SIEM AND THE ART OF LOG MANAGEMENT
PRESENTERS

Jeff Pold
- Director, Security Information Services, SpiderLabs Research
- 11 years on SIS
  - Intellitactics: 2004-2010
  - Trustwave: 2010-current

Ron Pettit
- SR. Security Specialist, Security Information Services, SpiderLabs Research
- 5 years on SIS
  - Trustwave: 2010-current
1 What is SIEM?
   • SIEM overview
   • The SIS Team

2 How to use SIEM effectively

3 SIEM management considerations
   • Self-managed SIEM
   • MSSP-managed SIEM
WHAT IS SIEM?
SIEM OVERVIEW

Security information and event management

- Collect, parse and normalize logs from various security devices
- Provide content to analyze parsed information
- Backup and long-term retention of logs
- Ensure compliance goals are met
WHERE DOES SIS COME IN?

Security Information Services

- Parsing/Normalization
  - Extract pertinent information
  - Normalize extracted values
  - Categorize/taxonomize events

- Content
  - Reports
  - Charts
  - Event searches
  - Alerts/notifications
  - Categorized lists
TRUSTWAVE SIEM

What do we support?

- SIEM products
  - SIEM log management appliances
  - SIEM Enterprise
  - MSS Managed SIEM
USING SIEM EFFECTIVELY
GET THE MOST FROM YOUR SIEM

Powerful tool when fully utilized

• Have a security plan
  – Zone your network
  – Decide what and where to monitor
  – Incidence response plan

• Monitoring vs. investigation
  – Trending via reports
  – Alerting on incidents
  – Investigating events
YOUR NETWORK ISN’T STATIC
And your SIEM shouldn’t be either

- Infrastructure Changes
  - Hardware replacements
  - Software updates
  - New services offered

- Personnel Factors
  - New employees
  - Elevated permissions

- External Factors
  - Malware threats
  - Unforeseen attacks
SPEC YOUR HARDWARE

Requirements may change over time

• Storage
  – Average events per day
  – Retention policy

• Processing Power
  – Events per second
  – Alerting timeliness

• High Availability
  – Failover
  – Data Backup
SELF-MANAGED SIEM
SELF-MANAGED SIEM

Monitor your own network

SIEM --> Network Security Devices

© 2015 Trustwave Holdings, Inc.
CHALLENGES OF SELF-MANAGED SIEM

• Building a team
  – Finding and retaining knowledgeable people

• Hardware cost
  – Initial build and ongoing maintenance

• Ramp-up time
  – Time from inception to production

• Using the SIEM
  – Configuration and monitoring
BENEFITS OF SELF-MANAGED SIEM

• You are in control
  – Only limited by your own resources

• Data doesn’t leave your site
  – You maintain ownership of your data

• Retain knowledge of your network
  – Learn your weak-points

• React quicker
  – Shorter communication times between onsite resources
MSSP-MANAGED SIEM
MSSP-MANAGED SIEM

Third-party monitoring

MSSP

SIEM

Collector

Your Network

Network Security Devices

© 2015 Trustwave Holdings, Inc.
CHALLENGES OF MSSP-MANAGED SIEM

- Externalizing your data
  - Must trust the MSSP with your logs
  - Geographic restrictions

- Reliance on outside intelligence
  - Potentially less involvement with your environment

- Time to alerts
  - More communication channels

- More generalized support
  - Potentially less customization options
BENEFITS OF MSSP-MANAGED SIEM

- Monitored by knowledgeable professionals
  - Recruiting and training not required
  - Observe and respond to global security trends
- Off-site backup of data
  - Your logs are protected off-site
- Latest SIEM technology
  - MSSP’s tend to use newest technologies
- Time to production
  - Standardized configuration procedures