

About the VRT

- Founded in 2001
- 20 team members
 - ▶ Core team members based in Columbia, Maryland (USA)
 - ▶ Additional offices in Seattle, Poland, Italy and Germany



- Mission

- ▶ Provide intelligence and protection to allow our customers to focus on their core business



- Responsibilities:

- ▶ The public face of Sourcefire in the security community
 - ▶ Producing and publishing all Sourcefire, Snort, and ClamAV protection profiles
 - SEU, Snort, VDB, ClamAV
 - ▶ Threat Intelligence and Monitoring
 - ▶ ClamAV Development



Threat Intelligence

- Private Vulnerability Feeds
 - ▶ MAPP
 - ▶ Other 3rd Party (ISV's)
- Public Vulnerability Feeds
 - ▶ CVE, NIST, Secunia, Bugtraq, etc
- Malware and Virus Feeds
 - ▶ 30,000 evaluated daily
- OpenSource Reports
- Blacklists
- HoneyPots, BotFinders, WebCrawlers

Coverage Categories

- Vulnerabilities
 - Most comprehensive of any IPS Vendor
- BotNet
 - Command and Control
 - Infection remediation
- Client-Side
 - Adobe, Microsoft, Active-X
- SCADA
- VoIP
- Policy Enforcement