Outline

Anomaly Detection

Threat Detection

What to Monitor
Recall: Network Segmentation

In case not possible to clearly identify boundaries of zone;

- VLANs
  - Any broadcast domain that is partitioned and isolated in a computer network at the data link layer
- Next generation firewall for application layer segmentation
- Variable-length subnet masking (VLSM)
  - Enables network layer communication without layer 3 device
Recall: Implementing Network Security Controls

All inbound and outbound traffic must be forced through one or more known network connections that can be monitored and controlled.

One or more security devices must be placed in-line at each of these connections.

<table>
<thead>
<tr>
<th>Criticality</th>
<th>Required Security</th>
<th>Recommended Enhancements</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 (highest)</td>
<td>NRC CFR 73.54: Unidirectional Perimeter,</td>
<td>Application layer monitoring,</td>
</tr>
<tr>
<td></td>
<td>NERC CIP 005: Firewall or IDS or IPS</td>
<td>Firewall, IDS and IPS</td>
</tr>
<tr>
<td>3</td>
<td>NRC CFR 73.54: Unidirectional Perimeter,</td>
<td>Application layer monitoring,</td>
</tr>
<tr>
<td></td>
<td>NERC CIP 005: Firewall or IDS or IPS</td>
<td>Firewall, IDS and IPS</td>
</tr>
<tr>
<td>2</td>
<td>NERC CIP 005: Firewall or IDS or IPS</td>
<td>Firewall and IDS and IPS</td>
</tr>
<tr>
<td>1</td>
<td>NERC CIP 005: Firewall or IDS or IPS</td>
<td>Firewall and IDS</td>
</tr>
<tr>
<td>0 (lowest)</td>
<td>NERC CIP 005: Firewall or IDS or IPS</td>
<td>Firewall and IPS</td>
</tr>
</tbody>
</table>
Recall: Firewall Configuration Guidelines

Using a defined configuration policy

- Typically consisting of Accept (allow) and Drop (deny) statements

Most firewalls will enforce a configuration in sequence, such that starting with a broadly defined policy, such as Deny All, which will drop all inbound traffic by default

- These broad rules can then be overruled by subsequent, more focused rules
- Therefore, the following firewall policy would only allow a single IP address to communicate outside of the firewall on port 80 (HTTP)

```
Deny All
Allow 10.0.0.2 to Any Port 80
```
Recall: Intrusion Detection and Prevention (IDS/IPS) Configuration Guidelines

Rule functions different than firewall, only dropping traffic from the source address in question if the HTTP traffic contains a POST request (used by many web forms or applications attempting to upload a file to a web server over HTTP)

```
drop tcp 10.2.2.1 80 -> any any (msg: "drop http POST"; content: "POST");
```

Example usage:

```
drop tcp 10.2.2.1 80 -> 192.168.1.1 80 (flags: <optional short flags>; msg: "<message text>"); content: "<this is what the rule is looking for>"; reference: "<reference to external threat source>");
```
Recall: Cautions for IDS/IPS Implementation

A false positive (a rule that triggers in response to unintended traffic, typically due to imprecisions in the detection signature) can block legitimate traffic and in a control system legitimate traffic could represent a necessary operational control

- Only use block IPS rules where absolutely necessary, and only after extensive testing

IDS and IPS signatures are only able to block known threats, meaning that the IDS/IPS policy must be kept current in order to detect more recently identified attacks (virus, exploits, etc.)

- IDS/IPS products must be included within the overall Patch Management Strategy in order for the devices to remain effective
Recall: Application and Protocol Monitoring in Industrial Networks

Many industrial operations are controlled using specialized industrial network protocols that issue commands, read and write data, etc. using defined function codes.

- Specialized devices can leverage that understanding along with Firewall, IDS, and IPS technology to enforce communications based on the specific operations being performed across the network.

In addition to the inspection of industrial protocol contents (e.g., DNP3 function codes), the applications themselves can also be inspected.

- Application Monitors provide a very broad and very deep look into how network traffic is being used.
- Useful in environments where both control systems and enterprise protocols and applications are in use.
Host Security and Access Controls

Host firewalls, Host IDS, Anti-virus, Application Whitelisting

All host access control and network security solutions should be implemented on all networked devices

- Not all devices capable of running such software
- Additional delay
- Some ICS vendors began to offer security features for embedded devices (i.e., Siemens S7-400 PLC)
Exception Reporting

Expect one behavior but see another -> potential threat

Exception reporting looks at all behaviors

- Unlike a hard policy defined at an enclave perimeter, which makes black-and-white decisions about what is good and bad, exception reporting can detect suspicious activities by compiling a wealth of seemingly benign security events
- Can be automated using many log analysis or security information management systems

Without an understanding of the policies that are in place, however, exceptions cannot be determined
## Suspicious Activity Examples

<table>
<thead>
<tr>
<th>Exception</th>
<th>Policy being Enforced</th>
<th>Detected by</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>A network flow originates from a different enclave than the destination IP address</td>
<td>Network separation of functional groups/enclaves</td>
<td>Firewall, Network Monitor, Network IDS/IPS, etc. using $Enclave_IP variables</td>
<td>Alert only, to create a report on inter-enclave communications</td>
</tr>
<tr>
<td>Network traffic originating from foreign IP addresses is seen within a secured enclave</td>
<td>Isolation of critical enclaves from the Internet</td>
<td>Log Manager/Analyzer, SIEM, etc., correlating $Enclave_IP variables and geolocation data</td>
<td>Critical Alert to indicate possible penetration of a secure enclave</td>
</tr>
<tr>
<td>An authorized user accessing the network from a new or different IP address</td>
<td>User access control policies</td>
<td>Log Manager/Analyzer, SIEM, etc., correlating $Enclave_IP variables to user authentication activity</td>
<td>Alert only, to create a report on abnormal administrator activity</td>
</tr>
<tr>
<td>An unauthorized user performing administrator functions</td>
<td>User access control policies</td>
<td>Log Manager/Analyzer, SIEM, etc., correlating $Admin_users variables to application activity</td>
<td>Critical Alert to indicate potential unauthorized privilege escalation</td>
</tr>
<tr>
<td>An industrial protocol is used in nonindustrial enclaves</td>
<td>Network separation of functional groups by protocol</td>
<td>Network Monitor, Network IDS/IPS, Application Monitor, Industrial Protocol Monitor, etc. using $Enclave_Protocol variables</td>
<td>Alert only, to create a report of abnormal protocol use</td>
</tr>
<tr>
<td>Write function codes are used outside of normal business hours</td>
<td>Administrative control policies</td>
<td>Application monitoring detects $Modbus_Administrator_Functions IDENTITY or authentication systems indicate normal administrative shifts</td>
<td>Alert only, to create an audit trail of unexpected admin behavior</td>
</tr>
<tr>
<td>Write function codes are originating from a device authenticated to a nonadministrative user</td>
<td>User access control policies</td>
<td>Application monitoring detects $Modbus_Administrator_Functions Authentication logs indicate a nonadministrative user</td>
<td>Critical Alert to indicate possible insider threat or sabotage</td>
</tr>
<tr>
<td>Application monitoring detects $Modbus_Administrator_Functions Authentication logs indicate a nonadministrative user</td>
<td>Application monitoring detects $Modbus_Administrator_Functions Authentication logs indicate a nonadministrative user</td>
<td>Critical Alert to indicate possible insider threat or sabotage</td>
<td></td>
</tr>
</tbody>
</table>
Behavioral Anomaly Detection

Anomalies can be detected by comparing monitored behavior against known “normal” values

- Cannot be detected without an established baseline of activity to compare against

Manually:
- Based on real-time monitoring or log review

Automated:
- Using a Network Behavior Anomaly Detection (NBAD) product, Log Analysis, or Security Information and Event Management (SIEM) tool
Measuring Baselines

Time-lagged calculations based on running averages

Provide a basis (base) for comparison against an expected value (line)

Useful for comparing past behaviors to current behaviors, but can also be used to measure network or application capacity, or any other operational metric that can be tracked over time

Should not be confused with a trend analysis

- Baseline is a value: nothing more, nothing less
- Trend analysis; a forward-looking application of known baselines to predict the continuation of observed trends
Example of One Year’s Data per Month

Is this useful?

For security context, little value

- Assume: 59,421,102 events over 30 days and 1,980,703 events per day average
- Daily 2m event is meaningful or not?
Corrected Example

Useful of observed activity within relevant contexts of time

- Essentially providing historical context to baseline averages

Spike in activity on Thursday might be seen as an anomaly and spur an extensive security analysis, rather than being clearly indicated as normal behavior

- There may be scheduled operations at the beginning of every month, at specific times of the day, or seasonally, causing expected changes in event volumes
## Measurement and Analysis of Baseline Metrics

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Measured Metric(s)</th>
<th>Measured by</th>
<th>Analyzed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Traffic</td>
<td>• Total unique Source IPs &lt;br&gt; • Total unique Destination IPs &lt;br&gt; • Total unique TCP/UDP ports &lt;br&gt; • Traffic Volume (total flows) &lt;br&gt; • Traffic Volume (total bytes) &lt;br&gt; • Flow duration</td>
<td>• Network switch/router flow logs (i.e., netFlow, jFlow, sFlow, or similar) &lt;br&gt; • Network probe (i.e., IDS/IPS, network monitor, etc.)</td>
<td>• Network Behavior Anomaly Detection (NBAD) system &lt;br&gt; • Log Management system &lt;br&gt; • SIEM system</td>
</tr>
<tr>
<td>User Activity</td>
<td>• Total unique active users &lt;br&gt; • Total logons &lt;br&gt; • Total logoffs &lt;br&gt; • Logons by user &lt;br&gt; • Logoffs by user &lt;br&gt; • Activity (e.g., configuration changes) by user</td>
<td>• Application Logs &lt;br&gt; • Database logs and/or transaction analysis &lt;br&gt; • Application logs and/or session analysis &lt;br&gt; • Centralized authentication (LDAP, Active Directory, IAM)</td>
<td>• Log Management system &lt;br&gt; • SIEM system &lt;br&gt; <strong>NOTE:</strong> user activity may need additional layers of correlation to consolidate multiple usernames/accounts associated with a single user</td>
</tr>
<tr>
<td>Process/Control Behavior</td>
<td>• Total unique function codes &lt;br&gt; • Total number per individual function code &lt;br&gt; • Total set point or other configuration changes</td>
<td>• Industrial Protocol Monitor &lt;br&gt; • Application Monitor &lt;br&gt; • Data Historian tags</td>
<td>• Data Historian &lt;br&gt; • SIEM System</td>
</tr>
<tr>
<td>Event/Incident Activity</td>
<td>• Total events &lt;br&gt; • Total events by criticality/severity &lt;br&gt; • Total events by security device</td>
<td>• Security device (i.e., firewall, IPS) logs</td>
<td>• Application Monitor &lt;br&gt; • Industrial Protocol Filter</td>
</tr>
</tbody>
</table>
Examples of Suspicious Anomalies

<table>
<thead>
<tr>
<th>Normal Behavior</th>
<th>Anomaly</th>
<th>Detected By</th>
<th>Indication</th>
</tr>
</thead>
</table>
| All Modbus communications to a group of PLCs originates from the same three HMI workstations | A fourth system communicates to the PLCs | A >20% increase in the number of unique source IP addresses, from analysis of:  
- Network flows  
- Security event logs from firewalls, IFS devices, etc.  
- Application logs  
- Etc. | A new, unauthorized device has been plugged into the network (e.g., an administrator's laptop)  
A rogue HMI is running using a spoofed IP address  
A new system was installed and brought online |
| Every device has a single MAC address and a single IP address | An IP address is seen originating from two or more distinct MAC addresses | >1 MAC Addresses per IP, from analysis of:  
- Network flows  
- Security event logs from firewalls, IFS devices, etc.  
- Application logs  
- Etc. | An attacker is spoofing an address  
A device has failed and been replaced with new hardware |
| A process within a Control System enclave is running a consistent control loop for extended periods | Traffic increases above expected volumes | A >20% increase in the total network traffic, in bytes, from analysis of network flows | An unauthorized service is running  
A scan or pen test is being run  
A shift change is underway  
A new batch or process has started |
| Traffic decreases below expected levels | A >20% decrease in the total network traffic, in bytes, from analysis of network flows | A service has stopped running  
A networked device has failed or is offline  
A batch or process has completed |
Examples of Suspicious Anomalies

<table>
<thead>
<tr>
<th>Normal Behavior</th>
<th>Anomaly</th>
<th>Detected By</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changes to Programmable Logic</td>
<td>Industrial network monitor such as a SCADA IDS Ladder Logic/Code Review</td>
<td>Any variation in the individual function codes and/or frequency of any function code, from analysis of: Industrial Protocol Monitors, Application Monitors, SCADA IDS/IPS logs</td>
<td>A process has been altered, A new process has been implemented, An old process has been removed, A process has been sabotaged</td>
</tr>
<tr>
<td>Authorized Users log on to common systems at the beginning of a shift</td>
<td>Unauthorized user logs on to a system normally accessed by administrators only</td>
<td>Any variation seen from analysis of authentication logs from: Active Directory Operating System logs, Application Logs</td>
<td>Personnel changes have been made, An administrator is on leave or absent and duties have been delegated to another user, A rogue user has authenticated to the system, An administrator account has been compromised and is in use by an attacker</td>
</tr>
</tbody>
</table>
Behavioral Whitelisting

User Whitelists

- Locking critical functions to administrative personnel

Asset Whitelists

- Authorized devices can be used to whitelist known good network devices

Application Behavior Whitelists

- Can be whitelisted per host
Some examples of application behavior whitelisting

Only “read-only” function codes are allowed

Master PDUs or Datagrams are only allowed from predefined assets

Only specifically defined function codes are allowed

Write commands are only allowed in native fieldbus protocols and not over TCP/IP

HMI applications in supervisor networks are only allowed to use read functions over TCP/IP-based protocols
Examples of Behavioral Whitelists

<table>
<thead>
<tr>
<th>Whitelist</th>
<th>Built Using</th>
<th>Enforced Using</th>
<th>Indications of a Violation</th>
</tr>
</thead>
</table>
| Authorized devices by IP | • Network monitor or probe (such as a Network IDS)  
• Network scan | • Firewall  
• Network Monitor  
• Network IDS/IPS | A rogue device is in use |
| Authorized applications by port | • Vulnerability assessment results  
• Port scan | • Firewall  
• Network IDS/IPS  
• Application Flow Monitor | A rogue application is in use |
| Authorized applications by content | | • Application Monitor | An application is being used outside of policy |
| Authorized Function Codes/Commands | • Industrial network monitor such as a SCADA IDS  
• Ladder Logic/Code Review | • Application Monitor  
• Industrial Protocol Monitor | A process is being manipulated outside of policy |
| Authorized Users | • Directory Services  
• IAM | • Access Control  
• Application Log Analysis  
• Application Monitoring | A rogue account is in use |
Threat Detection

For the detection of an incident (vs. a discrete event), it is, therefore, necessary to look at multiple events together and search for larger patterns.

- Even simple attacks consist of multiple steps.

Event Correlation

- Simplifies the threat detection process by making sense of the massive amounts of discrete event data, analyzing it as a whole to find the important patterns and incidents that require immediate attention.

- Events are collected from many types of information sources, such as firewalls, switches, authentication servers, etc.
Event Correlation

Events are compared against a defined set of known threat patterns or “correlation rules”

- If there is a match, an entry is made in a (typically) memory-resident state tree; if another sequence in the pattern is seen, the rule progresses until a complete match is determined
- For example, if a log matches the first condition of a rule, a new entry is made in the state tree, indicating that the first condition of a rule has been met

As more logs are assessed, there may be a match for a subsequent condition of an existing branch, at which point that branch is extended

A log may meet more than one condition of more than one rule, creating large and complex state trees
- For example, simple “brute force attack” rule can create several unique branches
Event
Correlation

1. Logs are examined in real time

2. If the log matches the condition of a rule, an entry is made in the state tree

3. As new conditions are met, the state tree grows until all of the conditions of a rule are met, or the branch times out.
## Example Event Correlation Rules

<table>
<thead>
<tr>
<th>Threat Pattern</th>
<th>Description</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brute Force Attack</td>
<td>Passwords are guessed randomly in quick succession in order to crack the password of a known user account.</td>
<td>A number $N$ of Failed Logon events, followed by one or more Successful Logon events, from the same Source IP.</td>
</tr>
<tr>
<td>Outbound Spambot behavior</td>
<td>A spambot (malware designed to send spam from the infected computer) is sending bulk unsolicited e-mails to outside addresses.</td>
<td>A large number $N$ of Outbound SMTP events, from one internal IP Address, each destined to a unique e-mail address.</td>
</tr>
<tr>
<td>HTTP Command and Control</td>
<td>A hidden communication channel inside of HTTP is used as a command and control channel for malware.</td>
<td>HTTP traffic is originating from servers that are not HTTP servers.</td>
</tr>
<tr>
<td>Covert botnet, command, and control</td>
<td>A distributed network of malware establishing covert communications channels over applications that are otherwise allowed by firewall or IPS policy.</td>
<td>Traffic originating from $N$ number of $&amp;\text{ControlSystem}<em>{\text{Enclave01_Devices}}$ to $&amp;\text{ControlSystem}</em>{\text{Enclave01_Devices}}$ with contents containing Base64 coding.</td>
</tr>
</tbody>
</table>
Data Enrichment

Process of appending or otherwise enhancing collected data with relevant context obtained from additional sources

- If a username is found within an application log, that username can be referenced against a central Identity system to obtain the user’s actual name, departmental roles, privileges, etc.
- Additional information “enriches” the original log with this context

Primary way

- By performing lookup at the time of collection and appending the contextual information into the log
Normalization

Classification system, which categorizes events according to a defined taxonomy.

Way the message is depicted varies sufficiently that without a compensating measure such as event normalization, a correlation rule looking for “logons” would need to explicitly define each known logon format.

<table>
<thead>
<tr>
<th>Log Source</th>
<th>Log Contents</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Router</td>
<td><code>&lt;57&gt; Dec 25 00:04:32: %SECLOGIN-5-LOGIN_SUCCESS: Login Success [user: jdoe] [Source:10.4.2.11] [Local]port:23] at 20:55:40 UTC Fri Feb 28 2006</code></td>
<td>Successful Logon</td>
</tr>
<tr>
<td>Redhat Linux</td>
<td><code>&lt;122&gt; Mar 4 09:23:15 localhost sshd[27577]: Accepted password for jdoe from ::ffff:192.168.138.35 port 2895 ssh2</code></td>
<td>Successful Logon</td>
</tr>
</tbody>
</table>
Cross-source Correlation

Ability to extend correlation across multiple sources so that common events from disparate systems (such as a firewall and an IPS) may be normalized and correlated together.

<table>
<thead>
<tr>
<th>Single-source Correlation Example</th>
<th>Cross-source Correlation Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple Failed Logon followed by one or more Successful Logon</td>
<td>Multiple Failed Logon events by an Admin user of Critical Assets, followed by one or more Successful Logon</td>
</tr>
<tr>
<td>Any Successful Logon to a Critical Asset</td>
<td>Any Successful Logon to a Critical Asset, by either a Terminated Employee or by an Admin User at a time outside of Normal shift hours.</td>
</tr>
<tr>
<td>HTTP traffic is originating from servers that are not HTTP servers</td>
<td>HTTP traffic is originating from servers that are not HTTP servers’ IP addresses with a geographic location outside of the United States</td>
</tr>
</tbody>
</table>
Tiered Correlation

One correlation rule within another correlation rule

- By stacking correlation rules within other rules, additional rules can be enabled to target more specific attack scenarios
Correlating between IT and OT Systems

To fully leverage the automated correlation capability built into most IT SIEM (security information and event management) products, OT data must first be collected into the SIEM.

- Then the normalization of one metric to another must be made using a common threat taxonomy.

<table>
<thead>
<tr>
<th>Incident</th>
<th>IT Event</th>
<th>OT Event</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network instability</td>
<td>Increased Latency, measured by TCP errors, reduction of TCP receive windows, increased round-trip TTL, etc.</td>
<td>Reduction in Efficiency, measured by historical batch comparisons</td>
<td>Manifestation of network condition in operational processes, Deliberate cyber sabotage</td>
</tr>
<tr>
<td>Operational change</td>
<td>No detected event</td>
<td>Change to operational set points, or other process change(s)</td>
<td>Benign process adjustment, Undetected cyber sabotage</td>
</tr>
<tr>
<td>Network breach</td>
<td>Detected threat or incident using event correlation, to determine successful penetration of IT system(s)</td>
<td>Change to operational set points, or other process change(s)</td>
<td>Benign process adjustment, Undetected cyber sabotage</td>
</tr>
<tr>
<td>Targeted incident</td>
<td>Detected threat or incident directly targeting industrial SCADA or DCS systems connected to IT networks</td>
<td>Abnormal change to operational set points, unexpected PLC code writes, etc.</td>
<td>Potential “Stuxnet-class” cyber incident or sabotage</td>
</tr>
</tbody>
</table>
MONITORING INDUSTRIAL CONTROL SYSTEMS
Determining What to Monitor

“Everything”
- But so much information that can exhaust the analyst as well as storage

Security Events
Assets
Configurations
Applications
Networks
Users
Behavior
Security Events

Generated by security products

- Network or host-based firewalls, Anti-Virus systems, intrusion detection and prevention systems, application monitors, application whitelisting systems, etc.

Ideally, they are relevant

- False positives?

SNORT IDS Policy violation (Windows update) warning

```
Jan 01 00:00:00 [69.20.59.59] snort: [1:2002948:6] ET POLICY
```
Assets

Devices in the network produce logs

Track activity on a variety of levels: the operating system itself produces many logs, including system application logs and file system logs

System logs are useful for tracking the status of devices and the approved services that are (or are not) running, as well as when patches are (or are not) applied

- These are also valuable in tracking which users (or applications) have authenticated to the asset, satisfying several compliance requirements
File system logs

Track when files are created, changed, or deleted, when access privileges or group ownerships are changed, and similar details

Extremely valuable for assuring the integrity of important files stored on an asset

- Such as configuration files (ensuring that the asset’s configurations remain within policy)
- The asset’s log files themselves (ensuring that logged activities are valid and have not been tampered with to cover up indications of illicit behavior)
Configurations

Process of monitoring baseline configurations for any indications of change, and is only a small part of Configuration Management (CM)

NIST SP 800-53 CM features:

- Configuration management policy and procedures
- Baseline configurations
- Change control
- Security impact analysis
- Access restrictions for change
- Configuration settings
- Least functionality
- Establishment of a configuration management plan
- Information service (IS) component (asset) inventory
Applications

Run on top of the operating system and perform specific functions

Direct monitoring of applications using a dedicated application monitoring product or application content firewall will provide a granular account of all application activities. Application logs can include when an application is executed or terminated, who logs into the application, and specific actions performed by users once logged in.
Networks

Network flows are records of network communications, from a source to one or more destinations

- Extremely useful for security analysis because it provides the information needed to trace the communications surrounding a security incident back to its source
- For ex.; if an application whitelisting agent detects malware on an asset, it is extremely important to know where that malware came from
- Path of propagation
- Typically tracked by network infrastructure devices such as switches and routers

Provides an overview of network usage over time
Networks

Also provides an indication of network performance

- Very important because of the negative impact that network performance can have on process quality and efficiency
- An increase in latency can cause certain industrial protocols to fail, halting industrial processes
User Identities and Authentication

Monitoring users and their activities is an ideal method for obtaining a clear picture of what is happening on the network, and who is responsible.

User monitoring is also an important component of compliance management:

- Specific controls around user privileges, access credentials, roles, and behaviors

The term “user” is vague:

- User account names, domain names, host names, user’s identity, etc.
- Necessary to normalize users to a common identity
User Identities and Authentication
## Additional Context

<table>
<thead>
<tr>
<th>Information Source</th>
<th>Provided Context</th>
<th>Security Implications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory services (e.g., active directory)</td>
<td>User identity information, asset identity information, and access privileges</td>
<td>Provides a repository of known users, assets, and roles that can be leveraged for security threat analysis and detection, as well as for compliance</td>
</tr>
<tr>
<td>Identity and Authentication Management systems</td>
<td>Detailed user identity information, usernames and account aliases, access privileges, and an audit trail of authentication activity</td>
<td>Enables the correlation of users to access and activities based upon privilege and policy. When used to enrich security events, provides a clear audit trail of activity versus authority that is necessary for compliance auditing</td>
</tr>
<tr>
<td>Vulnerability scanner</td>
<td>Asset details including the operating system, applications in use (ports and services), patch levels, identified vulnerabilities, and related known exploits</td>
<td>Enables security events to be weighted based upon the vulnerability of their target (i.e., a Windows virus is less concerning if it is targeting a Linux workstation) Also provides valuable asset details for use in exception reporting, event correlation, and other functions</td>
</tr>
<tr>
<td>Penetration tester</td>
<td>Exploitation success/failure, method of exploitation, evasion techniques, etc.</td>
<td>Like with a vulnerability scanner, pen test tools provide the context of an attack vector. Unlike VA scan results, which show what could be exploited, a pen test indicates what has been exploited—which is especially useful for determining evasion techniques, detecting mutating code, etc.</td>
</tr>
<tr>
<td>Threat database/CERT</td>
<td>Details, origins and recommendations for the remediation of exploits, malware, evasion techniques, etc.</td>
<td>Threat intelligence can be used in a purely advisory capacity (e.g., providing educational data associated with a detected threat), or in an analytical capacity (e.g., in association with vulnerability scan data to weight the severity calculation of a detected threat) Threat intelligence may also be used as “watchlists,” providing a cross-reference against which threats can be compared in order to highlight or otherwise call out threats of a specific category, severity, etc.</td>
</tr>
</tbody>
</table>
Additional Context

- What is the system's IP address? Other names? Location in the network? Geo location? Who is the owner? Who is the administrator? What else happened to this system?
- What is this service? What other messages did it produce? What other systems does it run on?
- Mar 20 08:44:35 px02 ssdh[263]: Accepted password for root from 216.101.197.234 port 56946 ssh2
- What is this user? Where is he/she coming from? What is his/her real name? What organizational or business unit? Roles? Privileges?
- What is this port? What is a common service that utilizes this port? Where else is this service being used?
Monitoring Security Zones

Log collection and analysis

- Directing the log output to a log aggregation point, such as a network storage facility and/or a dedicated Log Management system

Direct monitoring or network inspection

- Use of a probe or other device to examine network traffic or hosts directly
- Useful when the system being monitored does not produce logs natively
- Also useful as a verification of activity reported by logs
Monitoring Security Zones

Inferred monitoring via tangential systems

- One system is monitored in order to infer information about another system
  - For example, many applications connect to a database; monitoring the database in lieu of the application itself will provide valuable information about how the application is being used, even if the application itself is not producing logs or being directly monitoring by an Application Monitor

- It should be assured logs are transferred one direction
  - Otherwise, they can be accessed and corrupted within the zone

What about encrypted traffic?
Process for Enabling Security Zone Monitoring
Information Collection and Management Tools (Log Management Systems, SIEMs)

Syslog Aggregation and Log Search

Log Management Systems

Security Information and Event Management Systems

- Designed to support real-time monitoring and analytical functions, it will parse the contents of a log file at the time of collection, storing the parsed information in some sort of structured data store, typically a database or a specialized flat-file storage system

Data Historians