability/ [Accessed April 10, 2022].

Waizel, G., 2021. Why Ransomware is a national security crisis – and what to do about it. *TrapX Security*. Available at: https://www.trapx.com/why-ransomware-is-a-national-security-crisis-and-what-to-do-about-it/ [Accessed April 10, 2022].