Defence Research and Development Canada Recherche et développement pour la défense Canada

DRDC | RDDC
technologysciencetechnologie

Machine Learning in Vulnerability Assessment

Delfin Montuno
Solana Networks

Prepared by:
Solan Networks
301 Moodie Drive, Suite 215
Nepean, Ontario Canada
K2H 9C4
PSPC Contract Number: W7714-115274/001/SV
Technical Authority: Adrian Taylor, Defence Scientist
Contractor's date of publication: December 2018

Defence Research and Development Canada

Contract Report
DRDC-RDDC-2019-C067
April 2019

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada using the Schedule to the *Defence Production Act*.

Disclaimer: This document is not published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada but is to be catalogued in the Canadian Defence Information System (CANDIS), the national repository for Defence S&T documents. Her Majesty the Queen in Right of Canada (Department of National Defence) makes no representations or warranties, expressed or implied, of any kind whatsoever, and assumes no liability for the accuracy, reliability, completeness, currency or usefulness of any information, product, process or material included in this document. Nothing in this document should be interpreted as an endorsement for the specific use of any tool, technique or process examined in it. Any reliance on, or use of, any information, product, process or material included in this document is at the sole risk of the person so using it or relying on it. Canada does not assume any liability in respect of any damages or losses arising out of or in connection with the use of, or reliance on, any information, product, process or material included in this document.

Abstract

Machine Learning (ML) is increasingly being applied in vulnerability assessment and more generally in providing cyber security. We review ML applications in both those areas by commercial vendors. We also review recent results in adversarial learning; since ML requires training data to be effective, it is susceptible to adversarial attacks in which that data is poisoned to impair the ML's functionality or allow attackers to bypass it. As a result of this adversarial nature of the problem, we conclude that the automated nature of ML-based solutions increases the need for accurate ground truth input data, and that more research is required to ensure the safety and effectiveness of these approaches with human-machine cooperation in mind.

Résumé

On utilise de plus en plus l'apprentissage machine (AM) en évaluation des vulnérabilités et de façon plus générale en prestation de services de cybersécurité. Nous avons évalué les applications d'AM proposées dans ces deux domaines par des fabricants du secteur privé. Nous nous sommes aussi penchés sur des résultats récents en apprentissage adverse : comme l'AM a besoin de données d'entraînement pour être efficace, il est vulnérable à des attaques adverses par l'empoisonnement de ces données afin d'handicaper l'AM ou de l'aveugler à des attaques hostiles. Vu la nature adverse du problème, nous concluons que le caractère automatisé des solutions fondées sur l'AM rend encore plus vitale la fidélité à la réalité sur le terrain des données avec lesquelles on les alimente, et qu'il faut des recherches plus approfondies pour assurer la sécurité et l'efficacité de ces stratégies, en gardant en tête la coopération humain-machine.

Table of Contents

1. Introduction

In this document, we investigate how Machine Learning (ML) is being applied in vulnerability assessment in particular and in providing cyber security in general. In Section 2, we describe the limited application of ML in vulnerability management solutions and the no mention of ML related applications in vulnerability assessment solutions. There are, however, a number of applied ML based solutions in specific areas of cyber security as described in Section 3. Because ML based solutions in general, including those applied to cyber security, are susceptible to adversarial attacks, Section 4 describes the needs for adversarial machine learning. In Section 5, we describe possible future work and summarize this investigation.

2. Application of Machine Learning in Vulnerability Management Solutions

This section describes the top ranked vulnerability assessment/management solutions with only a few of them claimed to have been using ML-based solutions. Note that each solution is not examined in-depth to completely rule out the absence of embedded ML-based solutions. Also, the broadness of the problem scope may explain the reason why. However, in Section 3, we see a number of ML-based solutions for various specific aspects of vulnerability assessment/management.

2.1 Top 10 Vulnerability Management Solution Providers for 2018 [EnterpriseSecurityMag-2018]

In "A Comparison of Vulnerability and Security Configuration Assessment Solutions" [Barros-2017], there was no explicit mention of any machine learning based solutions in all of the vendors' solutions.

In May 2018 Enterprise Security Magazine [EnterpriseSecurityMag-2018, p. 15], top 10 vulnerability management solution providers for 2018 are listed as follows:

- Appknox (appknox.com) – "Provides mobile application security testing services to build a safe and secure mobile ecosystem using a system plus human approach to outsmart hackers"
- BeyondTrust (beyondtrust.com) – "Delivers the visibility to reduce risks and the control to act against internal and external data breach threats"
- GFI Software (gfi.com) – "Develops smart enterprise-class IT solutions enabling IT administrators to easily and efficiently manage and secure their business networks systems, and applications."
- KennaSecurity (kennasecurity.com) – Uses its Cyber Risk Context Technology platform in a computer and network security organization to identify and remediate cyber risks
- Loki Labs (lokilabs.io) – Helps companies steer clear of the vulnerabilities in their infrastructure
- Nteligen (nteligen.com) – "Offers comprehensive solutions for enterprises worldwide to protect data against loss, misuse, and destruction"
- Qualys (qualys.com) – "Helps organizations streamline and consolidate their security and

compliance solutions in a single platform for better business outcomes”

- Rapid7 (rapid7.com) – “Powered by advanced analytics, Rapid7 transforms data into insight, empowering IT and security professionals to progress and protect their organizations”
- Reveelium Inc. (itrust.fr) – Offers an ingenious behavioral analytic engine, Reveelium, that detects anomalies and weak signals in the information system
- Specialized Security Services (s3security.com) – “A privately held boutique cybersecurity consulting firm specializing in consulting, auditing, and implementation of best practices to secure enterprises”

Except for Rapid7 and Reveelium, none of the other top ten solution providers seems to explicitly advertise its ML related solutions, if at all present. Moreover, no additional ML related information is provided for Rapid7 in [EnterpriseSecurityMag-2018] – other than its solution is powered by advanced analytics. In [EnterpriseSecurityMag-2018, p.32], we do have more information about Reveelium.

- Reveelium uses machine learning and big data analytics to detect APTs, viruses, deviant behaviors, loss of confidential data, and DOS using the following three engines:
  - *Weak signal detection engine* detects weak signals and anomalies.
  - *Business correlation engine* “programmatically aggregates, normalizes and analyzes the event log data, to understand its nature and alert the system administrators in case of a problem.”
  - *Global knowledge base* “identifies and collects the behaviors of all the Reveelium systems implemented by the customers, in order to make each of them benefit from the experience of others.”

Although IBM QRadar Vulnerability Manager (QVM https://www.ibm.com/ca-en/marketplace/cognitive-security-analytics) is not one of the ten mentioned above, it is worthwhile noting that

- IBM QRadar Vulnerability Manager (QVM), with QRadar Risk Manager and QRadar Advisor with Watson automates routine SOC tasks, finds commonalities across investigations and provides actionable feedback to analysts, freeing them up to focus on more important elements of the investigation and increase analyst efficiency.
- It is built with AI for the front-line Security Analyst

3. Some Machine Learning based Security Solutions

This section lists the application of ML in various areas of cyber security.

3.1 WEB AND SOFTWARE APPLICATIONS

This subsection describes the application of ML to detect vulnerability in web and software applications.

- [Imperva]
  - "High-Tech Bridge's web security testing platform ImmuniWeb® allows companies and financial institutions to monitor, detect, mitigate and prevent risks and threats to their web applications in a simple and cost-effective manner. ImmuniWeb leverages a hybrid security testing approach and machine learning technology for intelligent automation of web vulnerability scanning, significantly reducing human time required for advanced web security testing. Complemented by human intelligence, it detects the most sophisticated web application vulnerabilities and contractually guarantees zero false-positives."
- [Kronjee-2018] Discovering vulnerabilities using data-flow analysis and machine learning, Demonstrated for PHP (Hypertext Preprocessor) applications
- [Ognawal-2018] Automatically Assessing Vulnerabilities Discovered by Compositional Analysis
- [Takaesu-2016] Overview of the 'Vulnerability Scanning AI' using the machine learning
  - crawling web pages
  - detecting vulnerable pages
  - reporting scanned results
- [RandM-2018] Innovations in Vulnerability Management, Machine Learning, and Web-Based Security
- [Sasi-2016] Making Machines Think about Security

3.2 VULNERABILITY DETECTION

This subsection describes the application of ML in dealing with various issues of cyber security such as intrusion, malware, phishing, spam, penetration testing, obfuscation, and Tor (The Onion Router) traffic.

3.2.1 Intrusion

- [Abubakar-2017] Machine Learning Based Intrusion Detection System for Software Defined Networks
- [Apruzzesse-2018] On the Effectiveness of Machine and Deep Learning for Cyber Security
- [Buczak-2016] A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection

- [O'Flaherty-2018] How to use machine learning and AI in cyber
    - to monitor network traffic and learn what's normal within a system, using this information to flag up any suspicious activity
    - to deceive the adversary
- [Xin-2018] Machine Learning and Deep Learning Methods for Cybersecurity

3.2.2 Malware

- [Apruzzesse-2018] On the Effectiveness of Machine and Deep Learning for Cyber Security
- [Avira-2018a, Avira-2018b] Malware detection and classification, Avira NightVision (an AI platform)
- [Crowdstrike-2017] Malware prevention arsenal (endpoint protection)
    - ML-based scanner technology to be incorporated into VirusTotal.
    - VirusTotal, a subsidiary of Google, is a free service that analyzes suspicious files and URLs to facilitate the quick detection of viruses, worms, trojans, and all kinds of malware
- [Rokach-2016] When Cyber Security Meets Machine Learning
- [Zabidi-2017] Machine Learning Applications for the Cyber Security Threats

3.2.3 Phishing

- [Rokach-2016] When Cyber Security Meets Machine Learning

3.2.4 Spam

- [Apruzzesse-2018] On the Effectiveness of Machine and Deep Learning for Cyber Security

3.2.5 Penetration Testing

- [BusinessWire-2018] SEWORKS Launches Pentoma, AI-Driven Pen Testing Tool, and New AppSolid Security Scanner at MWC 2018
- [More-2018] Vulnerability Assessment and Penetration Testing through Artificial Intelligence
- [Pauli-2016] Hackers demo prototype security scanner that thinks like a human build the human-like penetrating testing box

3.2.6 Obfuscation

- [Cho-2017] Security Assessment of Code Obfuscation Based on Dynamic Monitoring in Android Things
- [Rokach-2016] When Cyber Security Meets Machine Learning

3.2.7 Tor Traffic

- [Singh-2018] Using the Power of Deep Learning for Cyber Security

3.3 APT (Advanced Persistent Threat) and Exploiting Threat Intelligence

- [Nunes-2018] At-Risk System Identification via Analysis of Discussions on the Darkweb
- [Truve] 4 Ways Machine Learning Is Powering Smarter Threat Intelligence

3.4 Prioritizing Patches

- A.I. Driven Unified Asset Discovery, Scan & Risk Prioritization https://www.delve-labs.com/
- [Imperva] Application Vulnerability Assessment and Virtual Patching with High-Tech Bridge and Imperva
- [Marshall-2018] Vulnerability Remediation: Best Practice or Best Guess?

3.5 Leveraging Data Analytics

- [Cisco-2018] Cisco Security Analytics
- [EnterpriseSecurityMag-2018, p. 15]
  - Rapid7 (rapid7.com) – powered by advance analytics
- [EnterpriseSecurityMag-2018, p. 15 and p. 32]
  - Reveelium (itrust.fr) – offered an ingenious behavioral analytics engine to detect anomalies and weak signals
- [Flanagan-2018] Security Analytics on Asset Vulnerability for Information Abstraction and Risk Analysis
- [Maloof-2006] Machine Learning and Data Mining for Computer Security – Methods and Applications
- [Tecnica-2016] DeepInsight (technicacorp.com) https://deepinsight.io/
  - Leverage data science and the power of advanced analytics to support business decisions

3.6 Predicting Vulnerability That Could Be Exploited

- CYLANCE (https://www.cylance.com/en-us/index.html) Don’t Stop Breaches, Prevent Them

- [GlobeNewswire-2018] Kenna Security granted patent for machine learning methods used to predict exploits
- [Osborn-2018] How to Harness Supervised Machine Learning to Predict Exploitability
- [Raguseo-2017] Proactive Vulnerability Management in the Age of Analytics
- [Roytman-2018] Predicting Exploitability – Forecasts for Vulnerability Management

4. Needs for Adversarial Machine Learning

Machine Learning used to be mainly focused on prediction accuracy. As such, the key considerations are the following:

- learning architecture: choosing the right learning architecture
- training data quality: choosing/preprocessing the representative dataset
- training process:
    - choosing/learning the right feature set to use
    - evaluating performance through training and testing

That was when adversarial attacks were considered not probable – where one or more malicious actors can subvert the ML process and application by one or all of the following:

- poisoning the training data so that the learned algorithm classifies often anomalies as normal
- evading the trained algorithm with hidden data that looks normal or malicious features that are outside of the training feature set

To understand adversarial attacks, we can make assumptions on how much information the attackers have on the ML process. In [Biggio-2018], the authors describe and analyze the following situations:

- black box: attackers have no knowledge
- gray box: attackers have limited knowledge
- white box: attackers have complete knowledge

Therefore, in addition to the traditional ML process, we will need to make the trained learning algorithm to withstand adversarial attack. A possible solution is to train the learning algorithm with adversarial examples. For more details, see [Biggio-2018]

A short list of adversarial ML articles and books are given below to supplement the above discussion. Note that more than 150 papers on this subject were published on ArXiv (https://arxiv.org/) in the last two years only (2016-17).

- [Apruzzese-2018] On the Effectiveness of Machine and Deep Learning for Cyber Security
    - The authors describe an example of vulnerability to adversarial attacks. The problem is with respect to Domain Generation Algorithm (DGA) attack. A Random Forest (RF) classifier is trained to detect DGA using known datasets and is shown to identify DGA with good detection rates (85% to 96%).

    - However, the RF classifier fails miserably with artificially generated adversarial samples (48%).
    - They also show the need for and benefit of adversarial learning, “in which adversarial samples are included in the training dataset to harden the ML detector.” In fact, some improvement is achieved after RF classified is trained with adversarial learning.
- [Biggio-2018] “Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning”
    - The authors “provide a thorough overview of the evolution of this research area over the last ten years and beyond, starting from pioneering, earlier work on the security of non-deep learning algorithms up to more recent work aimed to understand the security properties of deep learning algorithms, in the context of computer vision and cybersecurity tasks.”
- [Chan-2006] Machine Learning for Computer Security
    - After reviewing the four papers out of 19 accepted for publication in the Journal of Machine Learning Research under the special topic of “Machine Learning for Computer Security”, the authors suggests developing approaches to “provide sustained good performance in adversarial environments where a malicious adversary takes actions to subvert a classifier” such as the following:
        - obscuring important discriminating input features
        - adding extraneous additional features to make an input appear more normal
        - altering the prior probabilities of abnormal inputs
        - taking a combination of the above over time
- [Huang-2011] Adversarial machine learning
    - The authors show “how two machine learning methods, SpamBayes and PCA-based network anomaly detection, are vulnerable to causative attacks” (that is, attacks that alter the training process through influence over the training data) and how to “restrict an adversary’s actions.”
    - Examine “exploratory attacks against learning systems”
    - Explore “approaches and challenges for privacy-preserving learning”
- [Joseph-2012] Machine Learning Methods for Computer Security
    - This is a report of a workshop that focuses on “
        - the role of learning in computer security applications
        - the paradigm of secure learning
        - the future applications for secure learning

      “
- [Vorbeychik-2018] Adversarial Machine Learning
    - Provides a technical overview of the field from machine learning concepts and approaches in adversarial context to machine learning attack categorization.
    - Deals also in the context of deep learning and approaches for improving its robustness.

5. Research Conclusion

5.1 FUTURE WORK

We list here some research work for future consideration.

- How to best leverage ML, in general and adversarial ML in particular
- How to best integrate human and ML solution interaction, See [Truve-2017] for some suggestions.
- How to use ML to minimize false positives in vulnerability assessment
- More in-depth analysis of vendor solutions to determine their applications of ML-based solutions
- Analysis of what class of machine learning algorithms is more suitable to which class of vulnerability assessment and cyber security problems

5.2 SUMMARY

In this investigation to understand how ML is being applied in vulnerability assessment, we looked into various vulnerability assessment/management solutions. We found few vendors claiming ML application in their overall solutions. However, ML has been applied in many different specific areas of cyber security, including vulnerability detection.

From this investigation, we observe that:

- Application of ML tends to shift the focus of the cyber security solutions from a reactive type to a more proactive/predictive type – from recovery to prevention.
- A consequence of the above is the need to maintain accurate network information in terms of assets and configurations so as to be able focus on the proactive cyber security defense effort.
- There is an emphasis on achieving cooperative human and ML solutions. (See [Truve-2017].)
- Adversarial attacks are inevitable and hence the need for adversarial machine learning
- As a consequence of the above statement, for security issue, it is imperative to enhance the traditionally machine learning solutions/processes to handle adversarial conditions.
- If ML can improve prediction, it may reduce the number of false positives.
- A machine learning solution is usually composed of multiple components. As an example, see Reveelium described in Section 2.1.

6. References

[Abubakar-2017]	A. Abubakar and B. Pranggono, "Machine Learning Based Intrusion Detection System for Software Defined Networks," 2017 Seventh International Conference on Emerging Security Technologies (EST), pp. 138-143.
[Apruzzese-2018]	G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, M. Marchetti, "On the Effectiveness of Machine and Deep Learning for Cyber Security," 2018 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects, T. Minárik, R. Jakschis, L. Lindström (Eds.), 2018 © NATO CCD COE Publications, Tallinn. https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2019%20On%20the%20Effectiveness%20of%20Machine%20and%20Deep%20Learning%20for%20Cyber%20Security.pdf
[Avira-2018a]	An Avira White Paper, "The Application of AI to Cybersecurity," 2018. Avira Operations GmbH & Co. KG. https://oem.avira.com/resources/whitepaper_AI_EN_20180306.pdf
[Avira-2018b]	An Avira White Paper, "NightVision – Using Machine Learning to Defeat Malware," 2018. Avira Operations GmbH & Co. KG. https://oem.avira.com/resources/whitepaper_NightVision_EN_20180306.pdf
[Barros-2017]	A. Barros, A. Chuvakin, M. L. Judd, "A Comparison of Vulnerability and Security Configuration Assessment Solutions," August 2017, Gartner Report.
[Biggio-2018]	B. Biggio and F. Roli, "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning," Pattern Recognition, Volume 84, December 2018, Pages 317-331. https://arxiv.org/pdf/1712.03141.pdf
[Buczak-2016]	A.L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, Vol. 18, No. 2, Second Quarter 2016, pp. 1153-1176.
[BusinessWire-2018]	Business Wire, "SEWORKS Launches Pentoma, AI-Driven Pen Testing Tool, and New AppSolid Security Scanner at MWC 2018," February 2018. https://www.businesswire.com/news/home/20180221005302/en/SEWORKS-Launches-Pentoma-AI-Driven-Pen-Testing-Tool
[Chan-2006]	P.K. Chan and R.P. Lippmann, "Machine Learning for Computer Security," Journal of Machine Learning Research 7 (2006) 2669-2672.

	http://www.jmlr.org/papers/volume7/MLSEC-intro06a/MLSEC-intro06a.pdf
[Chio-2018]	C. Chio and D. Freeman, “Machine Learning and Security – Protecting Systems with Data and Algorithms,” O’Reilly Media, February 2018. http://shop.oreilly.com/product/0636920065555.do
[Cho-2017]	T. Cho, H. Kim, and J.H. Yi, “Security Assessment of Code Obfuscation Based on Dynamic Monitoring in Android Things,” Security and Privacy in Applications and Services for Future Internet of Things, 2017 IEEE Access (Volume: 5). https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7898406
[Cisco-2018]	A Cisco White Paper, “Cisco Security Analytics,” 2018. https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/white-paper-c11-740605.pdf
[Crowdstrike-2017]	A Crowdstrike White Paper, “The Rise of Machine Learning in Cybersecurity,” 2017. https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperMachineLearning.pdf?aliId=8202056
[Darktrace-2016]	A Darktrace White Paper, “The Enterprise Immune System, Proven Mathematics and Machine Learning for Cyber Defense,” 2016. https://cyberexchange.uk.net/media/darktrace/resources/Enterprise%20Immune%20System%20%E2%80%94%20ROW.pdf
[Drinkwater-2017]	D. Drinkwater, “5 top m,achine learning use cases for security,” December 2017. https://www.cso.com.au/article/631162/5-top-machine-learning-use-cases-security/
[EnterpriseSecurityMag-2018]	Enterprise Security Magazine, “Vulnerability Management Special,” May 2018. https://www.enterprisesecuritymag.com/magazines/May2018/Vulnerability_Management/
[Flanagan-2016]	K. Flanagan, E. Fallon, A. Awad, and P. Connolly, “Security Analytics on Asset Vulnerability for Information Abstraction and Risk Analysis,” 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation, pp. 9-15.
[GlobeNewswire-2018]	Globe Newswire, “Kenna Security granted patent for machine learning methods used to predict exploits,” November 2018. https://globenewswire.com/news-release/2018/11/07/1647495/0/en/Kenna-Security-granted-patent-for-machine-learning-methods-used-to-predict-

	exploits.html
[Hema-2018]	P. Hema, “Machine Learning In Cyber Security,” Tata Cyber Security Community, August 2018. https://securitycommunity.tcs.com/infosecsoapbox/articles/2018/08/01/machine-learning-cyber-security
[Huang-2011]	L. Huang, A. D. Joseph, B. Nelson, B.I.P. Rubinstein, and J.D. Tygar, “Adversarial machine learning,” AISec '11 Proceedings of the 4th ACM workshop on Security and artificial intelligence, October 2011, pp. 43-58.
[Imperva]	An Imperva Solution Brief, “Application Vulnerability Assessment and Virtual Patching with High-Tech Bridge and Imperva,” https://www.imperva.com/docs/SB_Imperva_High-Tech_Bridge.pdf
[Joseph-2012]	A.D. Joseph, P.Laskov, F. Roli, J. Doug Tygar, and B. Nelson, “Machine Learning Methods for Computer Security,” Manifesto from Dagstuhl Perspectives Workshop 12371. http://drops.dagstuhl.de/opus/volltexte/2013/4356/pdf/dagman-v003-i001-p001-12371.pdf
[Koppula-2018]	R. Koppula, “Applications of Machine Learning in Cyber Security You need to Know About,” Apiumhub, March 2018. https://apiumhub.com/tech-blog-barcelona/applications-machine-learning-cyber-security/
[Kronjee-2018]	J.J. Kronjee, “Discovering vulnerabilities using data-flow analysis and machine learning, Demonstrated for PHP applications,“ 2018. https://dspace.ou.nl/bitstream/1820/9725/1/Kronjee%20J%20IM9906%20AF%20scriptie.pdf
[Maloof-2006]	M.A. Maloof (Ed.), “Machine Learning and Data Mining for Computer Security – Methods and Applications,” 2016. https://www.springer.com/gp/book/9781846280290
[Marshall-2018]	S. Marshall, “Vulnerability Remediation: Best Practice or Best Guess?” June 2018. https://www.securitynow.com/author.asp?section_id=654&doc_id=743466
[More-2018]	S. More and A. Rohela, “Vulnerability Assessment and Penetration Testing through Artificial Intelligence,” International Journal of Recent Trends in Engineering & Research, Volume 04, Issue 01; January 2018, pp. 217-224.

	https://www.ijrter.com/papers/volume-4/issue-1/vulnerability-assessment-and-penetration-testing-through-artificial-intelligence.pdf
[Nunes-2018]	E. Nunes, P. Shakarian, and G.I. Simari, “At-Risk System Identification via Analysis of Discussions on the Darkweb,” 2018 APWG Symposium on Electronic Crime Research (eCrime), May 2018, https://docs.apwg.org/ecrimeresearch/2018/5359943.pdf
[O’Flaherty-2018]	K. O’Flaherty, “How to use machine learning and AI in cyber security,” January 2018. https://www.itpro.co.uk/security/30102/how-to-use-machine-learning-and-ai-in-cyber-security
[Ognawal-2018]	S. Ognawala, R.N. Amato, A. Pretschner, and P. Kulkarni, “Automatically Assessing Vulnerabilities Discovered by Compositional Analysis,” MASES’18, September 2018, Montpellier, France. https://arxiv.org/pdf/1807.09160.pdf
[Osborn-2018]	S. Osborn, “How to Harness Supervised Machine Learning to Predict Exploitability,” April 2018. https://www.kennasecurity.com/how-to-harness-supervised-machine-learning-to-predict-exploitability/
[Pauli-2016]	D. Pauli, “Hackers demo prototype security scanner that thinks like a human,” March 2016. https://www.theregister.co.uk/2016/03/17/hackers_demo_prototype_security_scanner_that_thinks_like_a_human/
[Raguseo-2017]	D. Raguseo, P. Manganelli, and A. Pecorari, “Vulnerability Management in the Age of Analytics,” Security Intelligence, May 2017. https://securityintelligence.com/vulnerability-management-in-the-age-of-analytics/
[RandM-2018]	A Research and Markets Report, “Innovations in Vulnerability Management, Machine Learning, and Web-Based Security,” October 2018. https://www.researchandmarkets.com/research/m56hc6/innovations_in?w=4
[RecordedFuture-2018]	A Recorded Future Blog, “Machine Learning: Practical Applications for Cybersecurity,” March 2018. https://www.recordedfuture.com/machine-learning-cybersecurity-applications/
[Rokach-2016]	L. Rokach, “When Cyber Security Meets Machine Learning,” 2016. https://ucys.ugr.es/jnic2016/docs/MachineLearning_LiorRokachJNIC2016.pdf
[Roytman-	M. Roytman, “Predicting Exploitability – Forecasts for Vulnerability

2018]	Management," April 2018. https://www.slideshare.net/cisoplatform7/predicting-exploitabilityforecastsforvulnerabilitymanagement
[Sasi-2016]	R. Sasi, "Making Machines Think about Security," NULLCON GOA'16, https://regmedia.co.uk/2016/03/17/slides_987676587434243.pdf
[Singh-2018]	S. Singh and A.R. Balamurali, "Using the Power of Deep Learning for Cyber Security," A Guest Blog at Analytics Vidhya, July 2018. https://www.analyticsvidhya.com/blog/2018/07/using-power-deep-learning-cyber-security/
[Takaesu-2016]	I.Takaesu, "Overview of the 'Vulnerability Scanning AI' using the machine learning," 2016. https://www.mbsd.jp/blog/20160113_2.html
[Technica-2016]	A Technica White Paper, "Deep Learning for Cybersecurity Use Cases," 2016. http://technicacorp.com/wp-content/uploads/2017/01/WP_Deep-Learning-for-Cybersecurity_111716.pdf
[Truve]	S. Truve, "4 Ways Machine Learning is Powering Smarter Threat Intelligence," A Recorded Future White Paper. Can be requested from: https://go.recordedfuture.com/machine-learning
[Truve-2017]	S. Truve, "Machine Learning in Cyber Security: Age of the Centaurs," A Recorded Future 2017 White Paper. https://www.brookcourtsolutions.com/wp-content/uploads/2017/07/Machine-Learning-in-Cyber-Security-White-Paper-Brookcourt.pdf
[Veiga-2018]	A.P. Veiga, "Application of Artificial Intelligence (AI) to Network Security," 2018. https://arxiv.org/ftp/arxiv/papers/1803/1803.09992.pdf
[Vorobeychik-2018]	Y. Vorobeychik and M. Kantarcioglu, "Adversarial Machine Learning," 2018 by Morgan & Claypool.
[Xin-2018]	Y, Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, "Machine Learning and Deep Learning Methods for Cybersecurity," 2018 IEEE Access (Vol.: 6). https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8359287
[Zabidi-2017]	M.N.A. Zabidi, "Machine Learning Applications for the Cyber Security Threats," HGCI Summit 2017. https://www.endpoint.com/blog/2017/12/12/hgci-

	summit-2017/najmi_hgci_slides_2017.pdf

7. Appendix A: Some Reference on Machine Learning in Cyber Security

In this section, we list some articles and books on ML in the cyber security context.

- [Apruzzese-2018] On the Effectiveness of Machine and Deep Learning for Cyber Security (See Section 4 for a brief description.)
- [Avira-2018a] The Application of AI to Cybersecurity (See Section 3.2.2 for a brief description.)
- [Chan-2006] Machine Learning for Computer Security (See Section 4 for a brief description.)
- [Chio-2018] Machine Learning and Security Protecting Systems with Data and Algorithms
    - The authors “provide examples of how machine learning can be applied to augment or replace rule-based or heuristic solutions to problems like intrusion detection, malware classification, or network analysis. In addition to exploring the core machine learning algorithms and techniques, we focus on the challenges of building maintainable, reliable, and scalable data mining systems in the security space. Through worked examples and guided discussions, we show you how to think about data in an adversarial environment and how to identify the important signals that can get drowned out by noise.”
- [Crowdstrike-2017] The Rise of Machine Learning in Cybersecurity (See Section 3.2.2 for a brief description.)
- [Drinkwater-2017] 5 top machine learning use cases for security
  “
    - to detect malicious activity and stop attacks
    - to analyze mobile endpoints
    - to enhance human analysis
    - to automate repetitive security tasks
    - to close zero-day vulnerabilities

  “
- [Hema-2018] Machine Learning In Cyber Security
    - The author provides a list of successful applications and future applications.
- [Koppula-2018] Applications of Machine Learning in Cyber Security You Need to Know About
    - Describes how machine learning can help protect against spear phishing, watering hole, web shell, Ransomware, and remote exploitation.
- [Maloof-2006] Machine Learning and Data Mining for Computer Security

    - Though this book is a little dated, it "presents research conducted in academia and industry on methods and applications of machine learning and data mining for problems in computer security … "
- [O'Flaherty-2018] How to use machine learning and AI in cyber security
    - Describes the use of machine learning to detect anomaly and to deceive attackers.
- [RecordedFuture-2018] Machine Learning: Practical Applications for Cybersecurity
    - Argues for human and machine cooperation.
    - "One of the biggest barriers to human intelligence is language."
    - "The battle in threat intelligence is balancing time and context."
- [Rokach-2016] When Cyber Security Meets Machine Learning
    - Deals with a number cyber security issues
- [Singh-2018] Using the Power of Deep Learning for Cyber Security
    - Introduces "Deep Learning (DL) along with a few existing Information Security (hereby referred to as InfoSec) applications it enables. We then deep dive into the interesting problem of anonymous tor traffic detection and also present a DL-based solution to detect TOR traffic."
- [Technica-2016] Deep Learning for Cybersecurity Use Cases
    - Introduces deep learning and its applications
- [Truve-2017] Machine Learning in Cyber Security: Age of the Centaurs
    - Argues that "threat analyst centaurs – man and machine working together – will be teams capable of tackling the most difficult cyber adversaries."
- [Veiga-2018] Application of Artificial Intelligence (AI) to Network Security
    - A survey paper with a description of Darktrace
- [Xin-2018] Machine Learning and Deep Learning Methods for Cybersecurity
    - "This survey report describes key literature surveys on machine learning (ML) and deep learning (DL) methods for network analysis of intrusion detection and provides a brief tutorial description of each ML/DL method."

8. Appendix A: Some Machine Learning Patents in Cyber Security

- [GlobeNewswire-2018] reported that Kenna Security (https://www.kennasecurity.com/) "has been granted a patent for its groundbreaking use of machine learning to predict which cybersecurity exploits will become weaponized. The patent recognizes Kenna's use of machine learning to predict, at the moment a vulnerability is released, if an exploit will follow, and whether or not that exploit will be used in an attack."
- Darktrace (https://www.darktrace.com/en /) claims to have patented an algorithm known as "Enterprise Immune System", which is capable of defending an enterprise network by emulating the way the human body defends against infections. A filing of

the patent is given here:

- https://patents.google.com/patent/WO2016020660A1/en with 2014 priority date

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.) Solan Networks 301 Moodie Drive, Suite 215 Nepean, Ontario Canada K2H 9C4	2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.) CAN UNCLASSIFIED 2b. CONTROLLED GOODS NON-CONTROLLED GOODS DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

Machine Learning in Vulnerability Assessment

4. AUTHORS (Last name, followed by initials – ranks, titles, etc., not to be used)

Montuno, D.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)	6b. NO. OF REFS (Total references cited.)
December 2018	21	47

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

Contract Report

8. SPONSORING CENTRE (The name and address of the department project office or laboratory sponsoring the research and development.)

DRDC – Ottawa Research Centre
Defence Research and Development Canada, Shirley's Bay
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
05ac - Cyber Decision Making and Response (CDMR)	W7714-115274/001/SV
10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2019-C067	

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

Cyber; Cyber Defence; Cyber Security; Machine Learning

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

Machine Learning (ML) is increasingly being applied in vulnerability assessment and more generally in providing cyber security. We review ML applications in both those areas by commercial vendors. We also review recent results in adversarial learning; since ML requires training data to be effective, it is susceptible to adversarial attacks in which that data is poisoned to impair the ML's functionality or allow attackers to bypass it. As a result of this adversarial nature of the problem, we conclude that the automated nature of ML-based solutions increases the need for accurate ground truth input data, and that more research is required to ensure the safety and effectiveness of these approaches with human-machine cooperation in mind.

On utilise de plus en plus l'apprentissage machine (AM) en évaluation des vulnérabilités et de façon plus générale en prestation de services de cybersécurité. Nous avons évalué les applications d'AM proposées dans ces deux domaines par des fabricants du secteur privé. Nous nous sommes aussi penchés sur des résultats récents en apprentissage adverse : comme l'AM a besoin de données d'entraînement pour être efficace, il est vulnérable à des attaques adverses par l'empoisonnement de ces données afin d'handicaper l'AM ou de l'aveugler à des attaques hostiles. Vu la nature adverse du problème, nous concluons que le caractère automatisé des solutions fondées sur l'AM rend encore plus vitale la fidélité à la réalité sur le terrain des données avec lesquelles on les alimente, et qu'il faut des recherches plus approfondies pour assurer la sécurité et l'efficacité de ces stratégies, en gardant en tête la coopération humain-machine.