ISSA

Information Systems Security Association International

www.issa.org

ISSA Thought Leadership Webinar

2019 Cybersecurity Trends to Watch

December 5, 2018

2019 Cybersecurity Trends to Watch

Today's web conference is generously sponsored by:

KEYFACTOR

https://www.keyfactor.com/

2019 Cybersecurity Trends to Watch

Moderator

Michael Levin, CEO/Founder, Center for Information Security Awareness

Michael Levin is a nationally known cyber security professional who spent over twenty-two years in the U.S. Secret Service protecting Presidents and Heads of State. Michael retired from the U.S. Department of Homeland Security - as the Deputy Director of the National Cyber Security Division in Washington DC. He enjoyed a distinguished thirty-year career in public service and law enforcement.

After this distinguished career and seeing the need, Michael founded the Center for Information Security Awareness – www.CFISA.com The CFISA was created to explore ways to increase cyber security awareness among many audiences, including consumers, employees, businesses and law enforcement. CFISA provides online and on-site cyber security awareness training services to businesses and organizations of all sizes.

2019 Cybersecurity Trends to Watch

Speaker

Ted Shorter, CTO and Co-Founder, Keyfactor

Ted Shorter is the chief technology officer and co-founder of Keyfactor (formerly, Certified Security Solutions). A renowned Public Key Infrastructure (PKI) expert, Ted has provided oversight to hundreds of private-sector enterprise PKI deployments, in multiple vertical markets including: Healthcare, Finance, Manufacturing, Aerospace, and e-Commerce. Ted has worked in the security arena for over 25 years, in the fields of cryptography, application security, authentication and authorization services, and software vulnerability analysis.

2019 Cybersecurity Trends to Watch

Speaker

Jim Rutt, Chief Information Officer, Dana Foundation

Jim Rutt, CISSP, CISM, CISA, CGEIT, CRISC, C|CISO, CCSK, is the Chief Information Officer at the Dana Foundation. His responsibilities include providing strategic planning for information and technology management and overseeing all back office technology operations necessary to support the Foundation. Jim is an early adopter of cutting edge cloud security solutions, having led Dana through a complete cloud transformation three years ago. Jim has frequently spoken to peer organizations on corporate cybersecurity strategy and risk management, and also advises early stage technology companies on their sales strategy to the financial and healthcare sector.

Jim is a graduate of Stetson University, where he received a B.B.A. degree. He has 21 years of technology experience (spanning financial, healthcare and pharmaceutical sectors) and has been at Dana for eight years. Jim has presented at multiple CIO and leadership conferences, and has been quoted in the Wall Street Journal (among other publications) for his view on mobile security and governance. Jim is President and Chairman of the Board of Technology Affinity Group (TAG) and is Vice President and Board Director for the New York Metro Chapter of the Cloud Security Alliance. and is a member of Society for Information Management, SIM Foundation of NJ, CIO4Good, as well as a founding advisory board member of BWG Strategy LLC, a Work-Bench Venture Capital Mentor/Advisor, advisor to Lightspeed Ventures, a Silicon Venture capital company, and board advisor to multiple startups including Baffle, Axonius, Minerva Labs and Pixm.

2019 Cybersecurity Trends to Watch

Speaker

Ted Shorter, CTO and Co-Founder, Keyfactor

Ted Shorter is the chief technology officer and co-founder of Keyfactor (formerly, Certified Security Solutions). A renowned Public Key Infrastructure (PKI) expert, Ted has provided oversight to hundreds of private-sector enterprise PKI deployments, in multiple vertical markets including: Healthcare, Finance, Manufacturing, Aerospace, and e-Commerce. Ted has worked in the security arena for over 25 years, in the fields of cryptography, application security, authentication and authorization services, and software vulnerability analysis.

ISSA
Information Systems Security Association International

KEYFACTOR
COMMAND

SECURE DIGITAL IDENTITY FOR THE ENTIRE ENTERPRISE

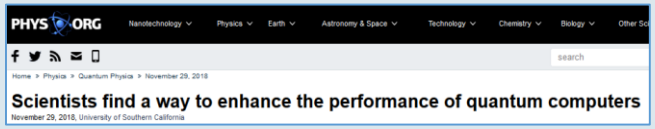
KEYFACTOR
CONTROL

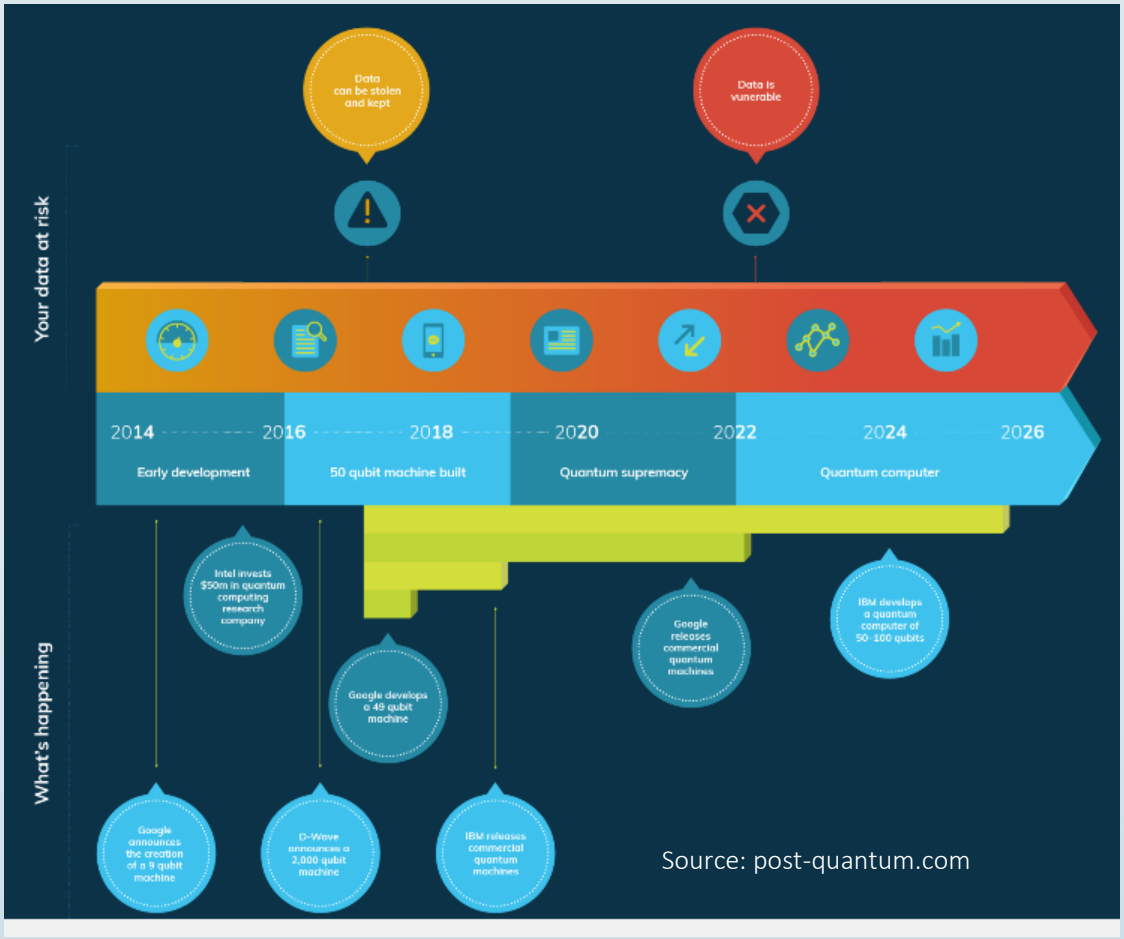
THE END-TO-END SECURE IDENTITY PLATFORM FOR CONNECTED DEVICES

CSS is now:

KEYFACTOR

Trend 1: Quantum Computing



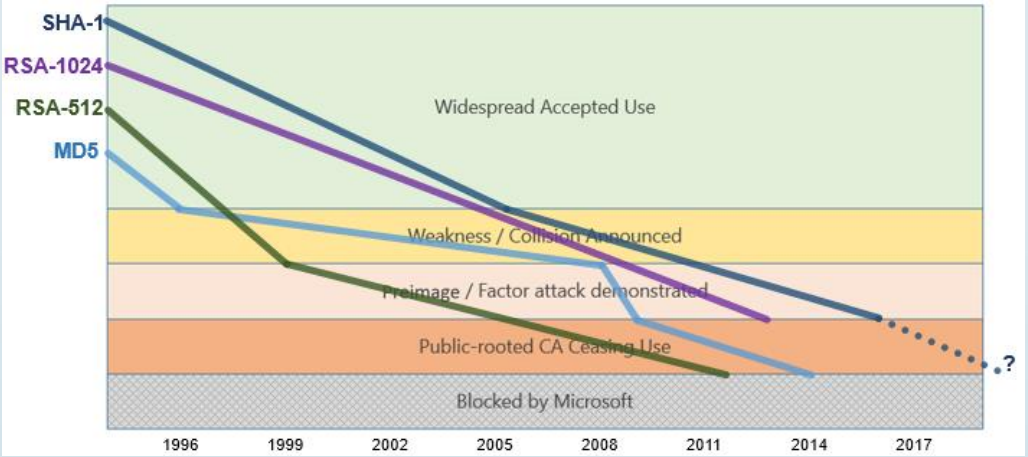


CSS is now:

KEYFACTOR

Crypto-Agility & Quantum

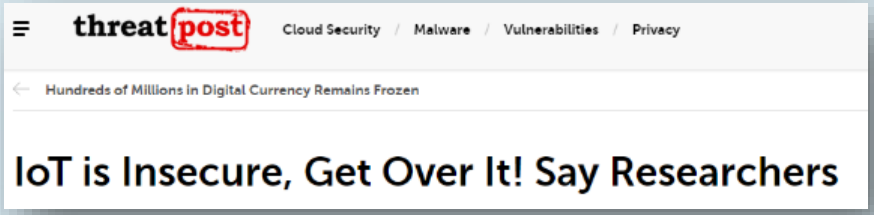
- Know what you have
  - Gather and maintain an inventory of all certificates and keys
- Develop response plans for crypto events:
  - Normal expiration / rotation / re-encryption
  - Algorithm breakage
  - Public root breach
  - Quantum breakthroughs



Trend 2: IoT Insecurity

2018 was a bad year for Internet-of-Things Security

IoT security at Black Hat 2018: The insecurity of things

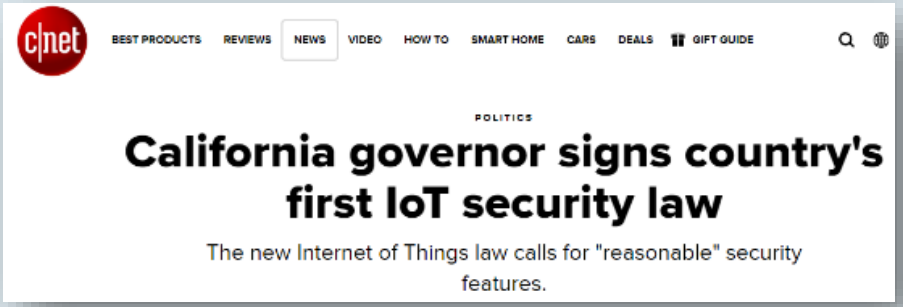


CSS is now: KEYFACTOR

2019 will likely be worse

Trend 3: IoT Security

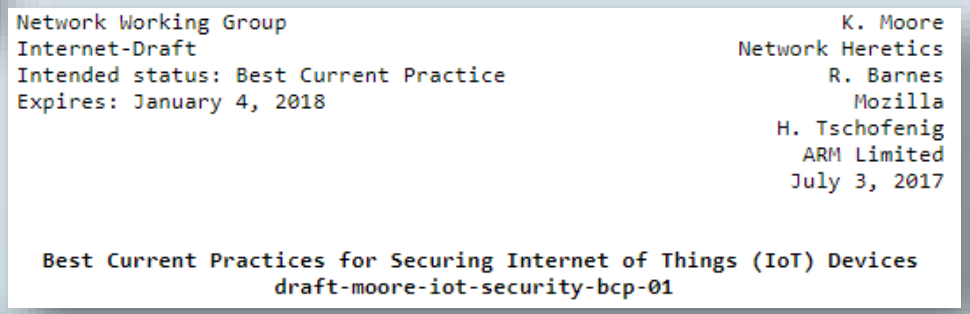
The first step is admitting you have a problem…


c|net BEST PRODUCTS REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS GIFT GUIDE

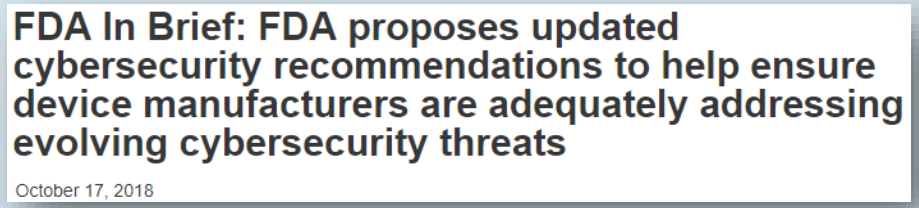
POLITICS

California governor signs country's first IoT security law

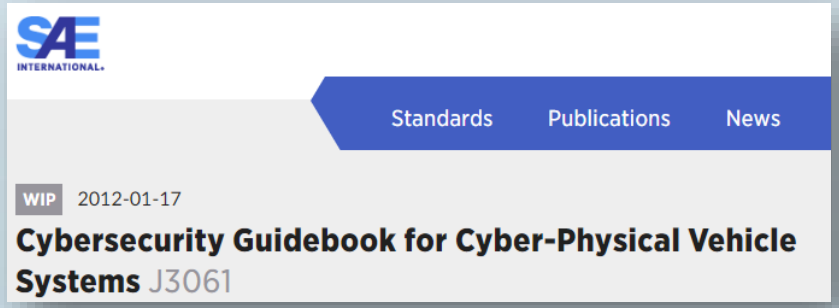
The new Internet of Things law calls for "reasonable" security features.


Network Working Group — K. Moore, Network Heretics
Internet-Draft — R. Barnes, Mozilla
Intended status: Best Current Practice — H. Tschofenig, ARM Limited
Expires: January 4, 2018 — July 3, 2017

Best Current Practices for Securing Internet of Things (IoT) Devices
draft-moore-iot-security-bcp-01


FDA In Brief: FDA proposes updated cybersecurity recommendations to help ensure device manufacturers are adequately addressing evolving cybersecurity threats

October 17, 2018


SAE INTERNATIONAL

Standards Publications News

WIP 2012-01-17

Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061

CSS is now:

KEYFACTOR

Trend 4: Cloud-First and Containerization

- Cloud IT
  - Enterprise PKI in the cloud is acceptable – and even preferred – by an increasing number of customers
- Cloud density of IT assets increases
- Impact on DevOps, DevSecOps
  - Certificate & key orchestration, securely – at scale

CSS is now:

KEYFACTOR

More Trends to Watch in 2019

- Cryptocurrencies & Blockchain
  - Is the recent coin crash just a “bump in the road”?
  - How intertwined are the fates of Blockchain and Cryptocurrencies?

- Data breach legislation
- IoT security legislation

Thank You

KEYFACTOR
SECURE EVERY DIGITAL IDENTITY

TED SHORTER

CHIEF TECHNOLOGY OFFICER

Ted.Shorter@keyfactor.com

About Keyfactor

Keyfactor, formerly Certified Security Solutions (CSS), is a leading provider of secure digital identity management solutions that enables organizations to confirm authenticity, and ensure the right things are interacting in the right ways in our connected world. Learn more at keyfactor.com

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?

Key cyber trends for 2019

Jim Rutt, CISSP, CISM, CISA, CGEIT, C|CISO, CRISC, CCSK

CIO, The Dana Foundation

My background

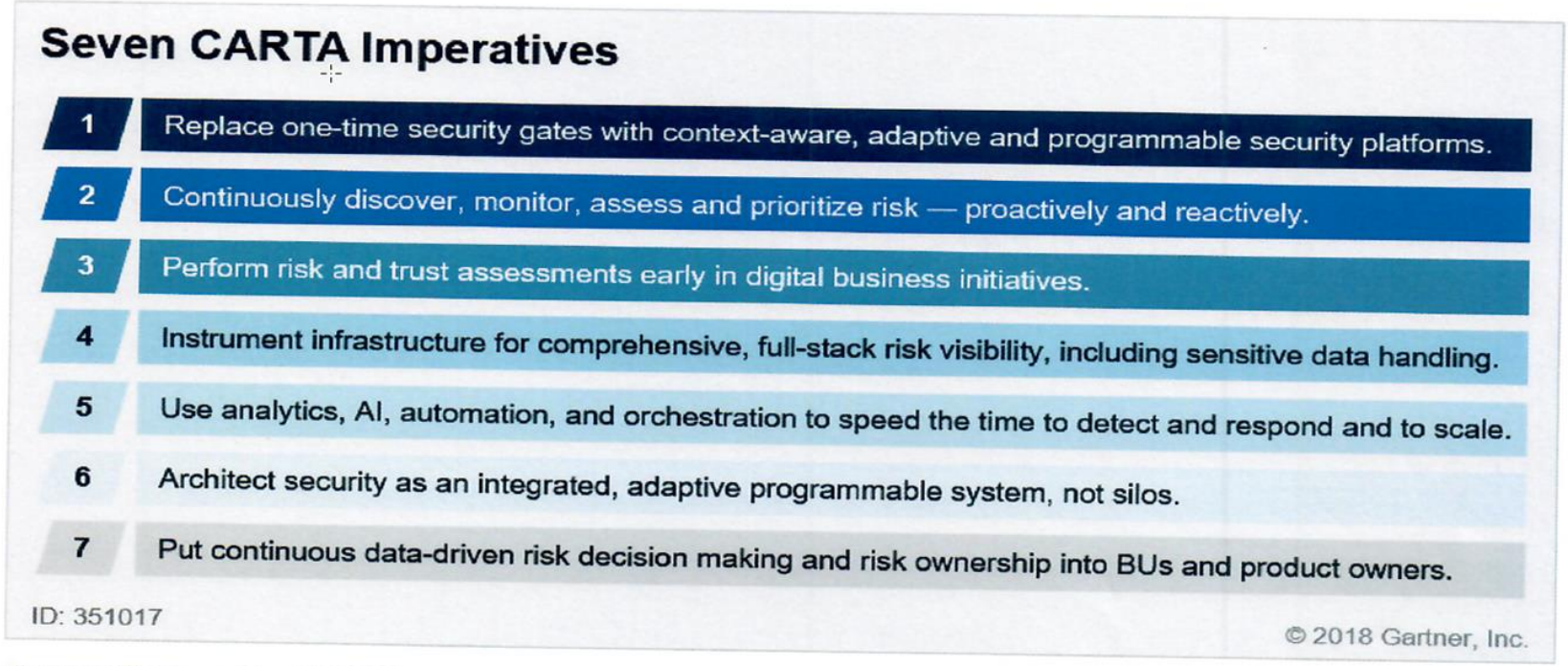
- CIO of the Dana Foundation
- President/Chairman of the Board of Technology Affinity Group (TAG)
- VP of the NY Metro Chapter of the Cloud Security Alliance
- Advisor to multiple VCs and dozens of startups

Key trends for 2019

- Zero Trust Networks/CARTA
- NaaS (Network as a Service)
- Rapid increase in use of SOAR
- CV (Computer Vision) supplementing End User Awareness
- Focused AI/ML as opposed to shotgun approach

CARTA (Continuous Adaptive Risk and Trust Assessment)

Figure 1. Seven CARTA Imperatives



Source: Gartner (April 2018)

Zero Trust Networking

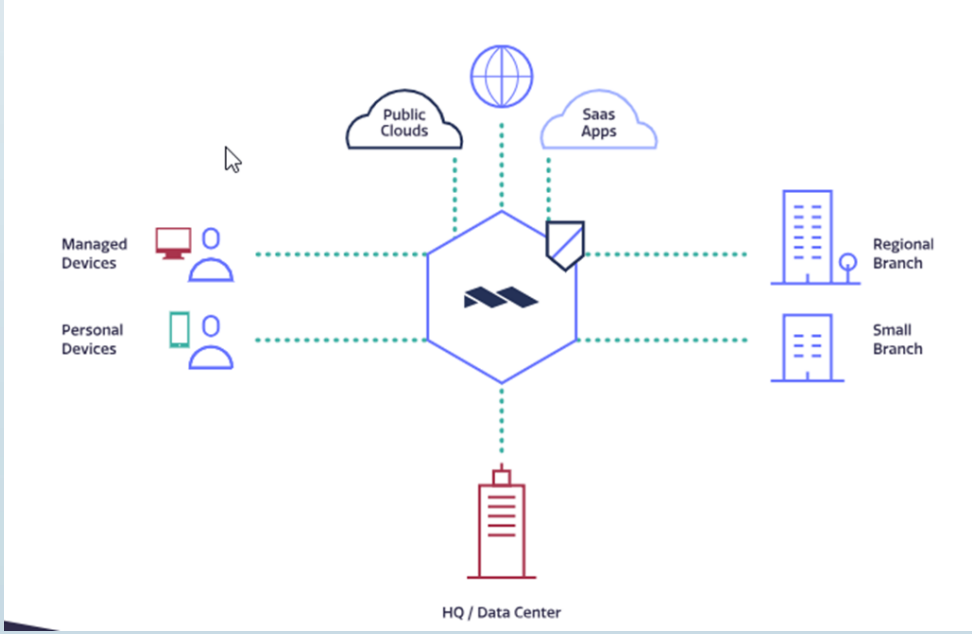
- Prevents lateral movement within networks
- One key driver is micro-segmentation
- Breaks away from traditional perimeter defense posture
- Assumes threat actors are already in proximity.

SOAR (Security Orchestrations, Analytics and Response)

- Use and expansion of use of SIEM (Security Incident and Event Management) to collect, correlate and analyze incidents
- Creation of incident workflows for rep
- Reduction of reliance on SOC analysts, who are hard to recruit and even harder to train
- One caveat: “chicken or egg” scenario where you need qualified staff to enable these platforms effectively

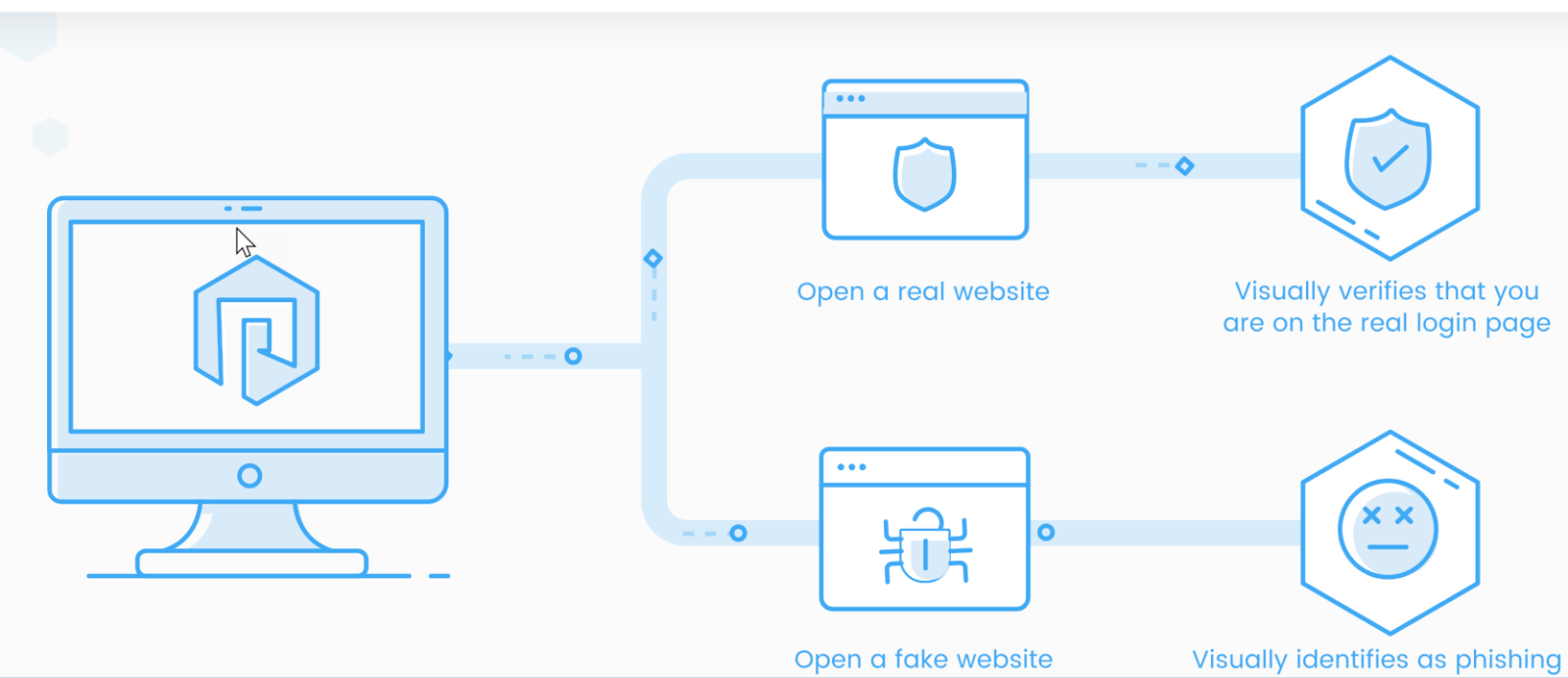
NaaS (Network as a Service)

- Enhances and enables zero-trust methodologies on the network side
- Focused on intelligent analysis of demarcation points at the application level, not just IP level
- Fits as a complement to the CARTA approach



CV (Computer Vision)

- The closest we can get to emulating true end user experiences, in order to mitigate social engineering wherever possible
- Practical application of Neural Networks
- Example: Pixm (antiphishing tool using CV)



AI/ML

- Apex of marketing hype
- Shotgun approach yields little differentiation
- What is marketed as AI may not truly be AI (“novel knowledge”)
- ML Use cases (Supervised and Unsupervised)*
  - Malware/spam classification
  - DNS Analytics
  - Threat Intelligence
  - UBEA

*”AI & ML in Cyber Security - Why Algorithms Are Dangerous”-Raffael Marty

Other general trends

- Increase in use of MFA
- Increase in use of Biometrics, despite common objections
- Focus on data protection in anticipation of wider adoption of GDPR-like regulations here in the US.

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?