Trusted and Anonymized Threat Sharing Using Blockchain Technology

Dr. Yair Allouche
IBM Cyber Security Center of Excellence, Beer Sheva
Feb 19, 2019
Agenda

Blockchain hype cycle

Visibility

Source: Gartner
Agenda

- **Vision**: Next generation threat sharing network
- Current Barriers for Threat Sharing
- Blockchain-based threat sharing platform
- Summary and Q&A

**Blockchain hype cycle**

*Source: Gartner*
Vision: Next Generation Threat Sharing Network

- Global and flexible
- Trusted and reliable
- Automated and well integrated within existing workflow
- Built in anonymity
Vision: Next Generation Threat Sharing Network

- Global and flexible
- Trusted and reliable
- Automated and well integrated within existing workflow
- Built-in anonymity
Next Generation Threat Sharing Network, Example 1

SIEM network
Next Generation Threat Sharing Network, Example 1

SIEM network
Next Generation Threat Sharing Network, Example 1

SIEM network
Next Generation Threat Sharing Network, Example 1

SIEM network
Next Generation Threat Sharing Network, Example 1

SIEM network
Next Generation Threat Sharing Network, Example 1

SIEM network
Next Generation Threat Sharing Network, Example 1

SIEM network
• Leveraging **collective knowledge, experience, and capabilities**
Next Generation Threat Sharing Network, Example 2

Different views according to trust level
Next Generation Threat Sharing Network, Example 2

Different views according to trust level
Next Generation Threat Sharing Network, Example 2

Different views according to trust level
Current Barriers for Threat Sharing

(Source: NIST SP 800-150)

- Establishing **trust**
- Achieving **interoperability** and **automation**
- Safeguarding **sensitive info**
- Protecting **classified info**
- Enabling information **consumption** and **publication**

**Threat Sharing Today: What are the Trust Models?**

**Model 1:**
Trusted Third Party

**Model 2:**
Rely on Personal relationships
Why Blockchain

- Provides **anonymity** with **trust**
- **Enable dynamic** and **flexible** data exchange between any two organizations in the network
- Uses smart contracts to enforce data exchange agreement
- Automatic, objective and immutable audit of exchanged information
- Transparency
Our Approach

- Blockchain is used to supervise access management
- Cyber Threat Intelligence is exchanged on the chain
Our Approach

Org profile
• Issuer: I-Cert
• Role: CISO
• Sector: Finance
• Headquarter: New York
• FS-ISAC Member
• Splunk costumer
• Reputation score ....

Blockchain Network
Our Approach

**Consumption/ Sharing policy**
- Issuer white/black list
- Reputation higher than ...

Blockchain Network
Our Approach

**Consumption/ Sharing policy**
- ISAC members
- Geo white/blacklist
Our Approach

**Consumption/ Sharing policy**

- Splunk customers
- white/black list of user rule

Blockchain Network
Our Approach

- Consumer Consumption Policy
- Producer Profile
- Consumer Profile
- Producer Sharing Policy

Blockchain Network

CTI producer

CTI Consumer
Our Approach

Sharing policy
- Issuer white/black list
- Reputation higher than ...
Our Approach

Sharing policy
- ISAC members
- Geo white/blacklist

Blockchain Network
Our Approach

Sharing policy
- Splunk customers
- White/black list of user rule
Summary: The Next Generation Threat Sharing Platform

- Blockchain can provide real benefits for threat sharing
- Reaching a critical mass is the key challenge
- IBM is running pilots with several stakeholders
- Working with partners to promote the solution globally

Contact information: yair@il.ibm.com
THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2018. 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.