Why Security and Privacy Shouldn’t be Enemies
Today’s Speakers

Avi Chesla – Founder & CEO, empow
• Cyber Security expert, speaker, author of over 30 patents.
• Previously CTO and VP of Security at Radware (NSDQ: RDWR) and CTO at V-Secure
• Brought Radware to market leadership in the attack mitigation space: from $0M into more than $100M annually, with over 5000 security customers

Aaron Baillio – Mgr. Security Operations and Architecture, University of Oklahoma
• Experienced professional with 15+ years in information technology, network design and cyber security.
• Spent over 10 years with the Department of Defense
Agenda

• The conflict
• Higher Ed. Security Challenges vs Privacy challenges
• Approaches & Principles to Follow
• About empow
The UNIVERSITY of OKLAHOMA

- Total Student Enrollment (Spring 2018) – **30,087**
  - Norman Campus – **24,217**
- Annual budget - **$942M**
- Carnegie Mellon R1 Doctoral University
  - **277** acre research campus
  - Ranked **#1** research campus in 2013
  - Research from Life Sciences to Robotics and Genomic Studies
  - National Weather Center – The nation’s premier weather research
SOONER SPORTS!

32 All Time National Championships in Men’s & Women’s Sports

3rd Softball Championship

Men’s and Women’s Gymnastics Championships

empow You have it in you.
The ability to hold two opposed ideas in the mind at the same time, and still retain the ability to function”

F. Scott Fitzgerald

Securing networks from attacks

Acting as zealous guardians of privacy

empow You have it in you.
The motivation behind cyber attacks

What they are after:

Operational data
- Academic research
- Courses & exams

Financial data:
- Tuition fees
- Students loans

Personally identifiable information (PII)

3rd party research data

Health & medical information
Security Challenges

Unmanaged Devices
Large and dynamic set of unmanaged BYOD devices.

Freedom of information
No restrictions for online traffic.

Lack of visibility
Little to no data governance & distributed IT.

Lack of proper network segmentation
As a result of remote, diversified, temporal, international staff and students.

The “experimental nature”
Frequent changes in security tools and the use of open source tools, creates a complex and cumbersome architecture.

SIEM misconfiguration
SIEMs require massive expert involvement, therefore are reactive, slow to respond and expensive.
The Challenge of Maintaining Privacy
Privacy VS Security
The challenges of monitoring privacy

- How do you protect the user from going into bad sites, while not exposing his/her browsing behavior?
- How do you protect the user from malware without looking into his/her emails and monitoring his/her web transactions?
- How do you inspect data without storing it?
- How do you do all this with minimal human touch?
Analyzing ALL the available information

**Affordability issues**
Analyzing all data can be expensive

**Slow to react**
Creates a “heavy” system that would be too slow to react.

**Privacy Regulations**
GDPR, HIPPA, PCI-DSS, FERPA

**Scalability issues**
Relying on access to all of the information creates scalability issues.

empow You have it in you.
Organizations in other verticals could have more strict security monitoring and controls
Approaches & Principles to Follow
How Privacy & Security Can Coexist

Introducing three principles:

1. Identify basic and advanced threats with “zero-human-touch” in the raw data

2. Use the existing “native” systems logs and storage... don’t duplicate

3. Choose solutions that can coordinate data visibility on a need to know basis
How Privacy & Security Can Coexist

Principle One:

Identify basic and advanced threats with “zero-human-touch” in the raw data

Understanding intent without reading the data using NLP algorithms

- Natural Language Processing - a field of artificial intelligence concerned with the interactions between computers and human (natural) languages

- NLP enables a machine to process structured and unstructured data and to get conclusions out of it
Alexa as a good example

Customer asks a question/gives a command

Alexa, how many centimeters are in 10 inches?

Customer hears the response from Alexa

10 inches is 25.4 centimeters

Alexa analyzes and understands the customer’s intent and processes the request

10 inches is 25.4 centimeters
Let’s use the same concept in security

What is the intent of W32.Ramint?

An analyst reads a security log and asks a question

W32. Ramint intent is to hijack online banking sessions, access and steal victim account info.

The analyst is provided with an answer

NLP-powered cybersecurity system understands the request, retrieves associated security research data, and processes it.

empow You have it in you.
Let’s use the same concept in security

What is the intent of W32.Ramint?

W32. Ramint intent is to hijack online banking sessions, access and steal victim account info.
Practical Use Cases

AI driven data analysis with virtually **zero human touch**

- Understand the Intent **the moment** you see the alert
- **Prioritize** intents according to your needs and assets
- Start **responding** the right away
- Plan the way you want to handle malwares with specific intent **in advance**
- Can be applied to **any kind of data**
- **Scale**
How Privacy & Security Can Coexist

Principle Two:

Use the existing “native” systems logs and storage... don’t duplicate

Cloud API logs
Flow stats logs
Application Logs
OS logs

Security tools

Logs infrastructure

Advanced logs repository and DB (e.g., Elastic Search)

Security Analytics

Results

• No need for additional storage
• Data minimization – keeps privacy
• Scalable and economical

empow You have it in you.
How Privacy & Security Can Coexist

Principle Three:

Choose solutions and systems that can coordinate data visibility on a need to know basis only, based on intent

- Show only the relevant data
- Coordinate the “tasks” per each
- Less exposure to privacy violation
Key Takeaways

Privacy and security can go hand in hand

Automate detection of attacks with “zero-human-touch” in the raw data
Maximize your existing, native, system logs - unlock the untapped power of your network infrastructure
Coordinate data visibility per need and risks

Don’t duplicate – Activate!

empow You have it in you.
Introducing empow
About empow

**APPROACH**
Maximize your investments – turn what you have into what you need

**SOLUTION**
NG SIEM: AI powered intent-based Security Orchestration.

**DNA & TEAM**
Data science, security professionals, SOC & incident response, software-defined and product strategy

**ADOPTION AND RECOGNITION**
Selected and deployed by several large customers in North America

**FORBES**
"...Replacing the security Tower of Babel of existing point solutions,..."

**Network World**
Breaking through the cybersecurity bubble

**FORBES**
Empow's unique approach listed among RSA 2017's four disruptive cyber trends.

---

**Oct. 2014**
Founded

$12M
Raised

2
Offices

15
Patents Filed. Core patent granted

Empow Cyber Security Ltd. Confidential
empow Next Generation SIEM

Deciphers the event intent

Machine Learning Classification Process

Inference analytics engine identifies attack intent

... and selects the best tool to execute it

Vendor attack DB

3rd party threat centers

Logs

Investigation Mitigation Remediation

... and selects the best tool to execute it
Customer Success Story

Cause-and-effect correlated attacks

Intent classification

High Risk risk-chains Insider and credential theft incidents

Attack Stories

Classified events

Logs

High: 7
Med: 64
Low: 6,317
Not relevant: 11,759

235,606,000
2,805,270
18,140
7

McAfee lastline paloalto Trend Micro Cisco

empow You have it in you.
Thank You.

Avi Chesla
avich@empownetworks.com
www.empownetworks.com

Aaron Baillio
abaillio@ou.edu

Meet us at upcoming events:

April 10-12, 2018
Baltimore

Booth: North Expo #3117