2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

HOW THREAT SHARING HONES YOUR COMPETITIVE EDGE

CYBER THREAT ALLIANCE

Michael Daniel
President and CEO

- It’s for the greater good
- The bad guys do it all the time, so the good guys should too
- It’s the right thing to do

Arguments for threat intelligence sharing rely on altruistic reasons.

THREAT SHARING IS EASY TO TALK ABOUT, BUT HARD TO DO IN PRACTICE

Even harder to do consistently at high quality and large scale

Really, really hard in the face of competitive pressures

CTA's sharing activities around WannaCry made the entire industry better off, but also directly helped our members

IMPEDIMENTS: WHAT MAKES SHARING HARD AND HOW TO OVERCOME THESE BARRIERS

WHAT MAKES THREAT SHARING SO HARD?

Five factors inhibit threat sharing:

Technical
Data volume, speed, and diversity pose problems

Economic
Hard to measure the ROI for sharing

Legal
Parameters for acceptable sharing can be unclear

Cultural
Sharing undercuts my business model

Conceptual
Threat sharing means different things to different people

WAYS TO OVERCOME THESE BARRIERS

Ways to move past the inhibitions:

Technical
Technical standards exist
Big data analytics common

Economic
Case studies show the benefits of sharing

Legal
US & EU have legal frameworks
Sharing organizations exist

Cultural
It's not what you know, but what you do with what you know

Conceptual
Different organizations share different information

- We have the tools to overcome the impediments but sharing remains ad hoc. Many do not engage it.
- Organizations must want to share for it to occur.
- If companies will not share based on altruism, what reason will motivate threat sharing?

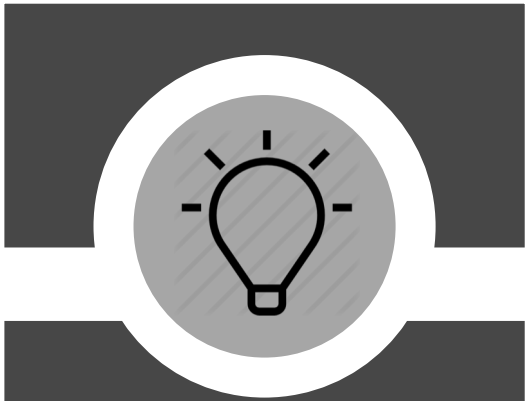
Competition

BEYOND ALTRUISM: THREAT SHARING MAKES A SECURITY PROVIDER MORE COMPETITIVE

HOW DOES THREAT SHARING ENHANCE YOUR COMPETITIVE EDGE?

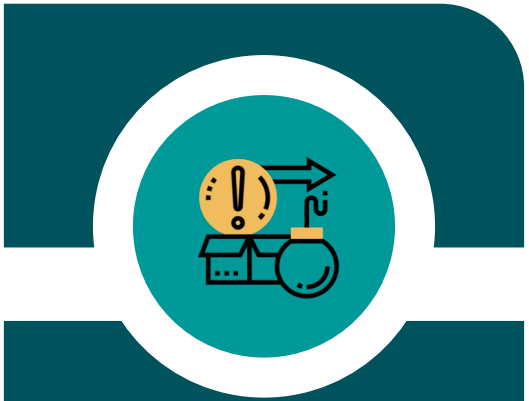
No single company sees all malicious activity

Every organization can learn something from sharing.



Regular sharing generates connections and ideas

Sharing forces you to defend your conclusions.



Exchanging business cards in a crisis is a bad idea

It builds the connections needed to deal with crises.

CYBER THREAT ALLIANCE

HOW DOES THREAT SHARING ENHANCE YOUR COMPETITIVE EDGE?

Cybersecurity is not just a technical problem

No organization has expertise in all the facets of cybersecurity.

Increased security comes from taking action

It's not what you know, but what you do with what you know.

End-users are demanding a team approach

Comparative advantage should drive what organizations do.

PRACTICING THE ART AND SCIENCE OF SHARING: HOW TO GET BETTER AT IT

- **Effective threat sharing requires answering three questions:**
  - Who is sharing?
  - What information are they sharing?
  - What purpose are they sharing it for?
- **The answers to these questions enable you to derive and identify the value you receive from sharing by:**
  - Focusing on relevant information
  - Aligning sharing goals with business needs
  - Tracking useful metrics to improve performance over time

Eight types of relevant information:

- ❑ Technical data
- ❑ Context
- ❑ Attribution
- ❑ Situational Awareness
- ❑ Strategic warning
- ❑ Tactical warning
- ❑ Best practices
- ❑ Defensive measures and mitigations

Five types of organizations:

1. Cybersecurity providers, platform providers, ISPs
2. Information sharing organizations
3. Large companies and organizations
4. National government agencies
5. Local government agencies, small and medium businesses, and individuals

MAKING SHARING WORK IN PRACTICE: LESSONS LEARNED FROM PREVIOUS SHARING

Automated sharing enhances outputs

Only way to achieve scope and scale

Situational threat sharing reduces the "fog of war"

Security community can get to the right answer much more quickly

Campaign threat sharing amplifies actions

Coordinated protections boost impact

Early sharing fills in gaps and enhances defenses

Recipients can put protections in place ahead of public release

Working Groups focus threat sharing on particular events or threats

Members use shared information to better disrupt malicious activity

Defensive measure threat sharing speeds up mitigation deployment

Customers are protected more quickly

- **Something is better than nothing**
  - Do not have to share everything for sharing to be useful
- **Automation is important for technical sharing**
  - Need speed and scale
- **Humans are important too**
  - People have to do something with the information
- **Sharing is hard work**
  - Technical parts can be challenging, but non-technical parts are more difficult

APPLYING THESE LESSONS IN THE REAL WORLD: CONCRETE STEPS TO IMPROVE SHARING

- **If your organization produces, collects, or provides threat intelligence:**
  - Analyze what you can share and what you could benefit from receiving
  - Join a formal threat sharing organization
  - Automate the technical intelligence sharing
- **If your organization consumes threat intelligence:**
  - Ask your vendors how they share threat intelligence across the industry
  - Ask your vendors to validate the intelligence they share with you
  - Make threat sharing an evaluation criterion in your cybersecurity contracts

- **If your organization shares threat intelligence amongst members:**
  - Update your business rules to encourage sharing
  - Focus on information types that fit your comparative advantage
  - Build relationships with other threat sharing organizations across sectors and geographic regions
- **If your organization is a national government agency:**
  - Articulate priorities clearly
  - Focus sharing with the private sector on your comparative advantage
  - Encourage cross-sector and international sharing

- **Translate sharing into action**
  - Identify specific actions for different parts of the ecosystem to take
  - Identify real/perceived barriers to action
  - Collaborate to systemically disrupt adversaries
- **Ensure policy and law supports sharing and collaboration activities**
  - Eliminate real or perceived barriers to sharing and collaboration
  - Create positive incentives for sharing and collaboration
  - Mitigate unintended consequences

- **Threat sharing makes a company more competitive**
  - No single company sees everything
  - A competitive edge comes from analysis not raw data
  - The benefits will vary depending on a company's business model
- **But threat sharing is hard work**
  - Cannot just turn on threat sharing
  - Requires on-going investment
  - Will not solve all security problems

ALIEN VAULT · Check Point SOFTWARE TECHNOLOGIES LTD. · CISCO · DRAGOS · Eleven Paths Telefónica CYBER SECURITY UNIT · FORTINET · INTSIGHTS · JUNIPER NETWORKS · K7 COMPUTING

lastline · McAfee · NEC · NETSCOUT · NTT · paloalto NETWORKS · panda · radware · RAPID7

REVERSING LABS · Scitum · SecureBrain A Hitachi Group Company · SK infosec · SONICWALL · SOPHOS · Symantec A Division of Broadcom · verizon

WE ARE THE CYBER THREAT ALLIANCE


2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音