

IT Security @Virginia Tech



Randy Marchany
VA Tech IT Security Office and Lab
marchany@vt.edu

Cybersecurity@VT

- IPV6 Research
 - Dual stack IPV4/IPV6 since 2005
 - Moving Target Defense (MT6D) –Patent pending
- Drones
 - Unmanned Systems Lab
 - IT Security Lab
- Mobile
 - Wireless@VT, ITSL,
- US Cyber Challenge Camp
 - Developed curriculum for USCC
- Cybersecurity Minor program
- Hume Center For Classified research

ITSL Teaching Hospital

- Critical National Need
 - Large # attacks, small # defenders
- Not enough to teach skills in class
- ITSO Teaching Hospital concept
 - Operational + Academic expertise
 - Analyze real data, make decisions, build tools
 - Cybercorps Scholarship for Service
 - Graduate, undergraduate working with analysts
 - Funnel skilled “residents” to jobs - Registry
 - Emphasis on Network Defense/Forensics

VT Cyber Security Strategy

- University has 3 main business processes
 - Academic, Administrative, Research
- Academic
 - Open access needed – THE ISP MODEL
- Administrative
 - Traditional corporate security model
- Research
 - Hybrid
 - Open access
 - Restricted research, e.g. ITAR

VT Cyber Security strategy must cover all 3 areas

VT Cyber Security Strategy

- Based on ISO 27002, NIST 800-53 Standards
- Implementing the 20 Critical Controls
- Continuous Monitoring based on NIST 800-137
- BYOD
 - All students required to purchase their own computers since 1984
- **Protect sensitive data regardless of location**
- Worry what leaves the net.

The awful truth

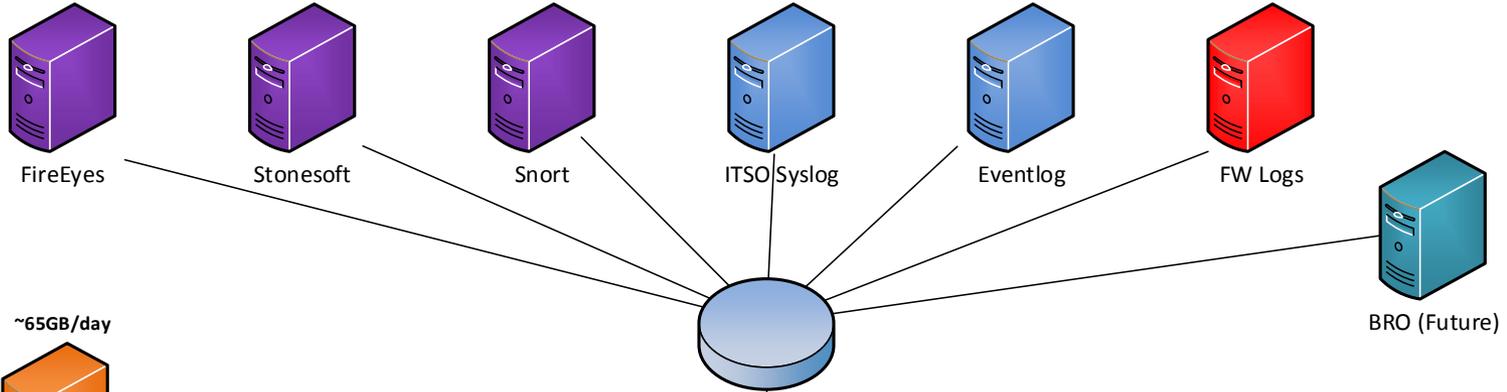
- Keeping someone from getting inside has failed miserably. [Why? Jimmy Kimmel knows!](#)
- Firewalls are not effective PROTECTION devices. They are effective DETECTION devices

Continuous Monitoring

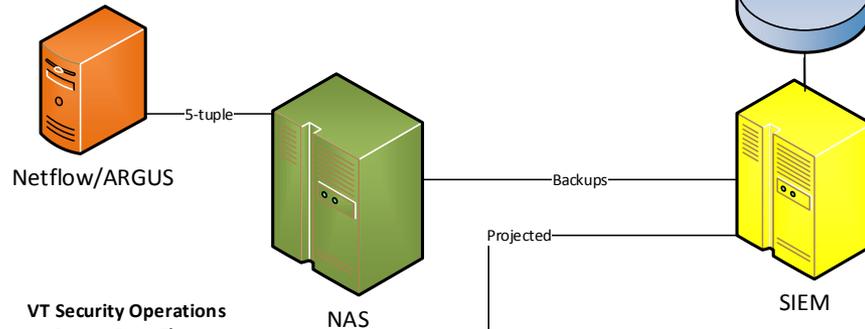
- Change the strategy
- Assume attackers are in so go hunt for the compromised hosts
- Monitor outbound traffic to interrupt their command and control communication
- Inbound monitors server side attacks; outbound monitors client side attacks

Continuous Monitoring Architecture

~50K events/day for most sensors



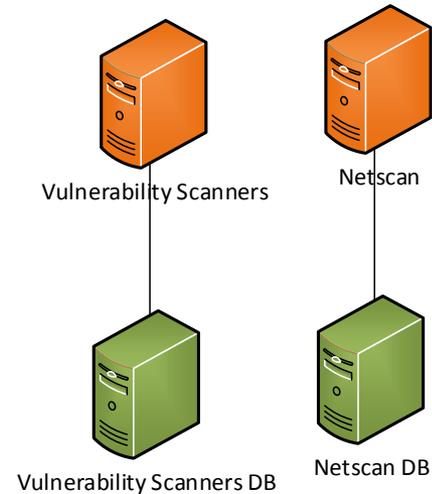
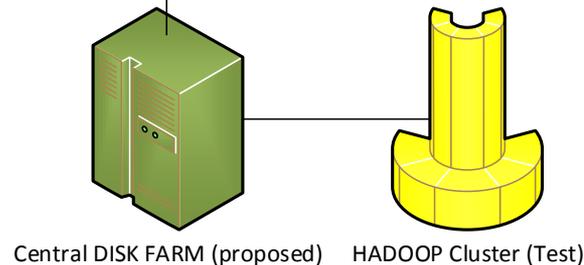
~65GB/day



VT Security Operations Center Data Flow 4/29/14

Color Codes:

- Blue – VT Network Sensors
- Red – RLAN only
- Purple – VT Network, NOVA and RLAN
- Green – disk storage
- Orange – ITSO "Silos"
- Yellow – Analysis Engines



RCM 8/9/2014

Thoughts on Metrics

- Metrics to answer these questions
 - Do you have this capability?
 - Forensic
 - How long does something take to occur?
 - How long has it been happening?
 - How widespread is it?
 - Ratio
 - What is leaving our net?
 - Compromised hosts vs. total hosts

Futures? The good

- Continuous monitoring increases the chances of successful detection and mitigation
- Can tailor defenses based on critical assets
 - find repeat offenders
 - create targeted training
- Provide justification for IT improvement
- Department and Enterprise staff, hardware, software, training
- Enhance university cybersecurity research

Contact Information

- Randy Marchany
- VA Tech IT Security Office & Lab
- 1300 Torgersen Hall
- Blacksburg, VA 24060
- 540-231-9523
- marchany@vt.edu
- <http://security.vt.edu> Twitter: @randymarchany
- <http://randymarchany.blogspot.com>