Enterprise Security Monitoring

Comprehensive Intel-Driven Detection

PRESENTED BY: David J. Bianco
@DavidJBianco

BSIDES DC
20 OCTOBER, 2013
First there was…
Then there was…
Now there is...

Enterprise Security Monitoring (ESM)
Benefits of Enterprise Security Monitoring

- Increased visibility across the entire organization
- Get more value out of existing systems
- Data aggregation is “hunter friendly”
- Better organization around:
  - Detection platform coverage
  - Detection planning
    - General
    - Threat-specific
  - Prioritization of detection resources
- Quicker, more accurate incident detection and response
- Leverage your detection/response infra as an offensive capability
Intel Lifecycle

Research

Conclude

Analyze
Detection Process

- Observe
- Compare
- Validate
- Alert
Response Cycle

- Contain
- Remediate
- Investigate
Intel-Driven Operations Process

- Research
- Conclude
- Analyze

Indicators

- Observe
- Validate
- Compare
- Alert

Alerts

- Contain
- Remediate
- Investigate

Feedback

- Intel DB
- Detect DB
- Respond DB
Intel-Driven Detection

Enterprise Security Monitor

NSM / IDS

Detection Processing

Alerts & Queries

Analysts

Other Enterprise Data

Firewalls
Routers
Switches
OS Logs
App Logs
Proxy Logs
Web Logs
Antivirus
HIDS/HIPS
Corporate Data
(Employee DB, Travel, etc.)
A piece of information that points to a certain conclusion
What it is not
Common Indicator Data Types

- IPv4 Address
- Domain / FQDN
- Hash (MD5, SHA1)
- URL
- Transaction Element (User-Agent, MTA)
- File Name / Path
- Mutex
- Registry Value
- User Name
- Email Address
Indicator Characteristics

- **Extractable**: Can I find this indicator in my data?
- **Actionable**: If I find this indicator in my data, can I do something with that information?
- **Purposeful**: To what use will I put this indicator?
Indicator Purposes

**Attribution**
- Who/what is responsible for this activity?

**Detection**
- If this event happens, I want to know about it.

**Profiling**
- What are the targeting parameters for this threat?

**Prediction**
- Given the current state, what can I expect from this threat in the future?
“a systematic process to target and engage an adversary to create desired effects.”

Mandiant Attack Lifecycle Diagram

- Initial Recon
- Initial Compromise
- Establish Foothold
- Escalate Privileges
- Maintain Presence
- Move Laterally
- Internal Recon
- Complete Mission
The Pyramid of Pain

- **Tough!**
- **Challenging**
- **Annoying**
- **Simple**
- **Easy**
- **Trivial**

- **TTPs**
- **Tools**
- **Network/Host Artifacts**
- **Domain Names**
- **IP Addresses**
- **Hash Values**
I don’t have a cool name for this. “Bed of Nails”? 

Reconnaissance  Weaponization  Delivery  Exploitation  Installation  Command & Control (C2)  Actions on Objectives
What scenarios do we need to be able to detect?
What are our options for detecting them?
What are the strengths and weaknesses of our detection program today?
What is our detection stance against specific actors?
What is our overall plan for detection across our enterprise?
What scenarios do we need to be able to detect?

<table>
<thead>
<tr>
<th>Reconnaissance</th>
<th>Weaponization</th>
<th>Delivery</th>
<th>Exploitation</th>
<th>Installation</th>
<th>Command &amp; Control (C2)</th>
<th>Actions on Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>- File - Name</td>
<td>- Code - Binary Code</td>
<td>- Behavior</td>
<td>- Behavior</td>
<td>- Behavior</td>
<td>- Behavior</td>
<td>- Behavior</td>
</tr>
<tr>
<td>- File</td>
<td></td>
<td>- File - Full Path</td>
<td>- Win Registry Key</td>
<td>- Win Registry Key</td>
<td>- Win Process</td>
<td>- Win Registry Key</td>
</tr>
<tr>
<td>- URI - URL</td>
<td>- File - Name</td>
<td>- File</td>
<td>- File - Name</td>
<td>- File - Full Path</td>
<td>- File</td>
<td>- Win Registry Key</td>
</tr>
<tr>
<td>- HTTP - GET</td>
<td>- File</td>
<td>- URI - URL</td>
<td>- File</td>
<td>- File - Name</td>
<td>- URI - URL</td>
<td>- Win Registry Key</td>
</tr>
<tr>
<td>- URI - Domain Name</td>
<td>- URI - URL</td>
<td>- HTTP - POST</td>
<td>- File</td>
<td>- File - Path</td>
<td>- HTTP - POST</td>
<td>- Win Registry Key</td>
</tr>
<tr>
<td>- Address - e-mail</td>
<td>- Email Header - Subject</td>
<td>- Email Header - X-Mailer</td>
<td>- URI - Domain Name</td>
<td>- URI - Domain Name</td>
<td>- HTTP - GET</td>
<td>- Win Registry Key</td>
</tr>
<tr>
<td>- Address - ipv4-addr</td>
<td>- URI - Domain Name</td>
<td>- Hash - MD5</td>
<td>- Hash - SHA1</td>
<td>- Hash - MD5</td>
<td>- HTTP - User Agent String</td>
<td>- Win Registry Key</td>
</tr>
<tr>
<td></td>
<td>- Hash - MD5</td>
<td>- Hash - SHA1</td>
<td>- Address - cidr</td>
<td>- Hash - SHA1</td>
<td>- URI - Domain Name</td>
<td>- Win Registry Key</td>
</tr>
<tr>
<td></td>
<td>- Address - e-mail</td>
<td>- Address - ipv4-addr</td>
<td>- Address - ipv4-addr</td>
<td>- Address - ipv4-addr</td>
<td>- URI - Domain Name</td>
<td>- Win Registry Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Win Process</td>
<td>- Win Process</td>
<td>- Win Process</td>
<td>- Win Process</td>
<td>- Win Process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Win Registry Key</td>
<td>- Win Registry Key</td>
<td>- Win Registry Key</td>
<td>- Win Registry Key</td>
<td>- Win Registry Key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- File - Full Path</td>
<td>- File - Full Path</td>
<td>- File - Full Path</td>
<td>- File - Full Path</td>
<td>- File - Full Path</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- File</td>
<td>- File</td>
<td>- File</td>
<td>- File</td>
<td>- File</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HTTP - POST</td>
<td>- HTTP - POST</td>
<td>- HTTP - POST</td>
<td>- HTTP - POST</td>
<td>- HTTP - POST</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- HTTP - User Agent String</td>
<td>- HTTP - User Agent String</td>
<td>- HTTP - User Agent String</td>
<td>- HTTP - User Agent String</td>
<td>- HTTP - User Agent String</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- URI - Domain Name</td>
<td>- URI - Domain Name</td>
<td>- URI - Domain Name</td>
<td>- URI - Domain Name</td>
<td>- URI - Domain Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Hash - MD5</td>
<td>- Hash - MD5</td>
<td>- Hash - MD5</td>
<td>- Hash - MD5</td>
<td>- Hash - MD5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Hash - SHA1</td>
<td>- Hash - SHA1</td>
<td>- Hash - SHA1</td>
<td>- Hash - SHA1</td>
<td>- Hash - SHA1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Address - e-mail</td>
<td>- Address - e-mail</td>
<td>- Address - e-mail</td>
<td>- Address - e-mail</td>
<td>- Address - e-mail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Address - ipv4-addr</td>
<td>- Address - ipv4-addr</td>
<td>- Address - ipv4-addr</td>
<td>- Address - ipv4-addr</td>
<td>- Address - ipv4-addr</td>
</tr>
</tbody>
</table>
Detection Options - HIPS

Reconnaissance
- File - Name
- File
- URL
- HTTP - GET
- HTTP - User-Agent String
- URI - Domain Name
- Address - e-mail
- Address - IPv4-addr

Weaponization
- Code - Binary Code
- File
- File - Path
- URL

Delivery
- Behavior
- Win Registry Key
- File - Name
- File
- URI - URL
- HTTP - POST
- Email Header - Subject
- Email Header - X-Mailer
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - e-mail
- Address - IPv4-addr

Exploitation
- Behavior
- Win Registry Key
- File - Name
- File
- URI - URL
- Streetname - McAfee
- Streetname - Sophos
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - cidr
- Address - IPv4-addr

Installation
- Code - Binary Code
- Win Process
- Win Registry Key
- File - Full Path
- File - Name
- File
- File - Path
- URI - URL
- HTTP - GET
- HTTP - POST
- HTTP - User-Agent String
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - IPv4-addr

Command & Control (C2)
- Behavior
- Win Process
- Win Registry Key
- File
- URI - URL
- HTTP - GET
- HTTP - POST
- HTTP - User-Agent String
- URI - Domain Name
- Hash - MD5
- Address - e-mail
- Address - IPv4-addr

Actions on Objectives
- Behavior
- Win Registry Key
- Win Service
- File - Full Path
- File - Name
- File
- File - Path
- URI - URL
- Streetname - Sophos
- URI - Domain Name
- Hash - MD5
- Address - e-mail
- Address - IPv4-addr

Streetname - McAfee
Streetname - Sophos
Hash - SSDEEP
Address - e-mail
Address - IPv4-addr
## Detection Options - MIR

<table>
<thead>
<tr>
<th>Category</th>
<th>Detection Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaisance</td>
<td>- File - Name&lt;br/&gt;- File - URI&lt;br/&gt;- HTTP - GET&lt;br/&gt;- HTTP - User Agent String&lt;br/&gt;- URI - Domain Name&lt;br/&gt;- Address - e-mail&lt;br/&gt;- Address - ipv4-addr</td>
</tr>
<tr>
<td>Weaponization</td>
<td>- Code - Binary_Code&lt;br/&gt;- File&lt;br/&gt;- File - Path&lt;br/&gt;- URL - URL</td>
</tr>
<tr>
<td>Delivery</td>
<td>- Behavior&lt;br/&gt;- Win Registry Key&lt;br/&gt;- File - Name&lt;br/&gt;- File&lt;br/&gt;- URI - URL&lt;br/&gt;- HTTP - POST&lt;br/&gt;- Streetname - McAfee&lt;br/&gt;- Streetname - Sophos&lt;br/&gt;- URI - Domain Name&lt;br/&gt;- Hash - MD5&lt;br/&gt;- Hash - SHA1&lt;br/&gt;- Address - cidr&lt;br/&gt;- Address - ipv4-addr</td>
</tr>
<tr>
<td>Exploitation</td>
<td>- Behavior&lt;br/&gt;- Win Registry Key&lt;br/&gt;- File - Name&lt;br/&gt;- File&lt;br/&gt;- URI - URL&lt;br/&gt;- Streetname - McAfee&lt;br/&gt;- Streetname - Sophos&lt;br/&gt;- URI - Domain Name&lt;br/&gt;- Hash - MD5&lt;br/&gt;- Hash - SHA1&lt;br/&gt;- Address - cidr&lt;br/&gt;- Address - ipv4-addr</td>
</tr>
<tr>
<td>Command &amp; Control (C2)</td>
<td>- Behavior&lt;br/&gt;- Win Registry Key&lt;br/&gt;- Win Registry Key&lt;br/&gt;- File&lt;br/&gt;- URI - URL&lt;br/&gt;- HTTP - GET&lt;br/&gt;- HTTP - POST&lt;br/&gt;- HTTP - User Agent String&lt;br/&gt;- URI - Domain Name&lt;br/&gt;- Hash - MD5&lt;br/&gt;- Address - e-mail&lt;br/&gt;- Address - ipv4-addr</td>
</tr>
<tr>
<td>Actions on Objectives</td>
<td>- Behavior&lt;br/&gt;- Win Registry Key&lt;br/&gt;- Win Registry Key&lt;br/&gt;- File&lt;br/&gt;- File - Full Path&lt;br/&gt;- File - Name&lt;br/&gt;- File&lt;br/&gt;- File - Path&lt;br/&gt;- URI - URL&lt;br/&gt;- HTTP - GET&lt;br/&gt;- HTTP - POST&lt;br/&gt;- HTTP - User Agent String&lt;br/&gt;- URI - Domain Name&lt;br/&gt;- Hash - MD5&lt;br/&gt;- Hash - SHA1&lt;br/&gt;- Address - cidr&lt;br/&gt;- Address - ipv4-addr</td>
</tr>
</tbody>
</table>
## Detection Options – Email Gateway Logs

<table>
<thead>
<tr>
<th>Stage</th>
<th>Options</th>
</tr>
</thead>
</table>
| **Reconnaissance** | • File - Name  
• File  
• URI - URL  
• HTTP - GET  
• HTTP - User Agent String  
• URI - Domain Name  
• Address - e-mail  
• Address - ipv4-addr |
| **Weaponization** | • File - Name  
• File  
• URI - URL  
• HTTP - GET  
• HTTP - User Agent String  
• URI - Domain Name  
• Hash - MD5  
• Hash - SHA1  
• Address - e-mail  
• Address - ipv4-addr |
| **Delivery** | • Behavior  
• Win Registry Key  
• File - Name  
• File  
• URI - URL  
• HTTP - GET  
• URI - Domain Name  
• Hash - MD5  
• Hash - SHA1  
• Address - cidr  
• Address - ipv4-addr |
| **Exploitation** | • Behavior  
• Win Registry Key  
• File - Name  
• File  
• URI - URL  
• HTTP - GET  
• URI - Domain Name  
• Hash - MD5  
• Hash - SHA1  
• Hash - SSDEEP  
• Address - e-mail  
• Address - ipv4-addr |
| **Installation** | • Behavior  
• Win Registry Key  
• Win Process  
• File - Name  
• File  
• URI - URL  
• HTTP - GET  
• URI - Domain Name  
• Hash - MD5  
• Hash - SHA1  
• Hash - SHA1  
• Address - cidr  
• Address - ipv4-addr |
| **Command & Control (C2)** | • Behavior  
• Win Process  
• Win Registry Key  
• File - Name  
• File  
• URI - URL  
• HTTP - GET  
• URI - Domain Name  
• Hash - MD5  
• Hash - SHA1  
• Address - e-mail  
• Address - ipv4-addr |
| **Actions on Objectives** | • Behavior  
• Win Service  
• File - Name  
• File  
• URI - URL  
• HTTP - GET  
• URI - Domain Name  
• Hash - MD5  
• Hash - SHA1  
• Address - ipv4-addr |
## Score Card: Use of Available Indicators

<table>
<thead>
<tr>
<th>Category</th>
<th>Indicators</th>
</tr>
</thead>
</table>
| **Reconnaissance**        | • File - Name  
• File - Path  
• URI - URL  
• URI - Domain Name  
• Address - e-mail  
• Address - ipv4-addr |
| **Weaponization**         | • Code - Binary_Code  
• File  
• File - Path  
• URI - URL |
| **Delivery**              | • Behavior  
• File - Full Path  
• File - Name  
• File  
• URI - URL  
• HTTP - POST  
• Email Header - Subject  
• Email Header - X-Mailer  
• URI - Domain Name  
• Hash - MD5  
• Hash - SHA1  
• Address - e-mail  
• Address - ipv4-addr |
| **Exploitation**          | • Behavior  
• Win Registry Key  
• File - Name  
• File  
• URI - URL  
• Streetname - McAfee  
• Streetname - Sophos  
• URI - Domain Name  
• Hash - MD5  
• Hash - SHA1  
• Address - cidr  
• Address - ipv4-addr |
| **Installation**          | • Code - Binary_Code  
• Win Process  
• Win Registry Key  
• File - Full Path  
• File - Name  
• File  
• URI - URL  
• HTTP - GET  
• HTTP - POST  
• HTTP - User Agent String  
• URI - Domain Name  
• Hash - MD5  
• Address - e-mail  
• Address - ipv4-addr |
| **Command & Control (C2)**| • Behavior  
• Win Process  
• Win Registry Key  
• File  
• URI - URL  
• HTTP - GET  
• HTTP - POST  
• HTTP - User Agent String  
• URI - Domain Name  
• Hash - MD5  
• Address - e-mail  
• Address - ipv4-addr |
| **Actions on Objectives** | • Behavior  
• Win Registry Key  
• Win Service  
• File - Full Path  
• File - Name  
• File  
• File - Path  
• URI - URL  
• Streetname - Sophos  
• URI - Domain Name  
• Hash - MD5  
• Hash - SHA1  
• Address - ipv4-addr  
• Address - ipv4-addr |
Score Card: Pyramid Effectiveness of Indicators

Reconnaissance
- File - Name
- File
- URI - URL
- HTTP - GET
- HTTP - User Agent String
- URI - Domain Name
- Address - e-mail
- Address - ipv4-addr

Weaponization
- Code - Binary Code
- File
- File - Path
- URI - URL

Delivery
- Behavior
- File - Full Path
- File - Name
- File
- URI - URL
- HTTP - POST
- Email Header - Subject
- Email Header - X-Mailer
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - e-mail
- Address - ipv4-addr

Exploitation
- Behavior
- Win Registry Key
- File - Name
- File
- URI - URL
- Streetname - McAfee
- Streetname - Sophos
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - cidr
- Address - ipv4-addr

Installation
- Code - Binary Code
- Win Process
- Win Registry Key
- File - Full Path
- File - Name
- File
- URI - URL
- HTTP - GET
- HTTP - POST
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - cidr
- Address - ipv4-addr

Command & Control (C2)
- Behavior
- Win Process
- Win Registry Key
- File
- URI - URL
- HTTP - GET
- HTTP - POST
- HTTP - User Agent String
- URI - Domain Name
- Hash - MD5
- Address - e-mail
- Address - ipv4-addr

Actions on Objectives
- Behavior
- Win Registry Key
- Win Service
- File - Full Path
- File - Name
- File
- File - Path
- URI - URL
- Streetname - Sophos
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - ipv4-addr

© Mandiant Corporation. All rights reserved.
Score Card: Effectiveness Against APT-π

Reconnaissance
- URI – Domain Name
- Address - ipv4-addr
- Email Header - Subject
- Email Header - X-Mailer
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - e-mail
- Address - ipv4-addr

Weaponization
- Win Registry Key
- File - Name
- File
- URI - URL
- Streetname - McAfee
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - cidr
- Address - ipv4-addr

Delivery
- Code - Binary_Code
- Win Process
- Win Registry Key
- File - Full Path
- File - Name
- File
- File - Path
- URI - URL
- HTTP - GET
- HTTP - User Agent String
- Streetname - McAfee
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - ipv4-addr

Exploitation
- Behavior
- Win Process
- Win Registry Key
- File
- URI - URL
- HTTP - GET
- HTTP - POST
- HTTP - User Agent String
- URI - Domain Name
- Hash - MD5
- Address - e-mail
- Address - ipv4-addr

Installation
- Behavior
- Win Registry Key
- Win Service
- File - Full Path
- File - Name
- File
- File - Path
- URI - URL
- Streetname - Sophos
- URI - Domain Name
- Hash - MD5
- Hash - SHA1
- Address - ipv4-addr

Command & Control (C2)

Actions on Objectives
## Enterprise Detection Plan

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Reconnaissance</th>
<th>Weaponization</th>
<th>Delivery</th>
<th>Exploitation</th>
<th>Installation</th>
<th>C2</th>
<th>Actions on Intent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code - Binary_Code</td>
<td></td>
<td>Email GW</td>
<td>NONE</td>
<td></td>
<td></td>
<td>Short</td>
<td>HIPS</td>
</tr>
<tr>
<td>Win Process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>Win Registry Key</td>
<td></td>
<td>HIPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>Win Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>File - Full Path</td>
<td></td>
<td>Snort</td>
<td></td>
<td></td>
<td></td>
<td>Short</td>
<td>HIPS</td>
</tr>
<tr>
<td>File - Name</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>File - Path</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>URI - URL</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>HTTP - GET</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>HTTP - POST</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>HTTP - User Agent String</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>Email Header - String</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>Email Header - Subject</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>Email Header - X-Mailer</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>Email Header - Message-ID</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>Streetname - McAfee</td>
<td></td>
<td>HIPS</td>
<td></td>
<td>HIPS</td>
<td></td>
<td>Short</td>
<td>HIPS</td>
</tr>
<tr>
<td>Streetname - Sophos</td>
<td></td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>Short</td>
<td>HIPS</td>
</tr>
<tr>
<td>URI - Domain Name</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>Hash - MDS</td>
<td></td>
<td>Email GW</td>
<td>HIPS</td>
<td>HIPS</td>
<td></td>
<td>Short</td>
<td>HIPS</td>
</tr>
<tr>
<td>Hash - SHA1</td>
<td></td>
<td>Email GW</td>
<td>HIPS</td>
<td>HIPS</td>
<td></td>
<td>Short</td>
<td>HIPS</td>
</tr>
<tr>
<td>Hash - SSDEEP</td>
<td></td>
<td>NONE</td>
<td></td>
<td>NONE</td>
<td></td>
<td>Short</td>
<td>HIPS</td>
</tr>
<tr>
<td>Address - e-mail</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>Address - cidr</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>Address - ipv4-addr</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
<tr>
<td>Address - ipv6-addr</td>
<td></td>
<td>Snort</td>
<td>Email GW</td>
<td></td>
<td></td>
<td></td>
<td>HIPS</td>
</tr>
</tbody>
</table>
Summary

- NSM:IDS :: ESM:NSM
- Collect and aggregate across your entire enterprise
  - Increased visibility
  - Maximum use of resources
  - Better for “hunting”
- Organize intel for better program insights
- Big improvements in detection & response capabilities for minimal investment
- Smart detection makes for frustrated adversaries!
Questions?

David J. Bianco

David.Bianco@mandiant.com

@DavidJBIanco
detect-respond.blogspot.com

Please fill out your speaker evals!

Honest feedback is much appreciated

https://www.surveymonkey.com/s/BSidesDC13-Speaker