RSAC Studio

CHANGE

Challenge today's security thinking

孫子兵法

Sun Tzu Meets the Cloud

Everything Is Different
Nothing Has Changed

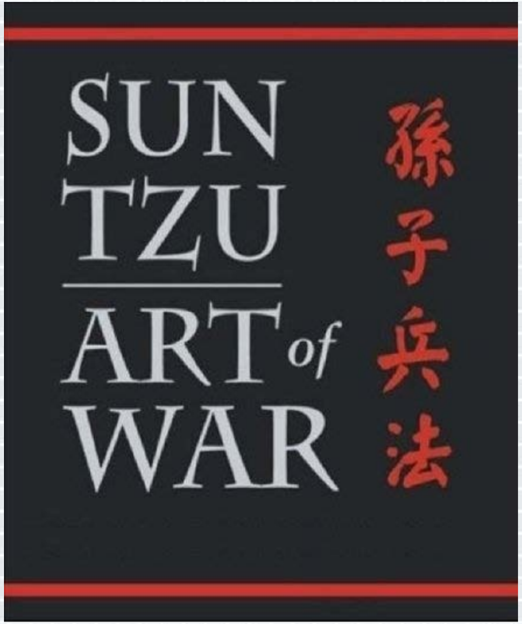
Sean Jennings, Co-founder & SVP Solutions Architecture EMEA & APAC

virtustream

@VCDX17 | @virtustream

#RSAC

Sun Who?



“The greatest victory is that which requires no battle.”

Everything is different…

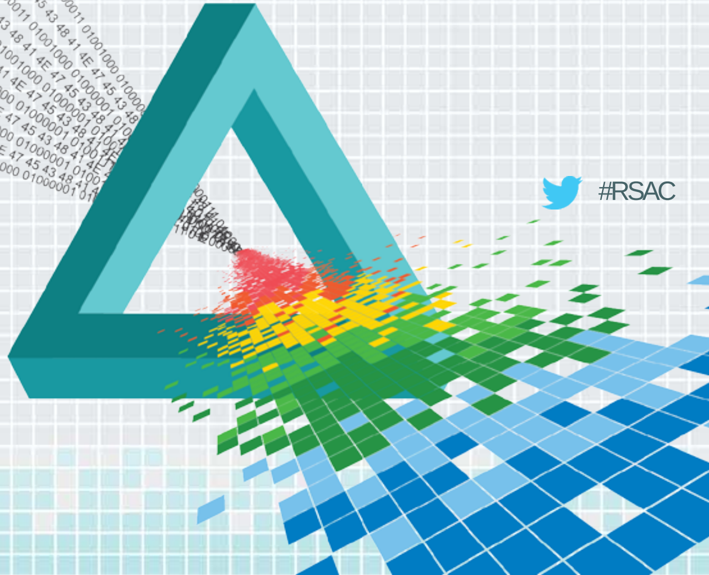
- The Perfect Storm: People, Process and Technology Changes
- Cloud has disintermediated IT from infrastructure being delivered
- Shadow IT has distributed Data & introduced unknown risks
- IT has become a broker responsible for vendor management
- Cloud’s main enabling technologies are it’s biggest vulnerabilities
- The “SDDC” complicates transparency & introduces new risk
- Exposure to “unknown unknowns” without automation

Nothing has changed

- Information has always been king, it just wasn't as plentiful
- Bad actors sought to steal data before the dawn of Mainframes
- Humans – mainly insiders – remain the weakest link in the chain
- Low cost distribution nearly always wins out
- Change is constant and continues to accelerate
- Convergence continues to blur lines of responsibility

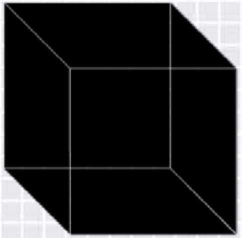
孫子兵法

“Know thy self, know thy enemy. A thousand battles, a thousand victories.”



Know thy self means know your providers

- Historically it was easy to know your computing estate
- Then servers became portable as Virtual Machines
  - VM Portability did to IT what the tank did to fortresses
- New insider threats enabled by the Hypervisor
  - Who are the CSP's Insiders? Who is watching them?
- How do I gain insight into the providers' risk & vulnerabilities?
- Transparency: How is the cloud audited and monitored?
- How do I to quantify and prioritize these risks? Ensure Compliance?



Know thy enemy – and discover risk

- Increased Surface Area and opportunity for attack without detection
- Thousands of Risks emerge each day across the IT Portfolio
  - How do I ensure my CSP is not at risk? And/or placing me at risk?
- Supply Chain Risks
  - Risk from compromised BIOS; Wholescale theft of systems
  - Chain of Custody & Data locality: where can systems and data run?
  - How secure is the Cloud Service Provider Portal?
- Transparency: How are emerging threats disclosed and reported?
- Which risks apply to my applications and how do I prioritize?

孫子兵法

“The wise general will use the highest intelligence of the army for the purposes of spying, and thereby they achieve great results.”

Become the enemy to defeat the enemy

“You can be sure of succeeding in your attacks if you only attack places which are undefended.”

- This is exactly what the attackers did in the Target POS breach
- Turn the Tables on the enemy with Cyber Situational Awareness
  - Use Continuous Monitoring to identify the undefended & OOC
  - Use Predictive Analytics & Big Data to find the vulnerabilities
  - Use Risk Scoring to prioritize the risks that must be addressed first
  - Then, fix them before they can be exploited by the enemy

RSAC® Studio

孫子兵法

“If ignorant both of your enemy and yourself, you are certain to be in peril.”

Apply: Know yourself, know your Cloud(s)

Next week, you should:

- Begin developing a plan for hardware attestation in Private Environments
- Query providers for committed attestation implementation dates

In the **next three months,** you should:

- Secure Provider commitments for transparent automated data feeds
- Begin deployment of comprehensive Continuous Monitoring toolset

Within six months, you should:

- Completely address all elements of transparency for risk monitoring
- Deploy Continuous Monitoring across all assets: cloud and on-premise

Apply: Know enemy, know your risk

Next week, you should:

- Identify critical cloud service(s) within your portfolio: Private & Public
- Establish a RACI for security ***and risk*** with your providers

In the **next three months,** you should:

- Investigate automated risk toolsets leveraging Continuous Monitoring
- Develop an understanding of where your blind spots are vis-à-vis risk

Within six months, you should:

- Be well into the deployment of your Automated Risk Management Toolset
- Begin to address newly identified risks

Thank You!

Talk to us, visit us, follow us…

Sean Jennings

Co-founder & SVP Solutions Architecture EMEA & APAC

Sean.Jennings@Virtustream.com | @VCDX17

virtustream®

www.virtustream.com | info@Virtustream.com | @Virtustream