PROTECT 2011

POWERED BY HP ENTERPRISE SECURITY

CSN29: Application Log Monitoring for Today's Threat Landscape

Michael Malarkey
Vice President of Information Security
Forbes Top 5 Financial Organization

Tracy Barella
ArcSight Solutions Architect

Diversity of Logs = Broader View

- Web Server Logs
- DB Logs
- Authentication Logs

Connectors Galore

- FlexConnectors – File + Apache + IIS
- Be ready for some major Regex usage
- Regex Tool?

Use Cases

- OWASP Threats
- Which to implement monitoring for
- What logs are required for the various threats
- Long-term solutions

Process/Scalability

- Business Engagement
- Gaining access to logs
- Management Buy-in
- Audit Requirements

Questions?