



Cyber-Security, an issue or an opportunity?

SOLUTIONS FOR SECURITY REQUIREMENTS

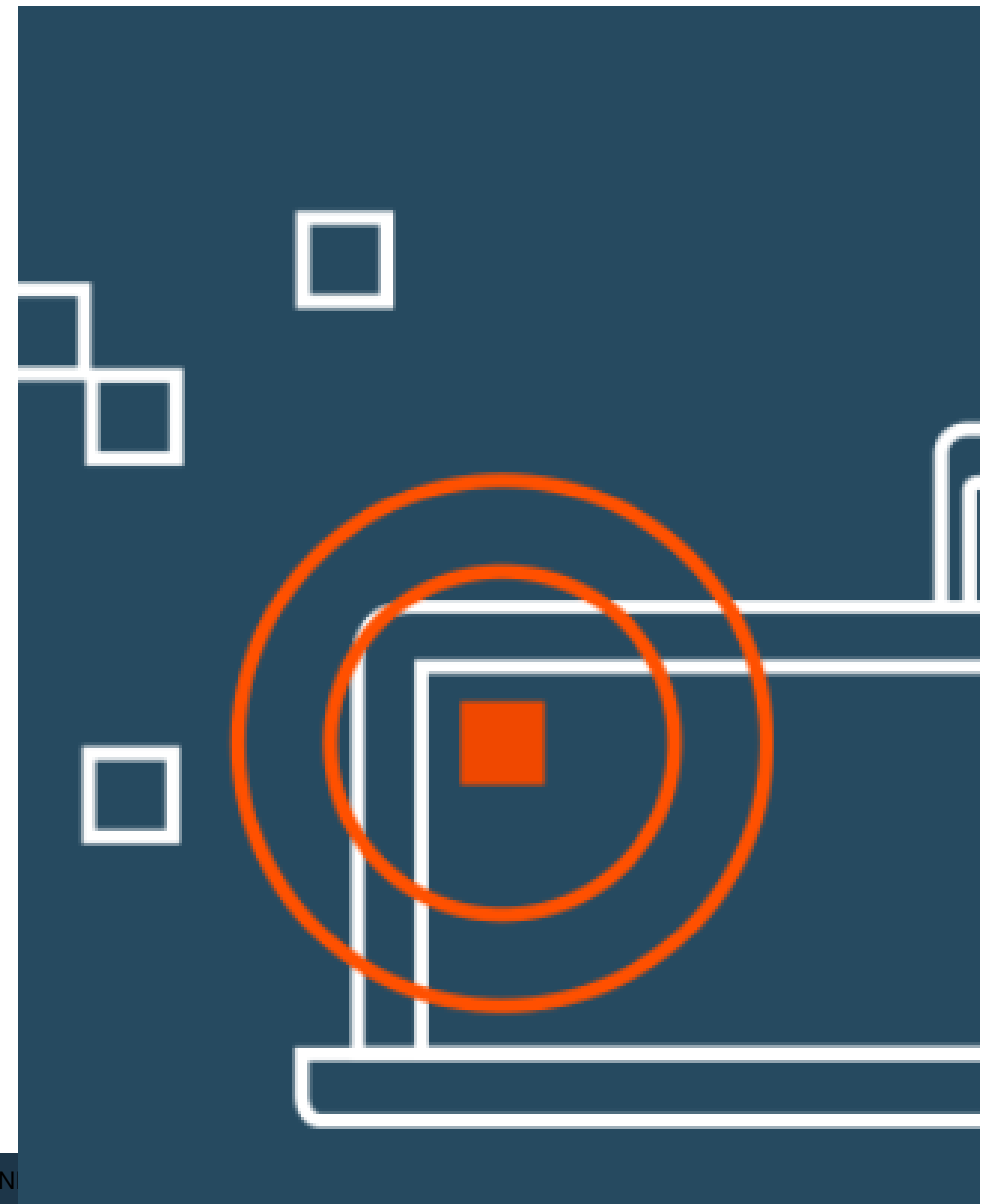

Domenico Raguseo
@domenicoraguseo

February 2019



Agenda

- Challenges
 - Need of Growth
 - Disconnected security capabilities are failing us
 - Difficult to develop best practices
 - Compliance
 - Sophistication of attackers
- How to address challenges
- Is AI a challenge or an opportunity ?
- Opportunities



Challenge #1 : Need of Growth

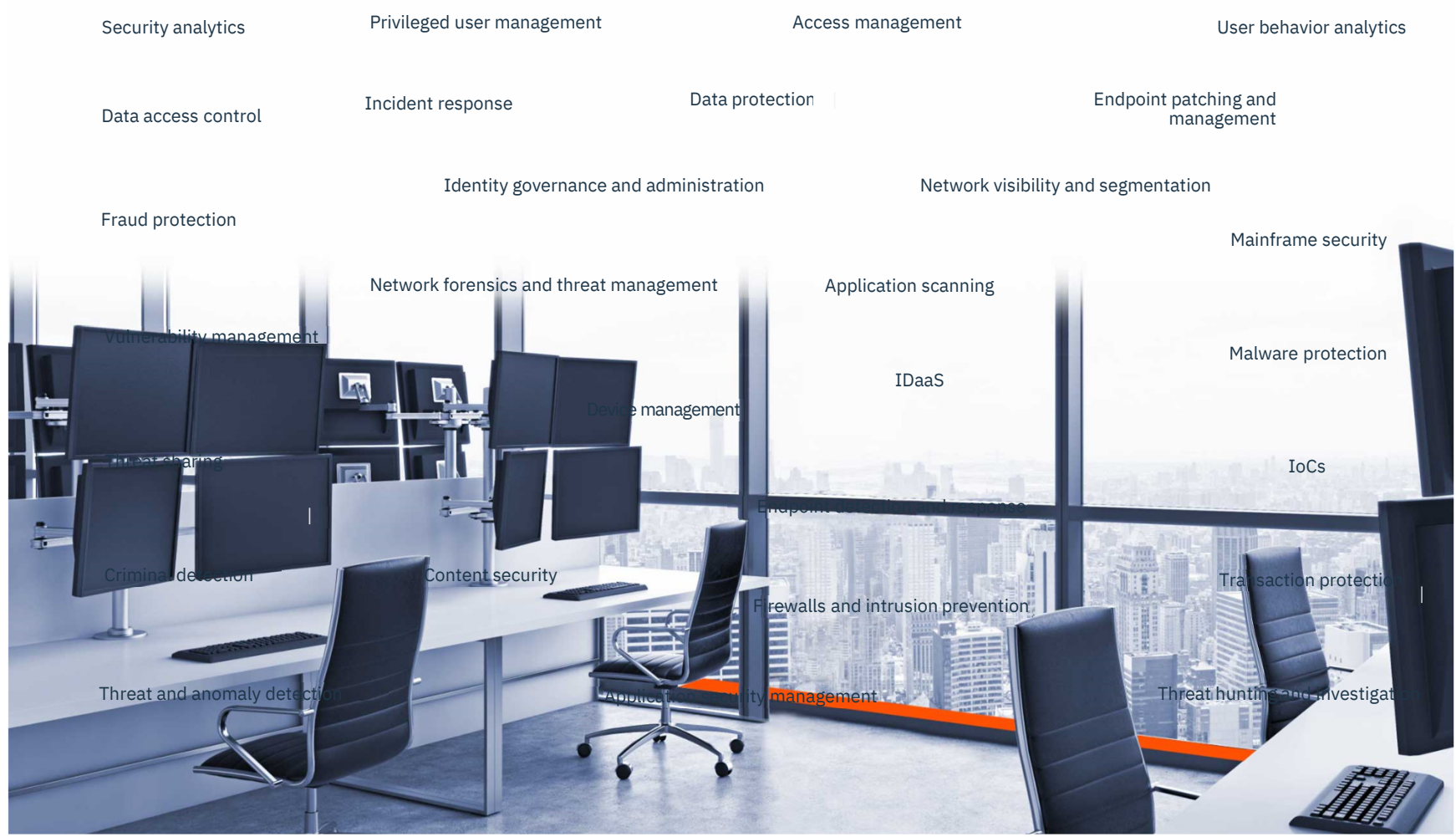
- Adopt and Adapt to regulations
- Utilizations of new technologies
 - IoT
 - Cloud
 - Quantum
- Open Banking
- Mirai
- CyberSecurity having an Intrinsic value



Insights From European Customers on Cybersecurity and Security Awareness

November 30, 2018 | By [Domenico Raguseo](#) Co-authored by [Jean-Luc Labbé](#) | [Pier Luigi Rotondo](#)

Challenge #2 - Disconnected security capabilities are failing us



Challenge #3 : Difficult to develop Best Practices

- Threat depends on several factors
- Risk mitigation requires continuous assessment

- Railway versus Airway
- Stuxnet versus Mirai

How Can We Make Smart Cities Even Smarter? Start With Security Intelligence

July 5, 2018 | By Domenico Raguseo



The Future of Cybersecurity

February 10, 2017 | By Domenico Raguseo



Challenge #4 : Compliance

- Does compliance helps ?

YES !!!

Securing Mobile Transactions and Payments in the Age of Connected Devices

November 30, 2017 | By [Domenico Raguseo](#)



Open Banking: Tremendous Opportunity for Consumers, New Security Challenges for Financial Institutions

April 13, 2018 | By [Domenico Raguseo](#)



Challenge #5 : Sophistication of attackers

- Who are the bad guys ?
 - Development of Malware is not illegal
 - Legal or not legal, possibilities of investigation depends on local regulation
- CyberCrime is a very well organized crime

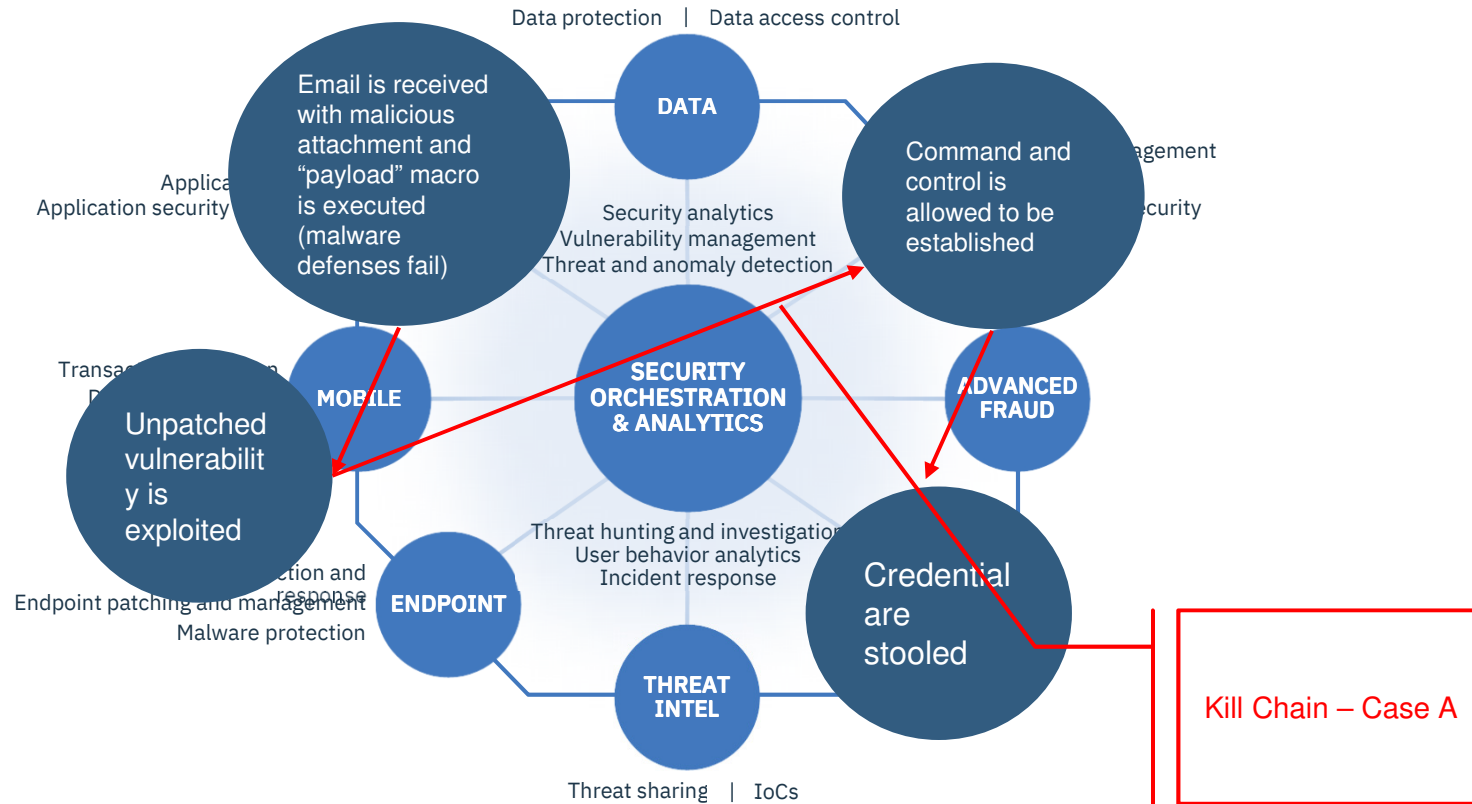


Analyze Attack Patterns to Make Your Environment Secure by Design

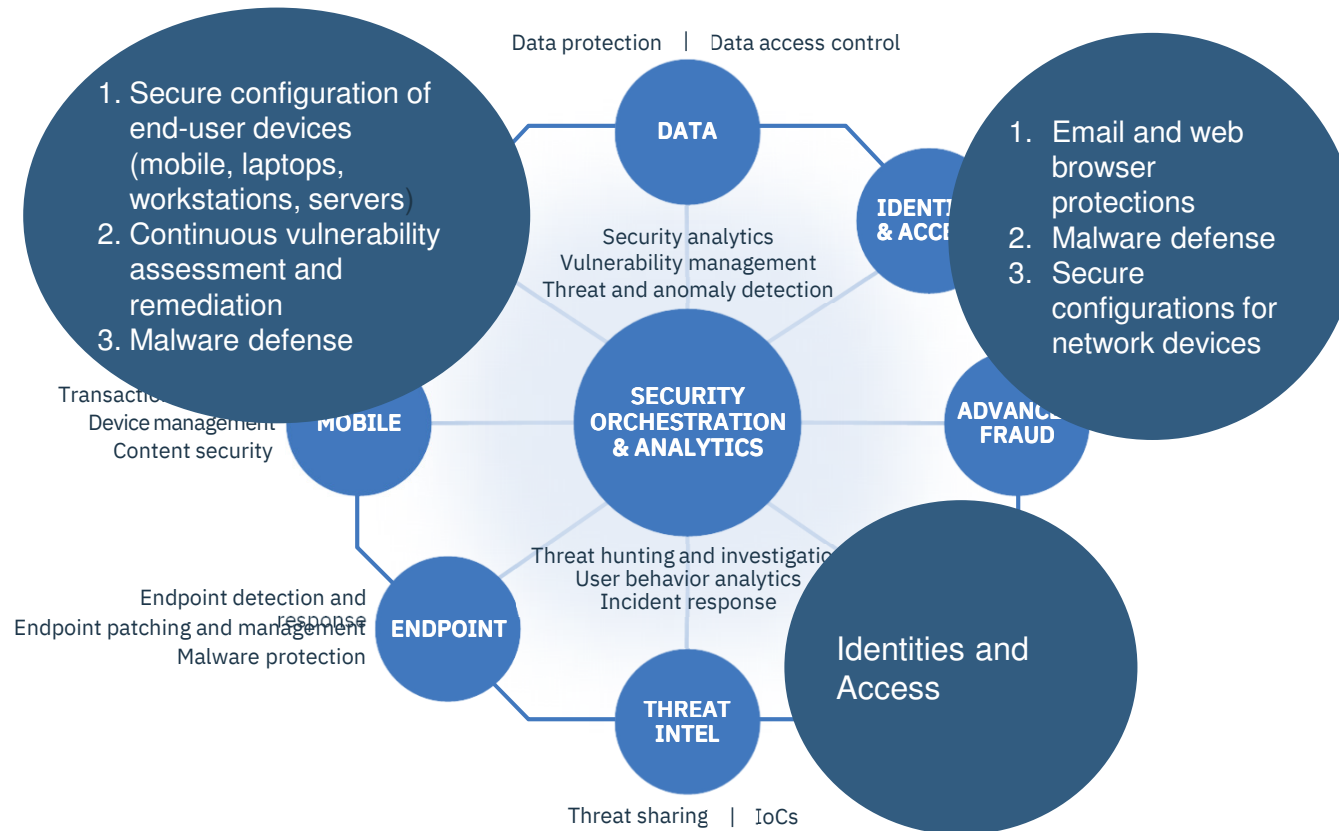
September 1, 2017 | By [Domenico Raguseo](#)

- Disfranchising
- Business Email Compromise

Activities performed during Business Email Compromise – Case A

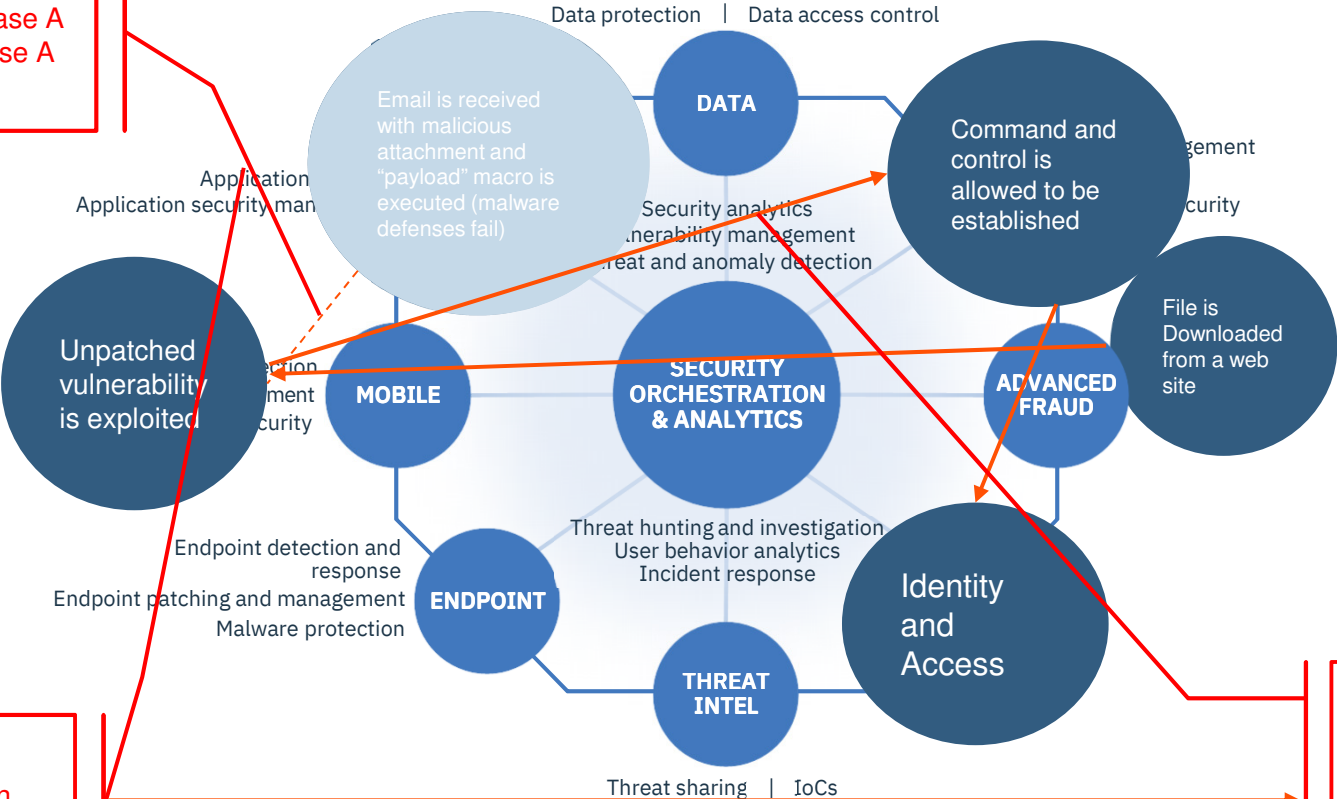


Security controls violated during Business Email Compromise



Watering hole .. A change in attach strategy . Case B

Kill Chain – Case A
Case B != Case A



Attach Pattern
A + B

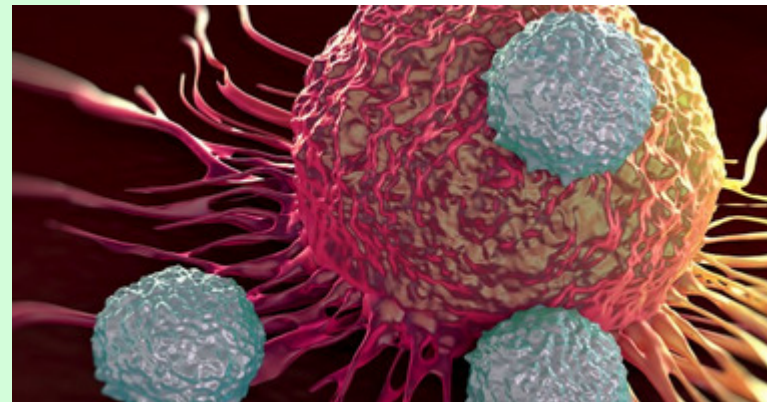
Kill Chain - Case B
Case B != Case A

How to address challenges

- Utilization of cognitive technologies and AI in the implementation of security controls
- Security by Design
 - Configuration Management
 - Security having an intrinsic value
 - Consider to implement security controls on demand
- Integration of security control
- Collaboration and awareness
- Focus on prevention but also detection and response

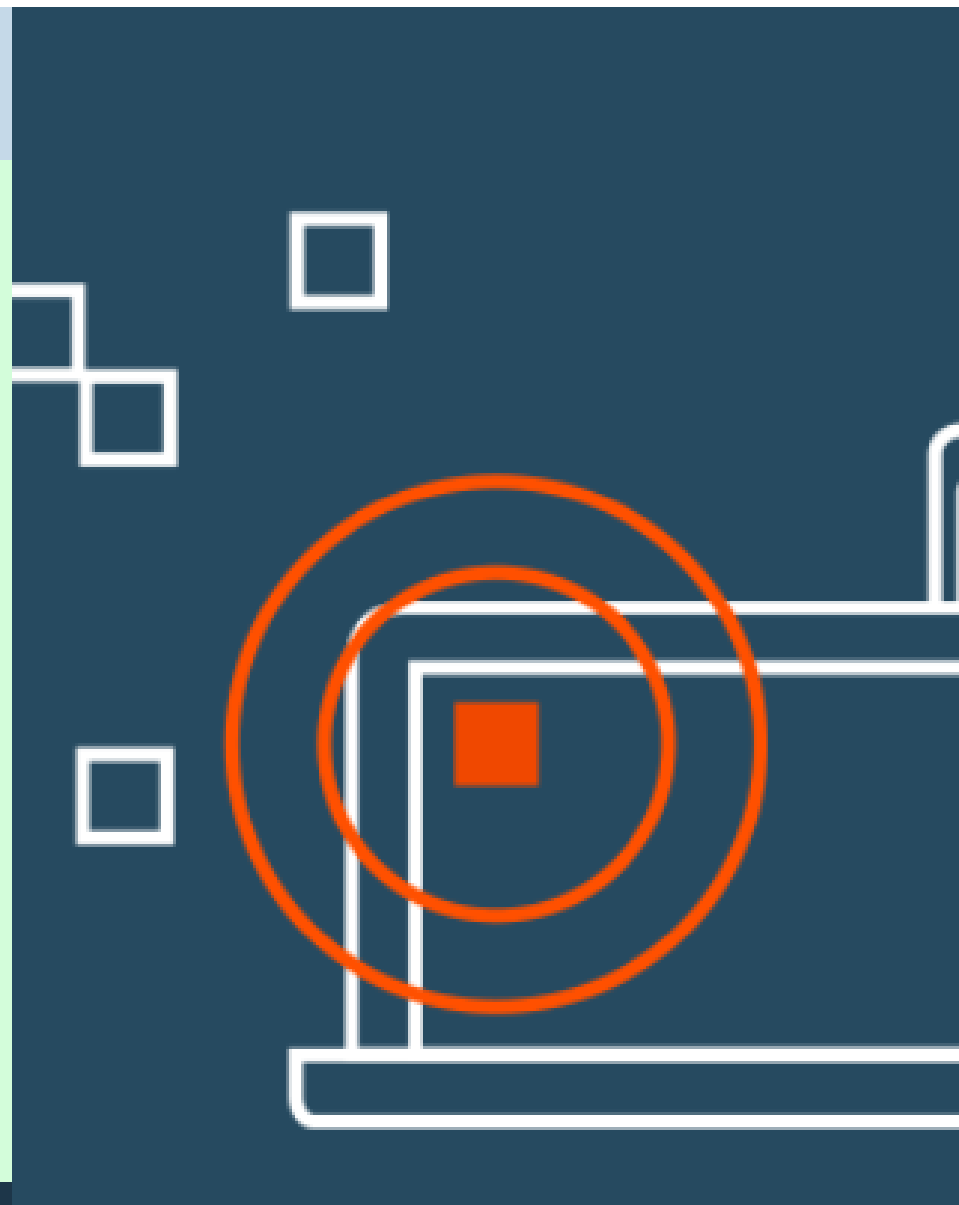
The Power of the Security Immune System

June 16, 2017 | By [Domenico Raguseo](#)



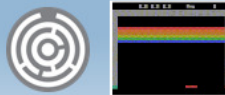


Opportunities

- The perfect crime does not exist in the cyber world
- Criminals use the digital ecosystem
- Cybersecurity technologies can be exported to the physical world
 - Authentication



Is AI a challenge or an Opportunity ?

- Threat Analysis
- Incident Triage
- Vulnerabilities to fix
- Anomaly Detection
- Biometrical Regognition

AI Powered Attacks	Attacking AI	Theft of AI
<ul style="list-style-type: none">• Generate: DeepHack tool learned SQL injection [DEFCON'17]• Automate: generate targeted phishing attacks on Twitter [Zerofox Blackhat'16]• Refine: Neural network powered password crackers• Evade: Generative adversarial networks learn novel steganographic channels	<ul style="list-style-type: none">• Poison: Microsoft Tay chatbot poisoning via Twitter (and Watson "poisoning" from Urban Dictionary) [Po]• Evade: Real-world attacks on computer vision for facial recognition biometrics [CCS'16] and autonomous vehicles [OpenAI] [Ev]• Harden: Genetic algorithms and reinforcement learning (OpenAI Gym) to evade malware detectors [Blackhat/DEFCON'17] [Ev]	<ul style="list-style-type: none">• Theft: Stealing machine learning models via public APIs [USENIX'16] [DE]• Transferability: Practical black-box attacks learn surrogate models for transfer attacks [ASIACCS'17] [ME, Ev]• Privacy: Model inversion attacks steal training data [CCS'15] [DE]
		



THANK YOU

FOLLOW US ON:



ibm.com/security



securityintelligence.com



xforce.ibmcloud.com



[@ibmsecurity](https://twitter.com/ibmsecurity)



youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

