Questioning The Clouds

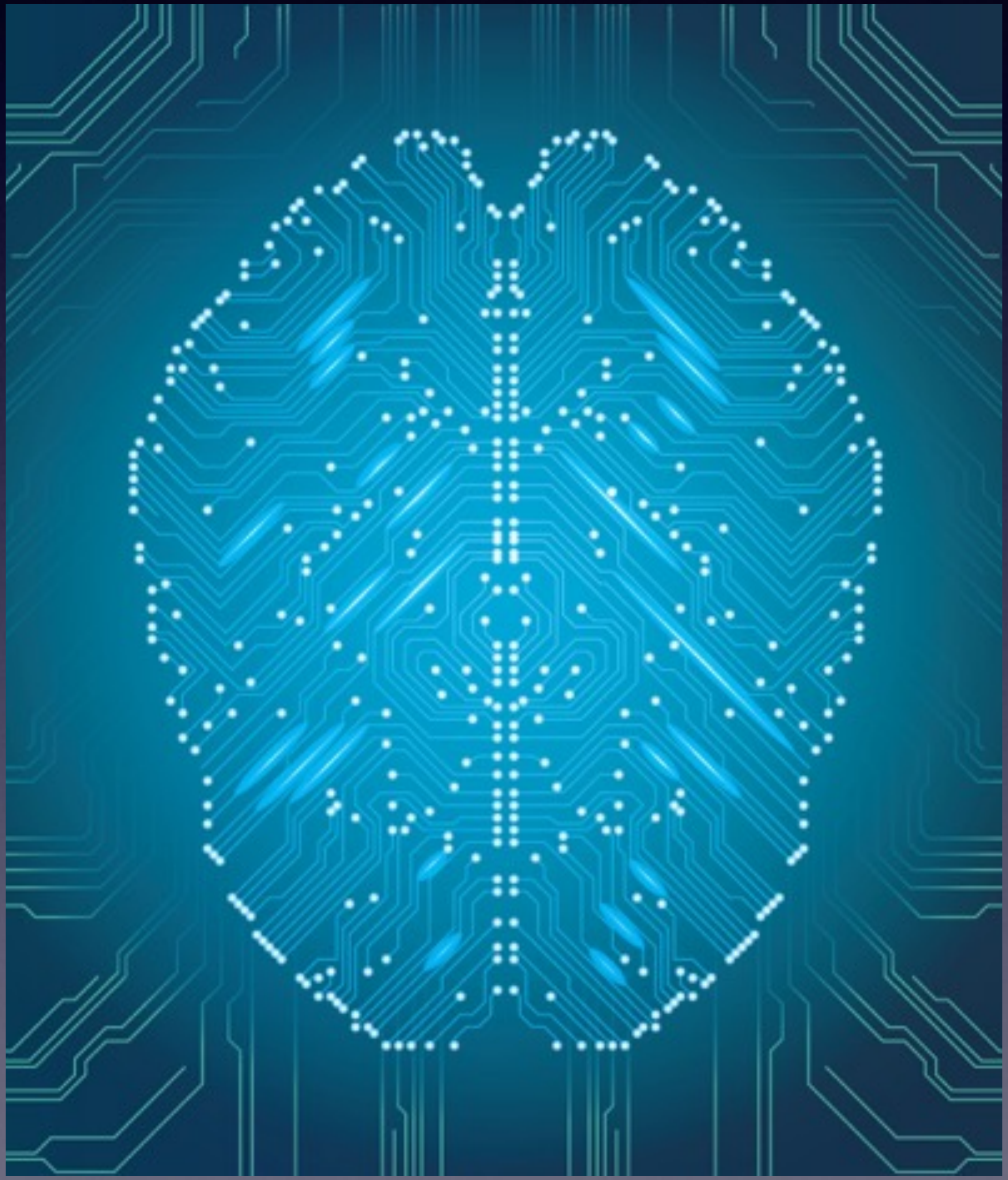
Rational Doubt In The Age Of Aggregated Computing

Brent Huston, Security Evangelist & CEO
@lbhuston

MSI MICROSOLVED, INC.

Ready, Set, What Happened?

- How I got here…
  - I ask A LOT of questions! :)
  - TigerTrax™ & "Cyber-Economics"
- Why am I here?
  - Insights from the front lines & from the adversary…
- What the heck is "the cloud" in this context?
  - Your stuff on other people's hardware…
- My alignment? "Chaotic good" when it comes to the cloud…



Obligatory Traditional Security Slide

- Talk to people who worked on mainframes to learn historic models *<PS: They love to be interviewed!>*
- Not going to cover Cloud Security Alliance - everyone knows this, right? :)
    - https://cloudsecurityalliance.org
    - Controls, best practices, standards, research
- Read, adopt, leverage the community, participate!

You’re Still Here? Good, Then Let’s Talk…

- Cloud providers are better at security, right?
    - Their ONLY focus is to provide network services for you?
    - Do they use their own environments? How do they segment, specifically? What controls do they consider critical?
- How complex are their network, application & management environments? Ask!
    - Complexity & security models are NOT friends…

Where Are The Cloud Breaches?

- Language matters…
  - "What's a cloud again?"
  - Hosting, backup providers, firmware, software, thousands of data services!!!
- A question of incentive?
- They're better at prevention & detection magic though, right?
- Does LinkedIn show the depth of talent pool needed to scale?

Questions Matter As Much As Answers

- **Lesson learned**: Ask for a clear, written, legal definition of these terms in your SLA.
  - Breach
  - Compromise
  - Incident
  - Investigation
  - Reporting
- It's all in how & whom you ask…

What Do Bad Guys Think?

- Always remember attacker asymmetry…
    - Risk/cost of attack vs ROI
        - Asymmetric returns & attacker value chains
- Data density creates an amplifier for asymmetry
- Make better risk decisions when you consider attacker economics

BackPlane :: A Common "Cloud" Threat We See Daily…

- Shared hosting of sites using DNS or content mapping
  - Your site(s), usually housed on same VM as many others, can also apply to separate VM & load balancing
  - Common cheap hosting, global footprint
- ***Your site is as (in)secure as least secure site on host***
- Impacts range from reputational, operational to breach of sensitive data
- Sometimes money instead of exploits - stolen credit cards work too! :/
- ***How do you decide on host allocation & placement? How do you monitor site content & behavior, specifically? Can you show us your site separation model, in detail?***

What Can I Do? It’s Their Hardware & Network!

- ***Obviously, risk assessment & vendor selection matter…***

- Generate & maintain EXCELLENT attack surface maps for all environments, especially cloud provided environments

- Create & actively maintain accurate threat models for all data, especially cloud lifted data, reconcile these with controls…

- Run periodic tabletop exercises where you practice & refine maps, models & processes - improve!

- Use targeted threat intelligence & passive assessments before selecting vendors & as an ongoing validation of their SLA requirements - *be wary of attestations & certifications…*

Thanks & More

- info@microsolved.com
- @lbhuston
- stateofsecurity.com & Podcast
- **“Don’t live in fear of the cloud. Focus on risk reduction. Ask the right questions.”**