Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 19: Monitoring Security and Access Controls

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

Anomaly Detection

Threat Detection

What to Monitor

Recall: Network Segmentation

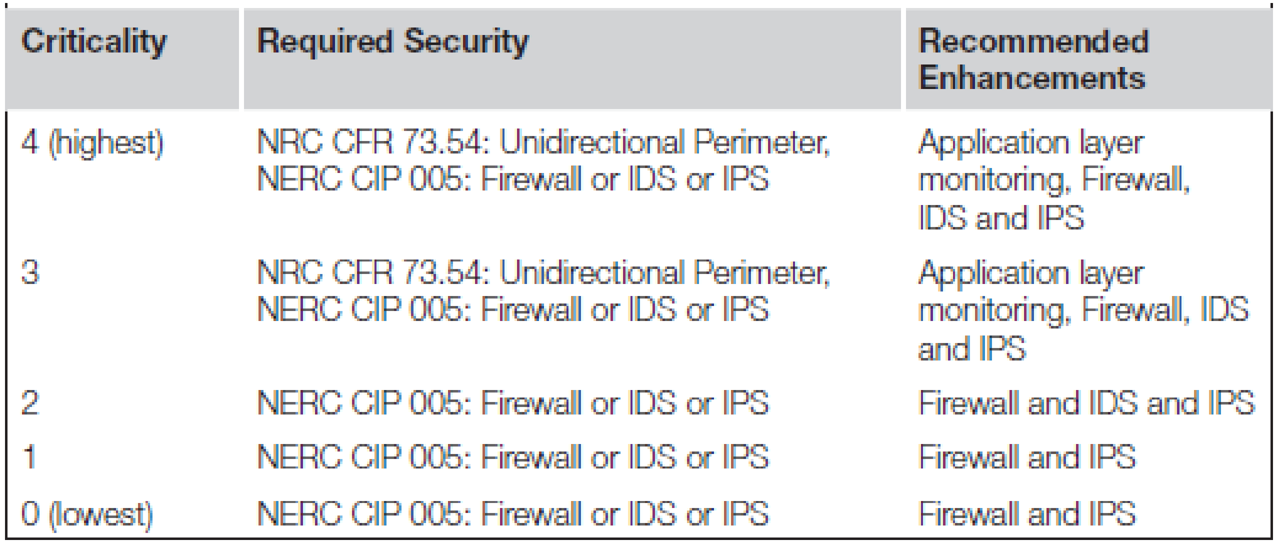
In case not possible to clearly identify boundaries of zone;

- 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



Criticality	Required Security	Recommended Enhancements
4 (highest)	NRC CFR 73.54: Unidirectional Perimeter, NERC CIP 005: Firewall or IDS or IPS	Application layer monitoring, Firewall, IDS and IPS
3	NRC CFR 73.54: Unidirectional Perimeter, NERC CIP 005: Firewall or IDS or IPS	Application layer monitoring, Firewall, IDS and IPS
2	NERC CIP 005: Firewall or IDS or IPS	Firewall and IDS and IPS
1	NERC CIP 005: Firewall or IDS or IPS	Firewall and IPS
0 (lowest)	NERC CIP 005: Firewall or IDS or IPS	Firewall and IPS

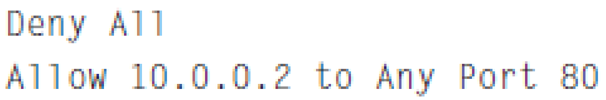
Recall: Firewall Configuration Guidelines

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

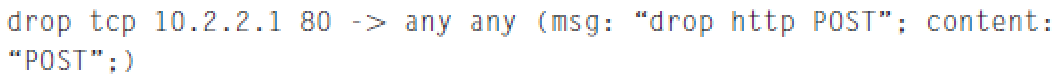
- These broad rules can then be overruled by subsequent, more focused rules
- Therefore, the following firewall policy would only allow a single IP address to communicate outside of the firewall on port 80 (HTTP)



```
Deny All
Allow 10.0.0.2 to Any Port 80
```

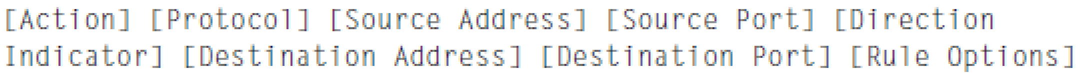
Recall: Intrusion Detection and Prevention (IDS/IPS) Configuration Guidelines

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)

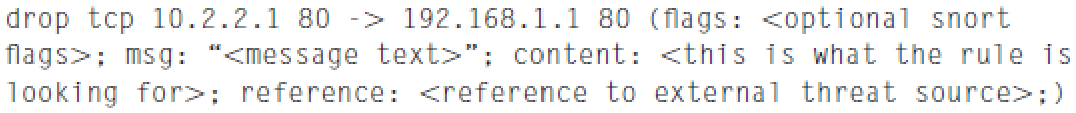


```
drop tcp 10.2.2.1 80 -> any any (msg: “drop http POST”; content:
“POST”;)
```

Example usage:



```
[Action] [Protocol] [Source Address] [Source Port] [Direction
Indicator] [Destination Address] [Destination Port] [Rule Options]
```



```
drop tcp 10.2.2.1 80 -> 192.168.1.1 80 (flags: <optional snort
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

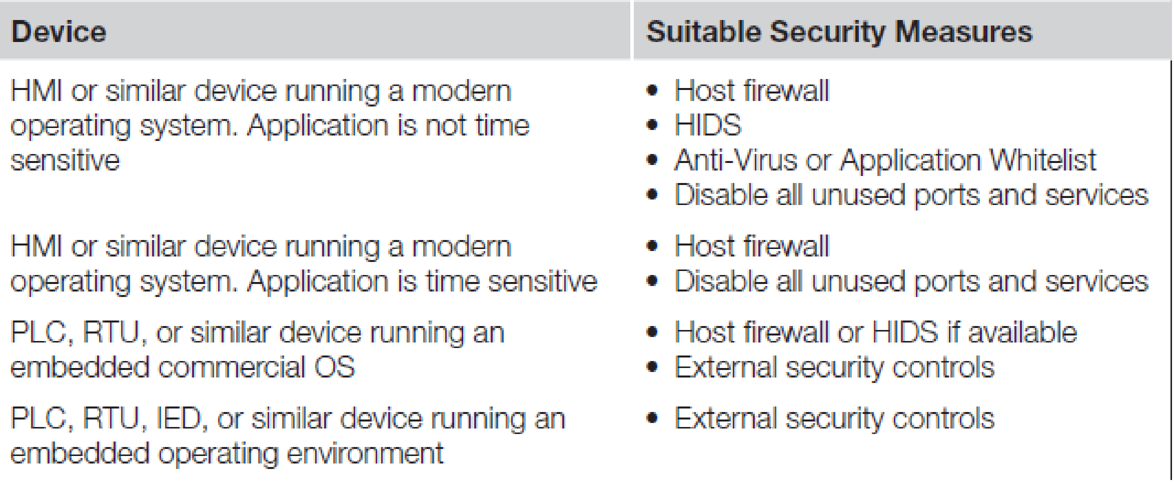
- Application Monitors provide a very broad and very deep look into how network traffic is being used
- Useful in environments where both control systems and enterprise protocols and applications are in use

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)



Device	Suitable Security Measures
HMI or similar device running a modern operating system. Application is not time sensitive	• Host firewall • HIDS • Anti-Virus or Application Whitelist • Disable all unused ports and services
HMI or similar device running a modern operating system. Application is time sensitive	• Host firewall • Disable all unused ports and services
PLC, RTU, or similar device running an embedded commercial OS	• Host firewall or HIDS if available • External security controls
PLC, RTU, IED, or similar device running an embedded operating environment	• External security controls

Exception Reporting

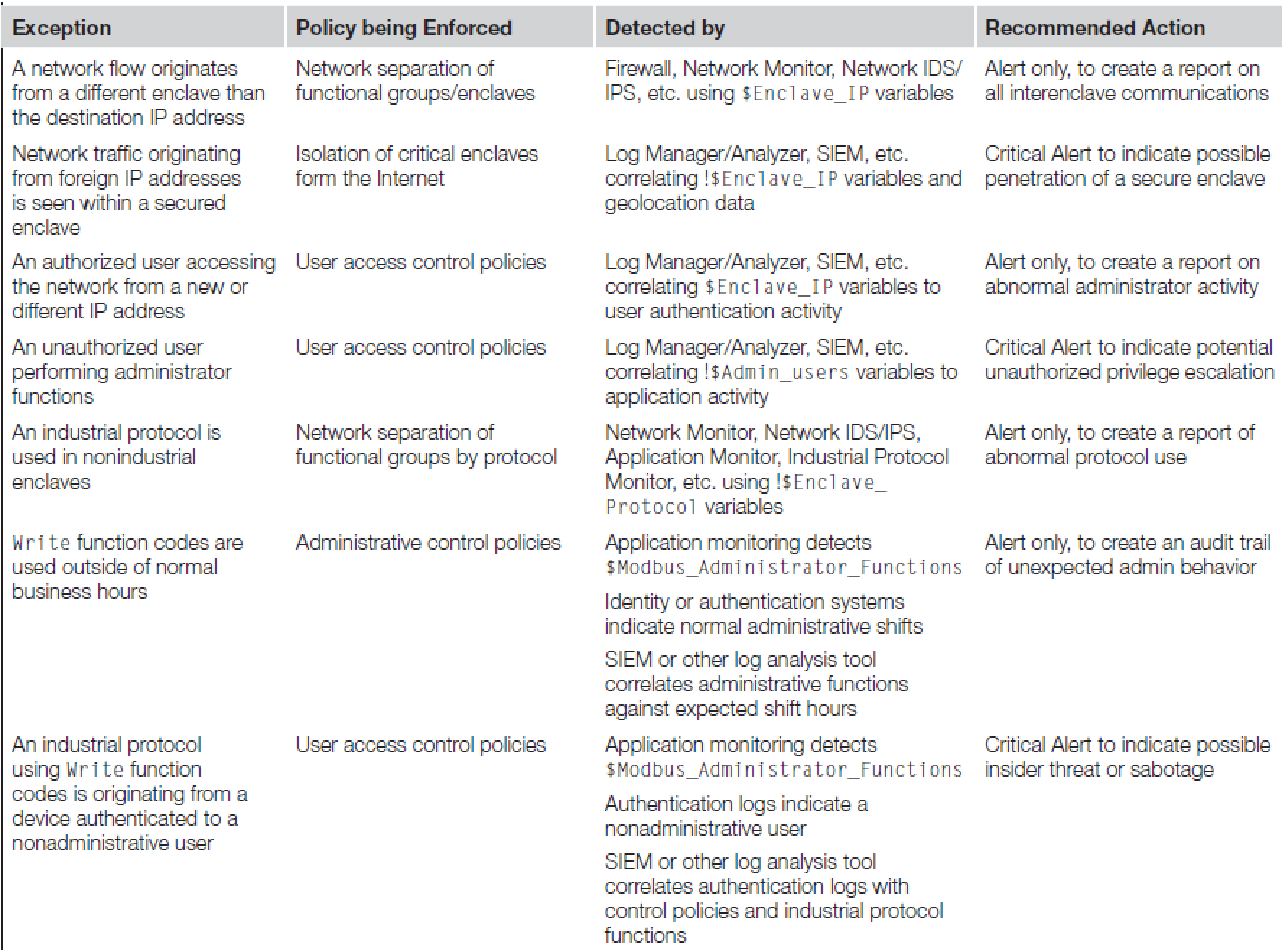
Expect one behavior but see another -> potential threat

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



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

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

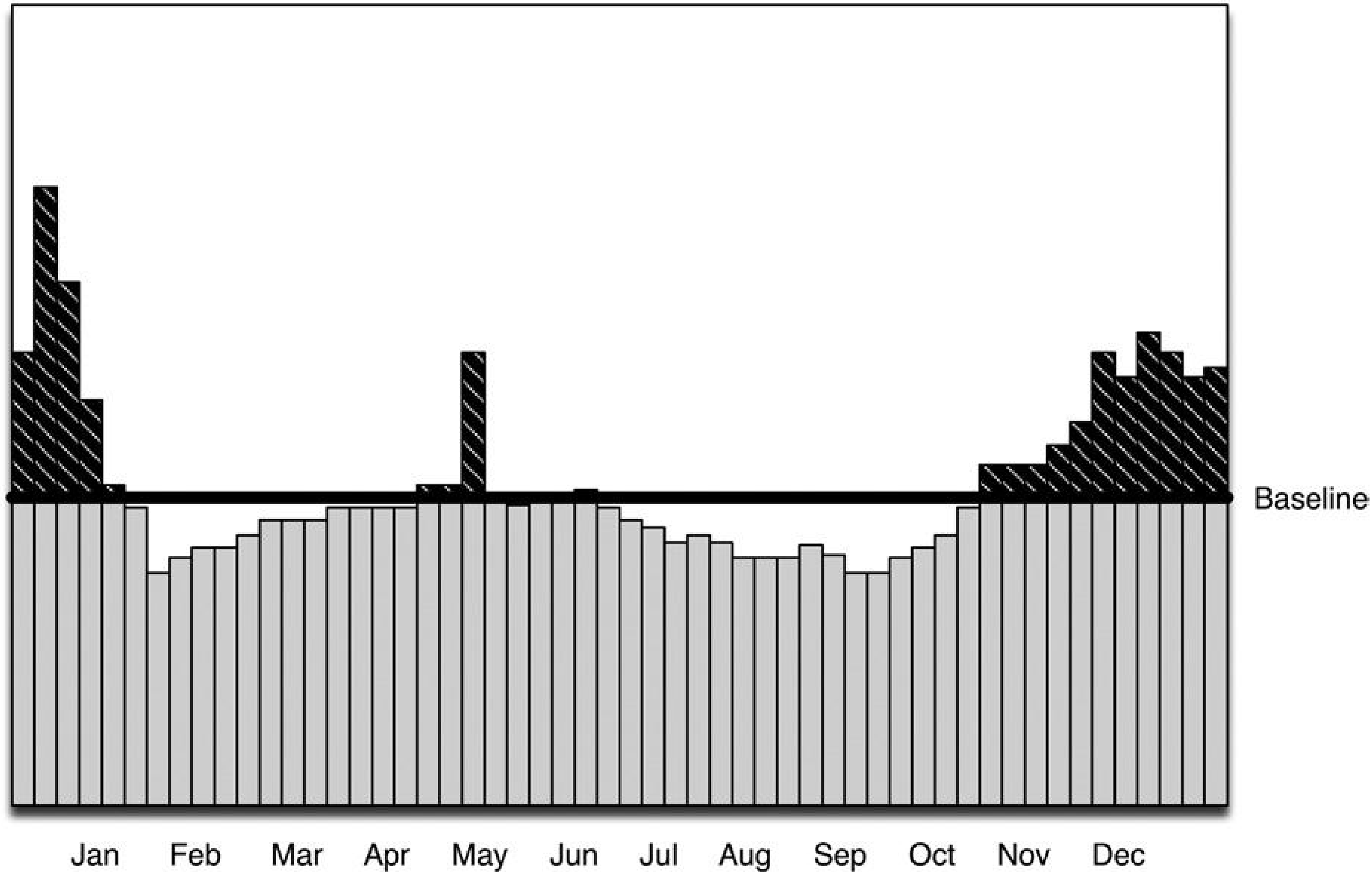
- Baseline is a value: nothing more, nothing less
- Trend analysis; a forward-looking application of known baselines to predict the continuation of observed trends

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

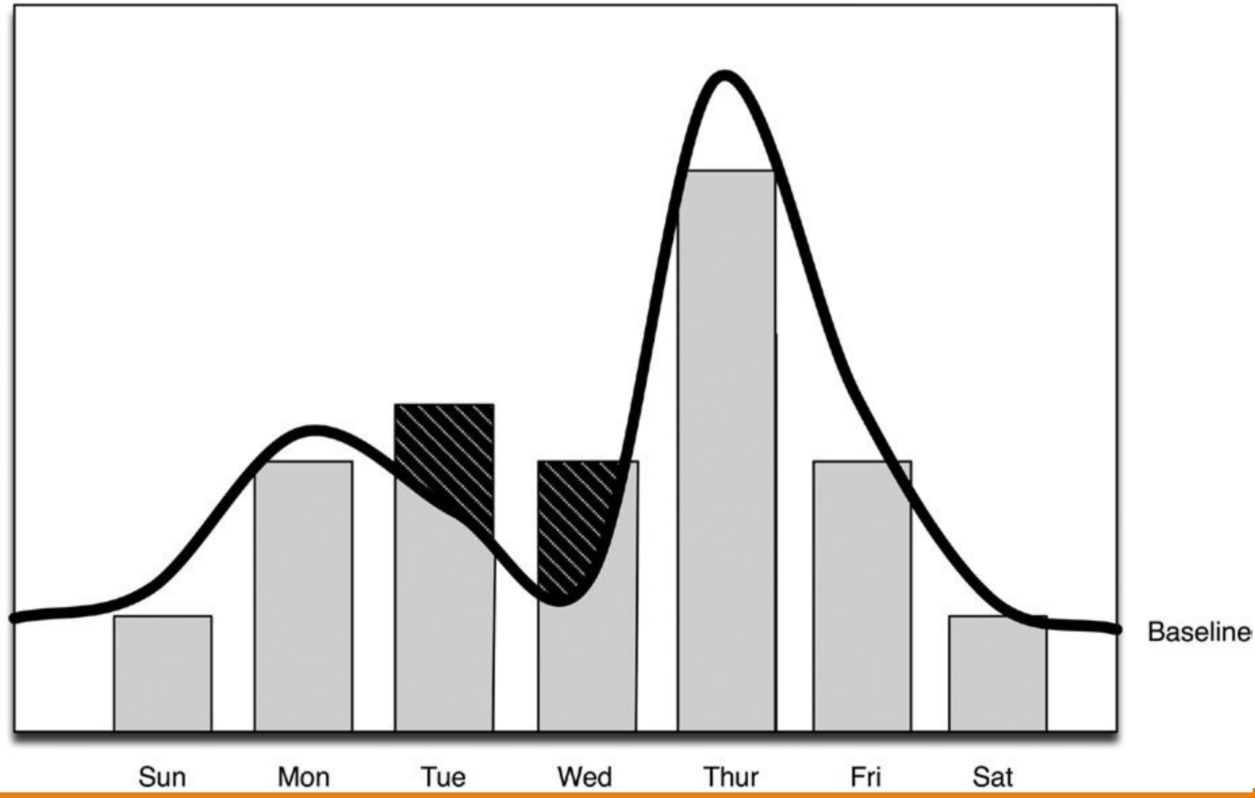
Useful of observed activity within relevant contexts of time

- Essentially providing historical context to baseline averages

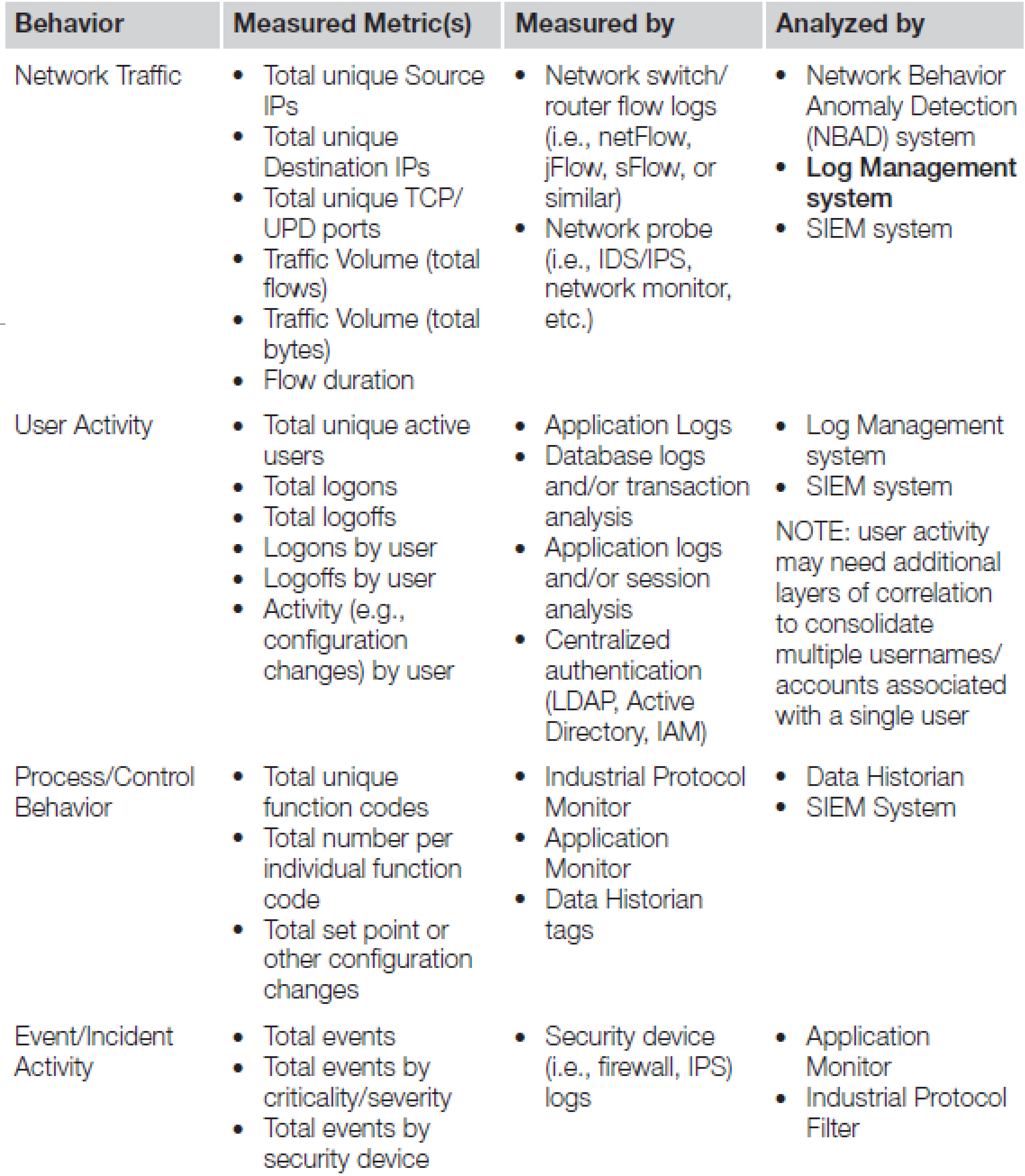
Spike in activity on Thursday might be seen as an anomaly and spur an extensive security analysis, rather than being clearly indicated as normal behavior

- 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

A Time-Correlated Baseline Shows Dip on Weekends, Peak on Thursdays

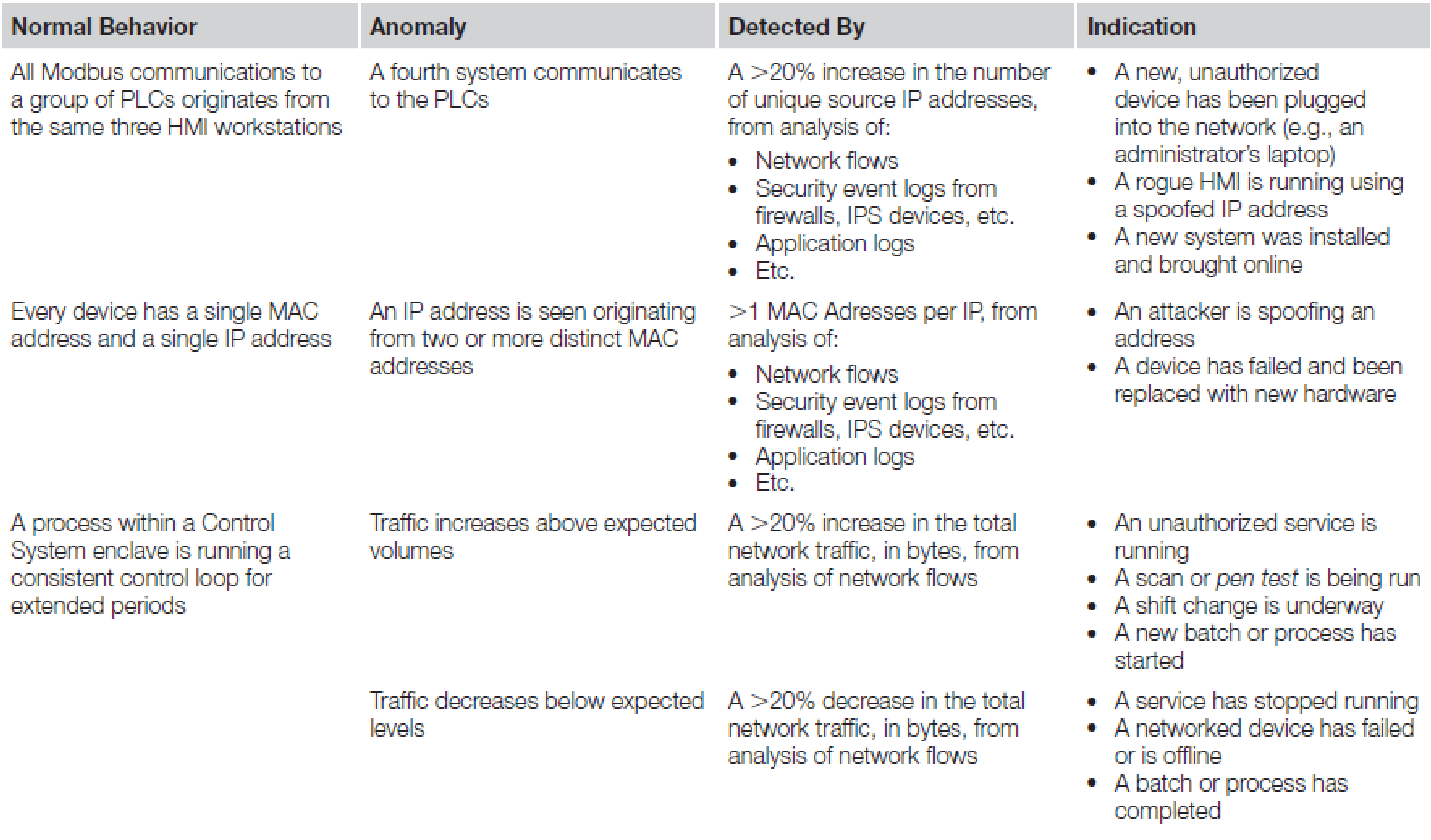


Measurement and Analysis of Baseline Metrics



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

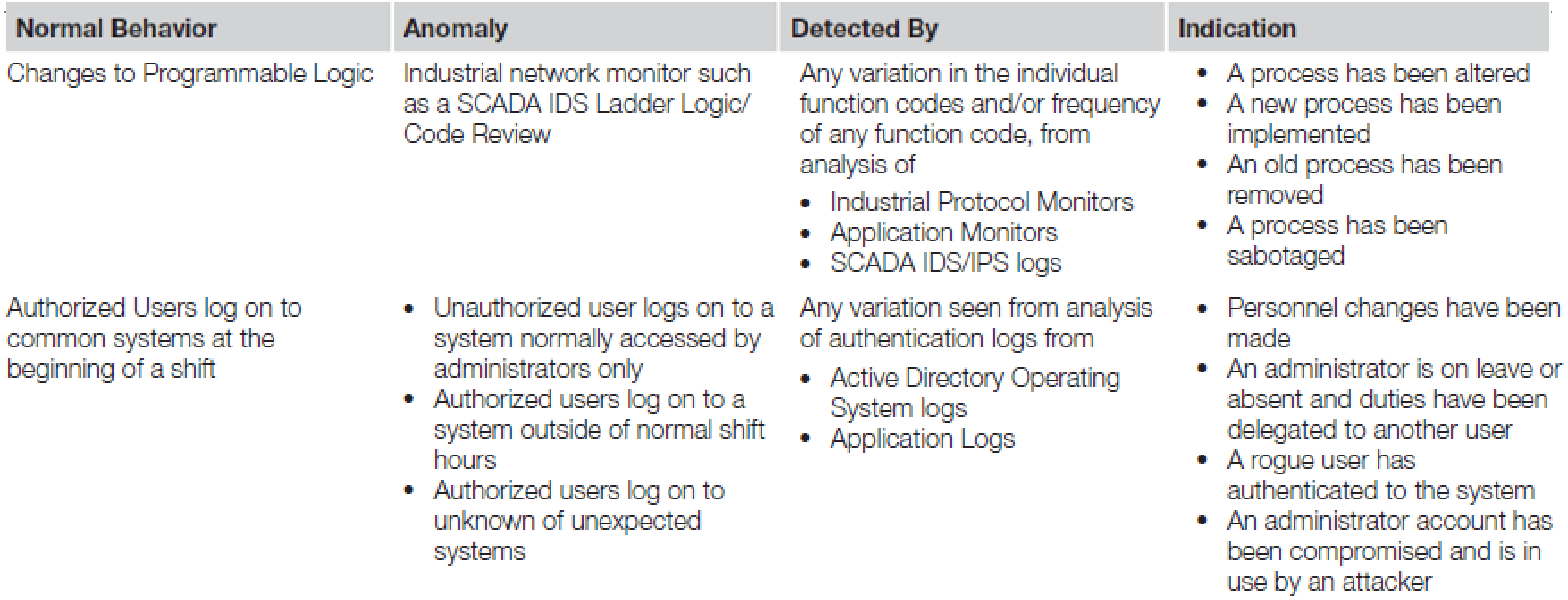
Examples of Suspicious Anomalies



Normal Behavior	Anomaly	Detected By	Indication
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, IPS 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 Adresses per IP, from analysis of: • Network flows • Security event logs from firewalls, IPS 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

Southern Illinois University
CARBONDALE

Examples of Suspicious Anomalies



Normal Behavior	Anomaly	Detected By	Indication
Changes to Programmable Logic	Industrial network monitor such as a SCADA IDS Ladder Logic/ Code Review	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	• A process has been altered • A new process has been implemented • An old process has been removed • A process has been sabotaged
Authorized Users log on to common systems at the beginning of a shift	• Unauthorized user logs on to a system normally accessed by administrators only • Authorized users log on to a system outside of normal shift hours • Authorized users log on to unknown of unexpected systems	Any variation seen from analysis of authentication logs from • Active Directory Operating System logs • Application Logs	• 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

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

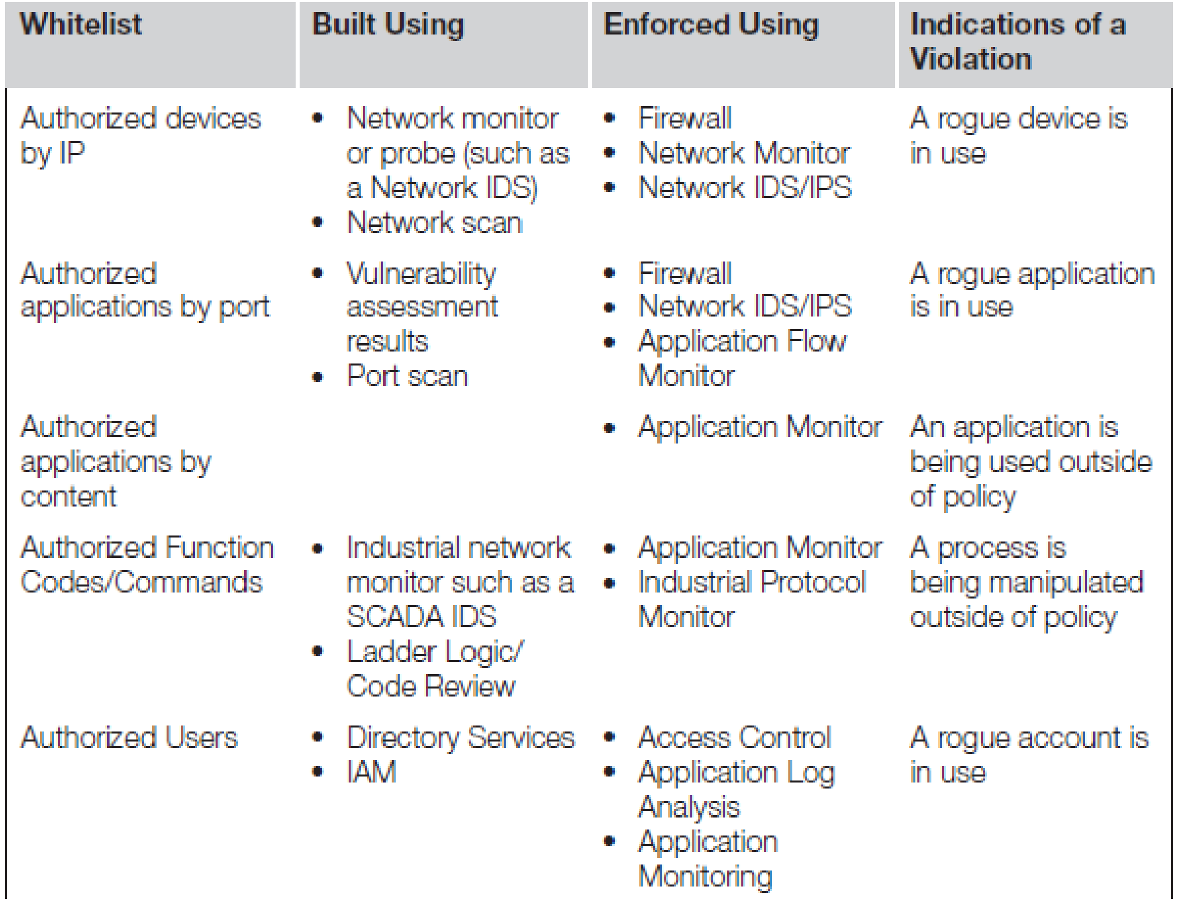
Master PDUs or Datagrams are only allowed from predefined assets

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



Whitelist	Built Using	Enforced Using	Indications of a Violation
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"

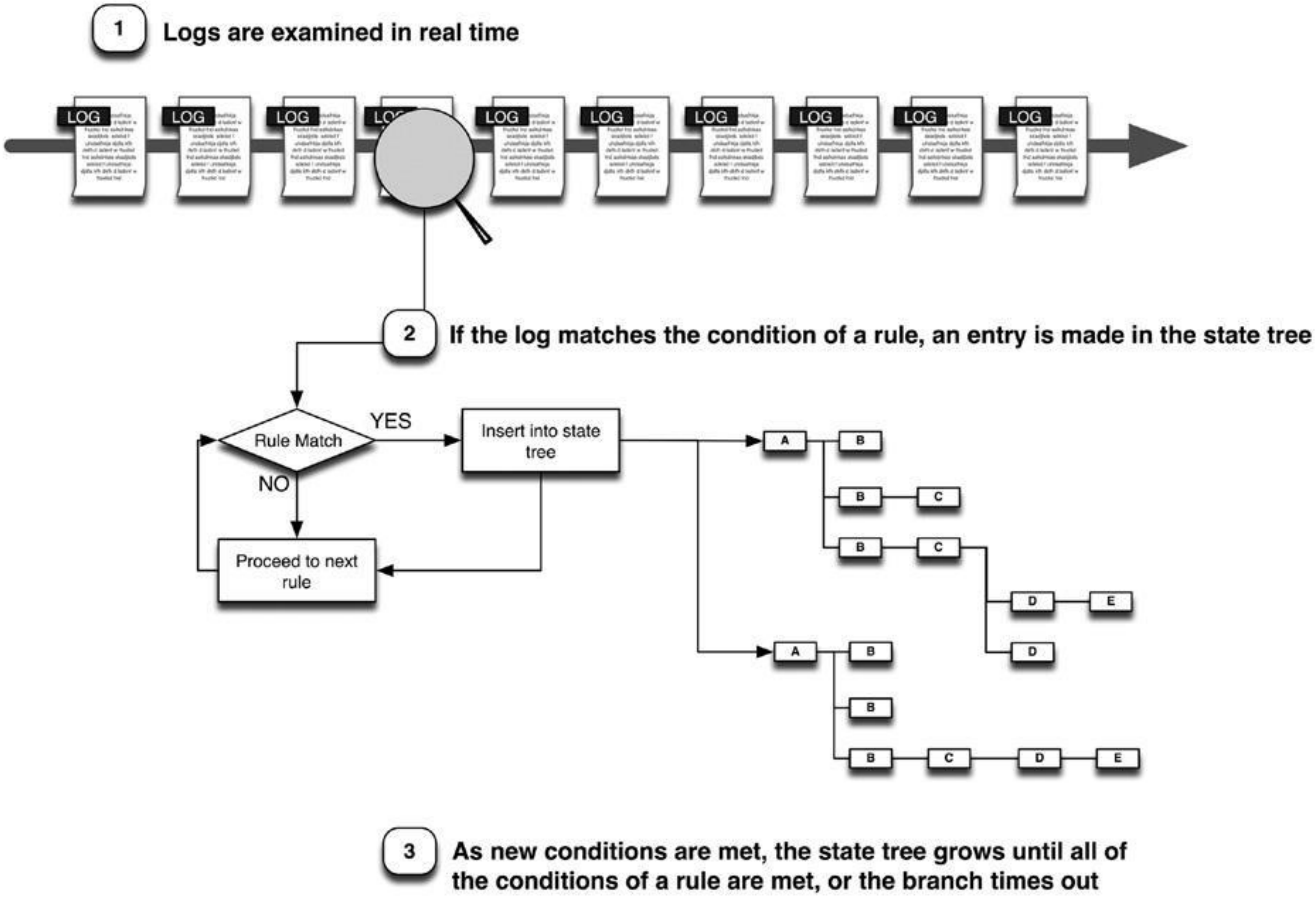
- If there is a match, an entry is made in a (typically) memory-resident state tree; if another sequence in the pattern is seen, the rule progresses until a complete match is determined
- For example, if a log matches the first condition of a rule, a new entry is made in the state tree, indicating that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

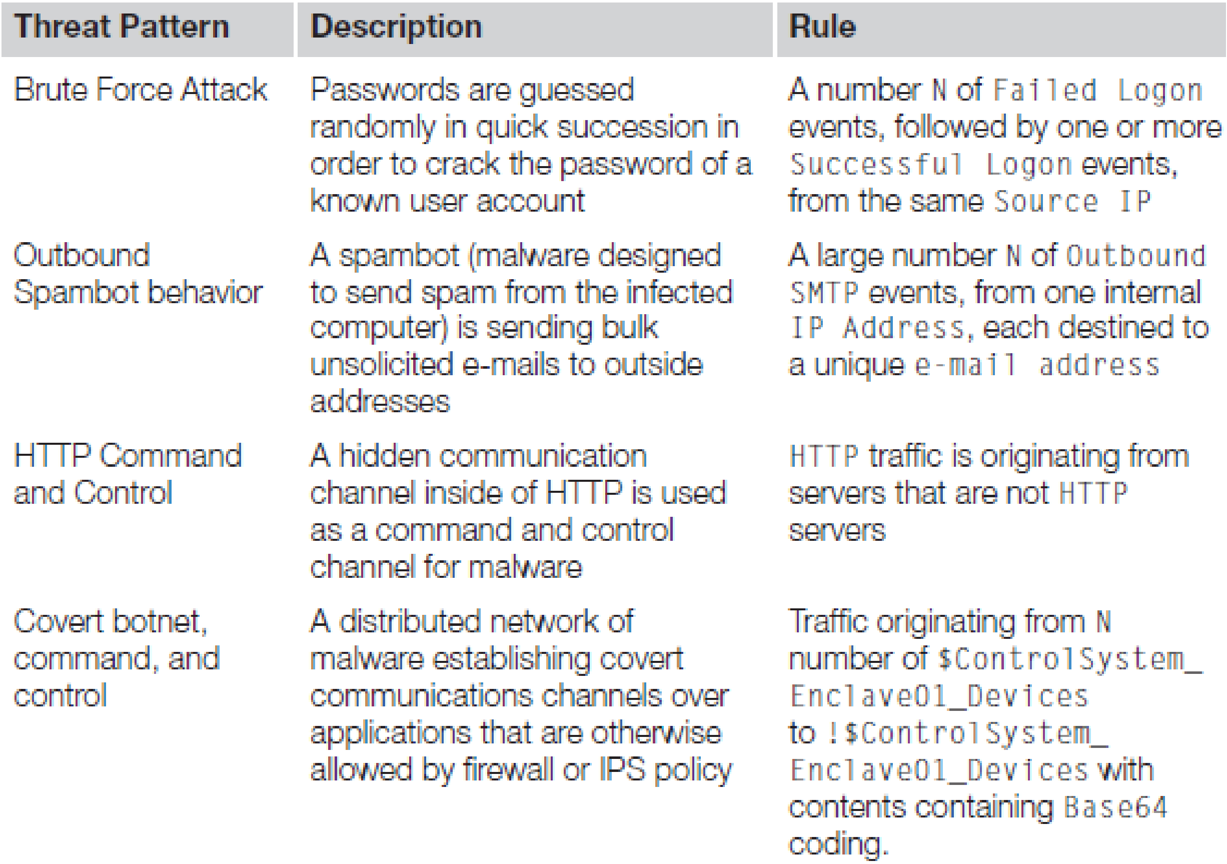


1 Logs are examined in real time

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



Threat Pattern	Description	Rule
Brute Force Attack	Passwords are guessed randomly in quick succession in order to crack the password of a known user account	A number N of Failed Logon events, followed by one or more Successful Logon events, from the same Source IP
Outbound Spambot behavior	A spambot (malware designed to send spam from the infected computer) is sending bulk unsolicited e-mails to outside addresses	A large number N of Outbound SMTP events, from one internal IP Address, each destined to a unique e-mail address
HTTP Command and Control	A hidden communication channel inside of HTTP is used as a command and control channel for malware	HTTP traffic is originating from servers that are not HTTP servers
Covert botnet, command, and control	A distributed network of malware establishing covert communications channels over applications that are otherwise allowed by firewall or IPS policy	Traffic originating from N number of $ControlSystem_Enclave01_Devices to !$ControlSystem_Enclave01_Devices with contents containing Base64 coding.

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

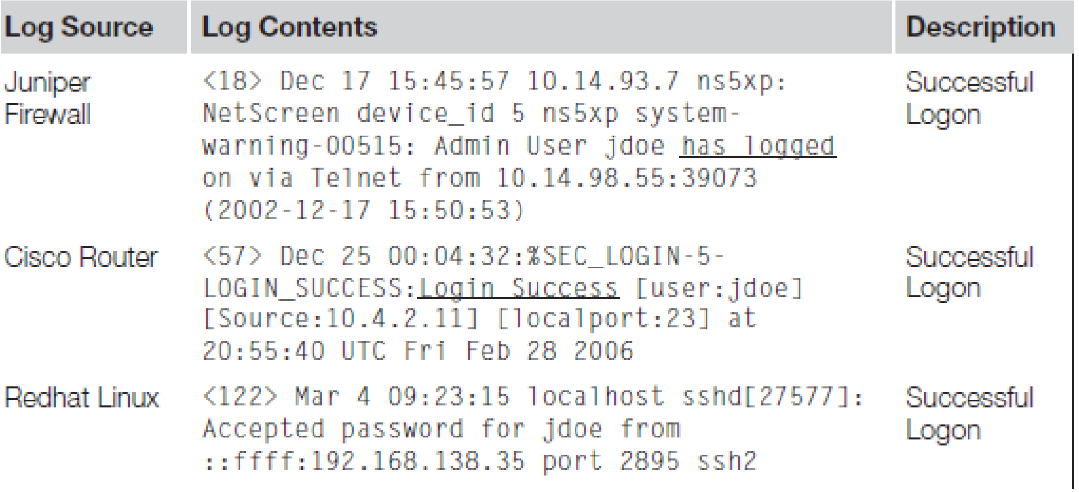
Primary way

- 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

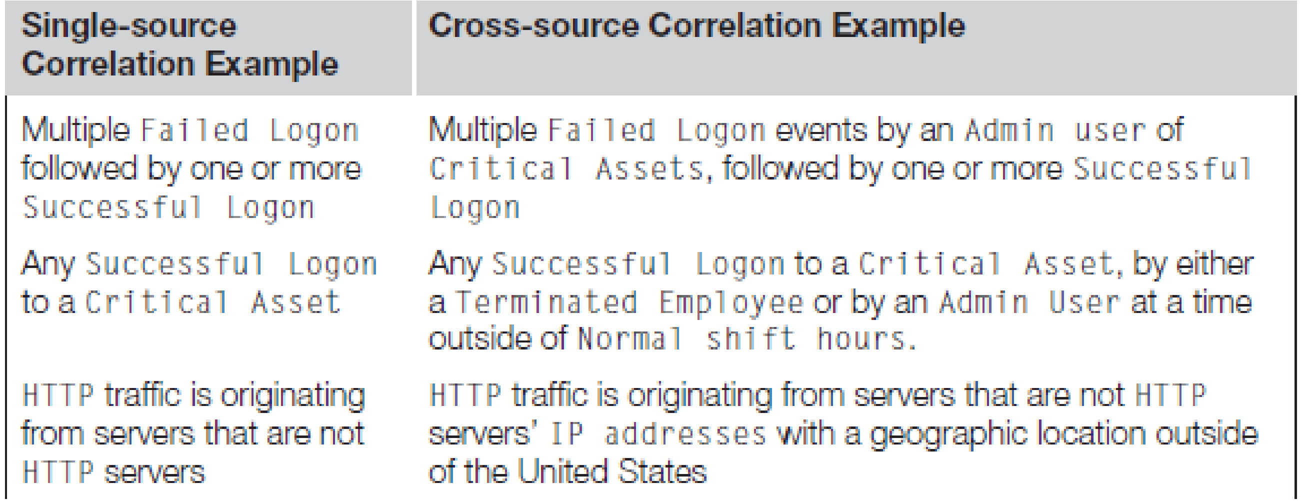
Way the message is depicted varies sufficiently that without a compensating measure such as event normalization, a correlation rule looking for "logons" would need to explicitly define each known logon format



Log Source	Log Contents	Description
Juniper Firewall	<18> Dec 17 15:45:57 10.14.93.7 ns5xp: NetScreen device_id 5 ns5xp system-warning-00515: Admin User jdoe has logged on via Telnet from 10.14.98.55:39073 (2002-12-17 15:50:53)	Successful Logon
Cisco Router	<57> Dec 25 00:04:32:%SEC_LOGIN-5-LOGIN_SUCCESS:Login Success [user:jdoe] [Source:10.4.2.11] [localport:23] at 20:55:40 UTC Fri Feb 28 2006	Successful Logon
Redhat Linux	<122> Mar 4 09:23:15 localhost sshd[27577]: Accepted password for jdoe from ::ffff:192.168.138.35 port 2895 ssh2	Successful Logon

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

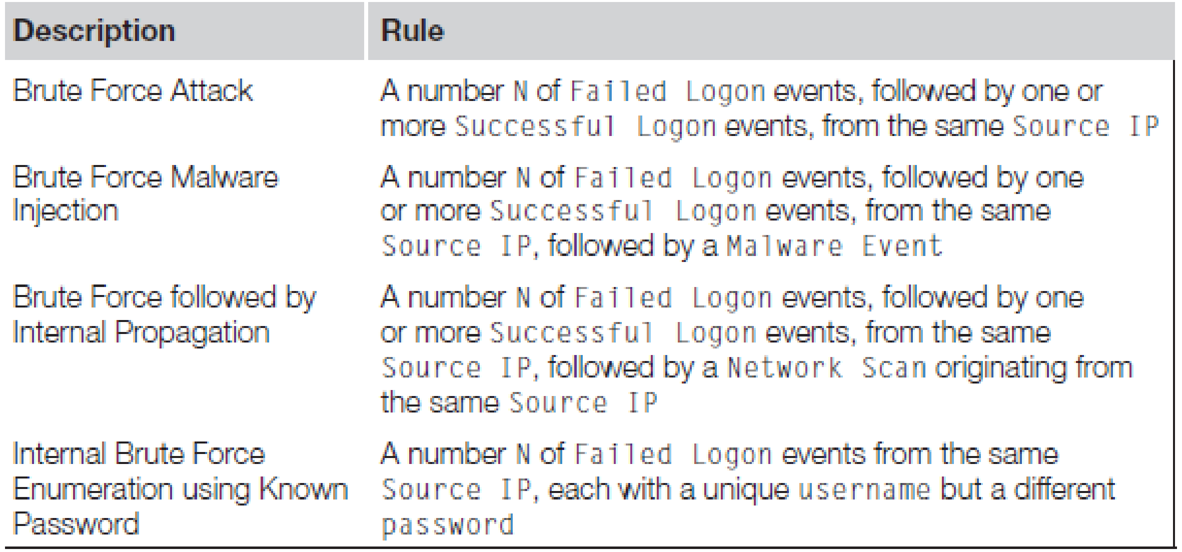


Single-source Correlation Example	Cross-source Correlation Example
Multiple Failed Logon followed by one or more Successful Logon	Multiple Failed Logon events by an Admin user of Critical Assets, followed by one or more Successful Logon
Any Successful Logon to a Critical Asset	Any Successful Logon to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

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

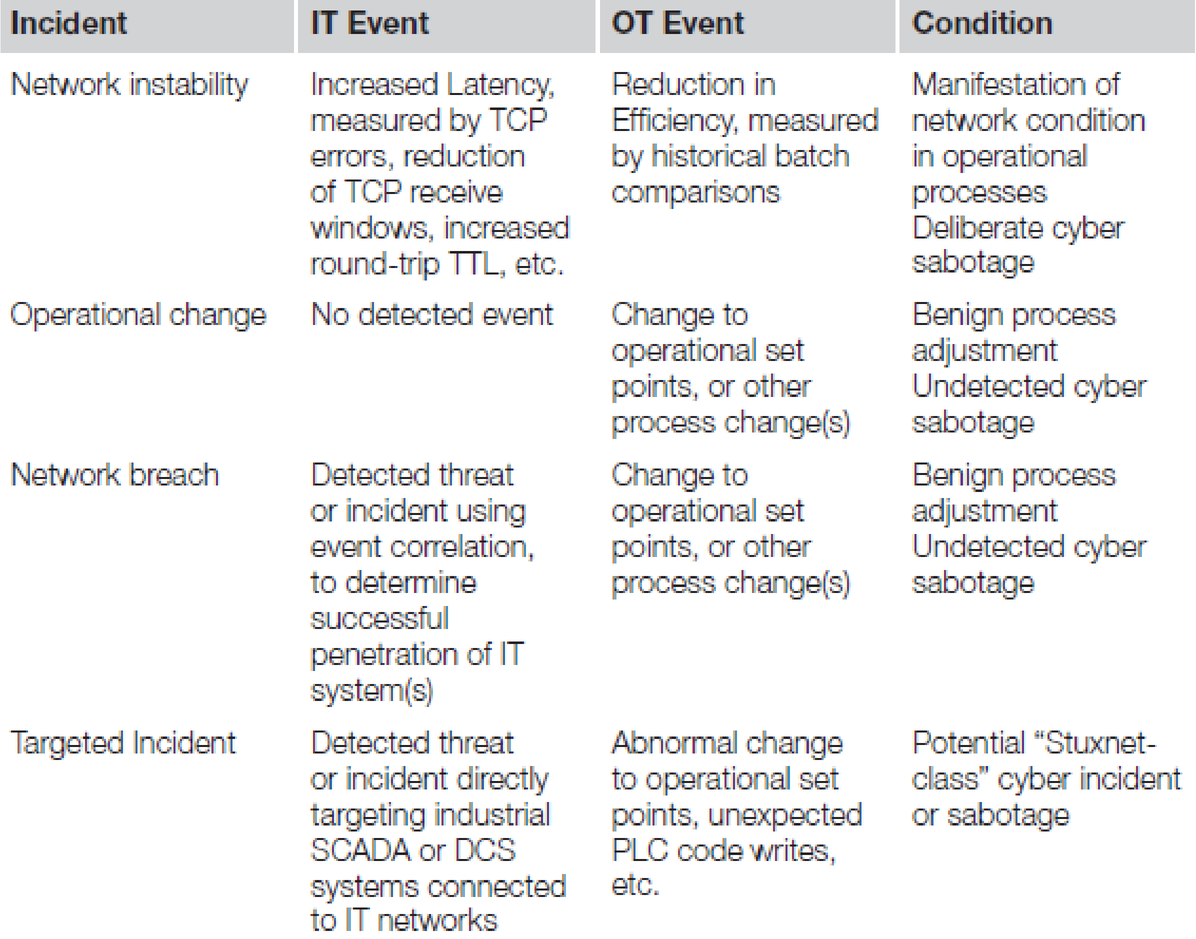


Description	Rule
Brute Force Attack	A number N of Failed Logon events, followed by one or more Successful Logon events, from the same Source IP
Brute Force Malware Injection	A number N of Failed Logon events, followed by one or more Successful Logon events, from the same Source IP, followed by a Malware Event
Brute Force followed by Internal Propagation	A number N of Failed Logon events, followed by one or more Successful Logon events, from the same Source IP, followed by a Network Scan originating from the same Source IP
Internal Brute Force Enumeration using Known Password	A number N of Failed Logon events from the same Source IP, each with a unique username but a different password

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



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

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

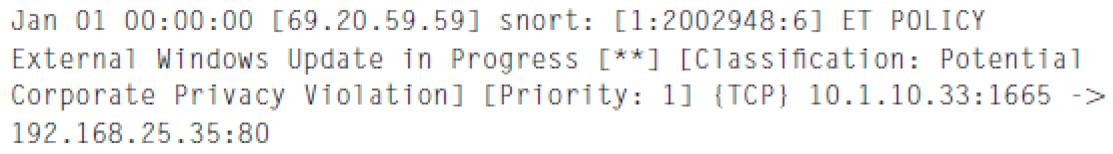
Generated by security products

- 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
External Windows Update in Progress [**] [Classification: Potential
Corporate Privacy Violation] [Priority: 1] {TCP} 10.1.10.33:1665 ->
192.168.25.35:80
```

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

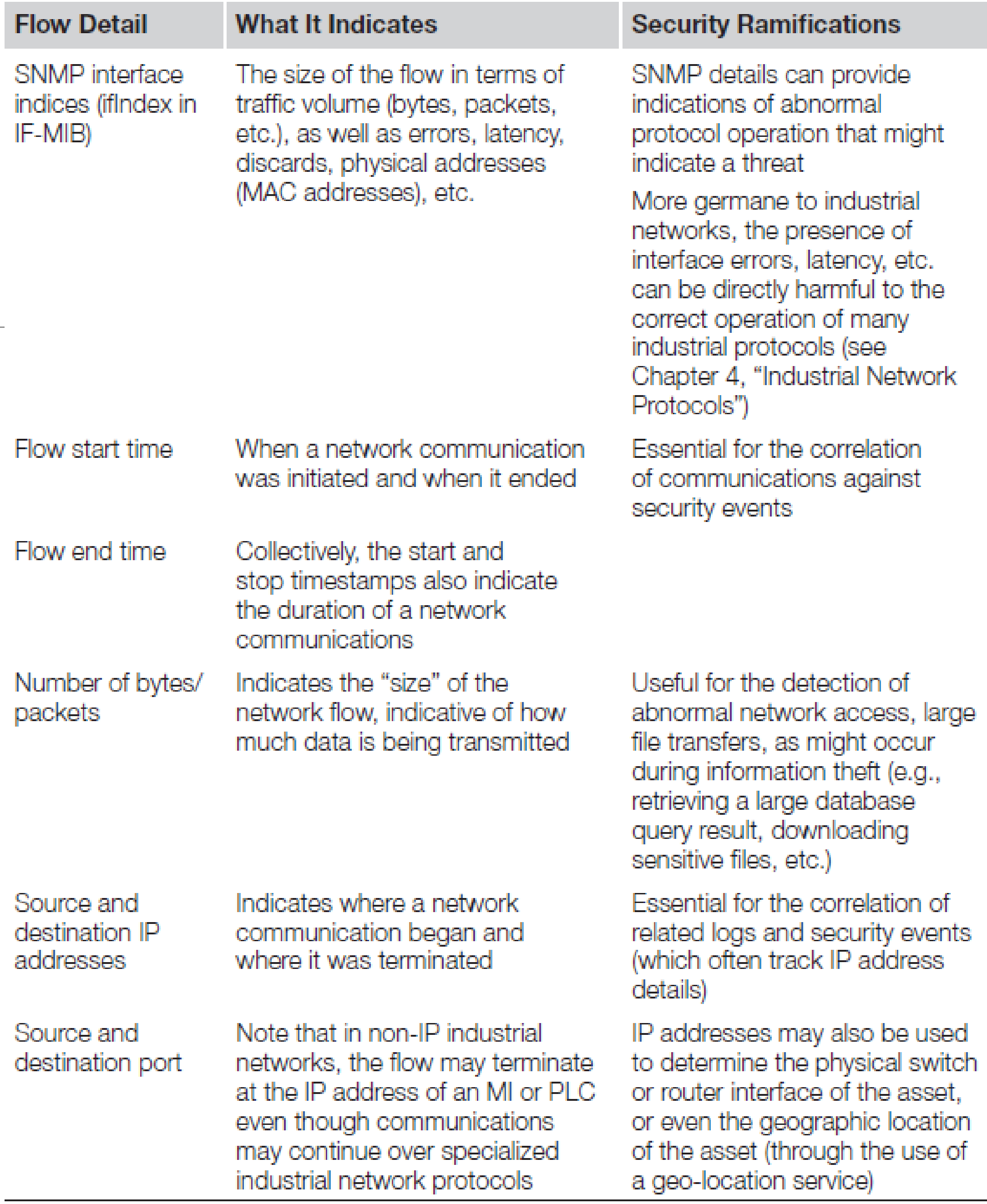
- Extremely useful for security analysis because it provides the information needed to trace the communications surrounding a security incident back to its source
  - For ex.; if an application whitelisting agent detects malware on an asset, it is extremely important to know where that malware came from
  - 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



Flow Detail	What It Indicates	Security Ramifications
SNMP interface indices (ifIndex in IF-MIB)	The size of the flow in terms of traffic volume (bytes, packets, etc.), as well as errors, latency, discards, physical addresses (MAC addresses), etc.	SNMP details can provide indications of abnormal protocol operation that might indicate a threat More germane to industrial networks, the presence of interface errors, latency, etc. can be directly harmful to the correct operation of many industrial protocols (see Chapter 4, "Industrial Network Protocols")
Flow start time	When a network communication was initiated and when it ended	Essential for the correlation of communications against security events
Flow end time	Collectively, the start and stop timestamps also indicate the duration of a network communications	
Number of bytes/ packets	Indicates the "size" of the network flow, indicative of how much data is being transmitted	Useful for the detection of abnormal network access, large file transfers, as might occur during information theft (e.g., retrieving a large database query result, downloading sensitive files, etc.)
Source and destination IP addresses	Indicates where a network communication began and where it was terminated	Essential for the correlation of related logs and security events (which often track IP address details)
Source and destination port	Note that in non-IP industrial networks, the flow may terminate at the IP address of an MI or PLC even though communications may continue over specialized industrial network protocols	IP addresses may also be used to determine the physical switch or router interface of the asset, or even the geographic location of the asset (through the use of a geo-location service)

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

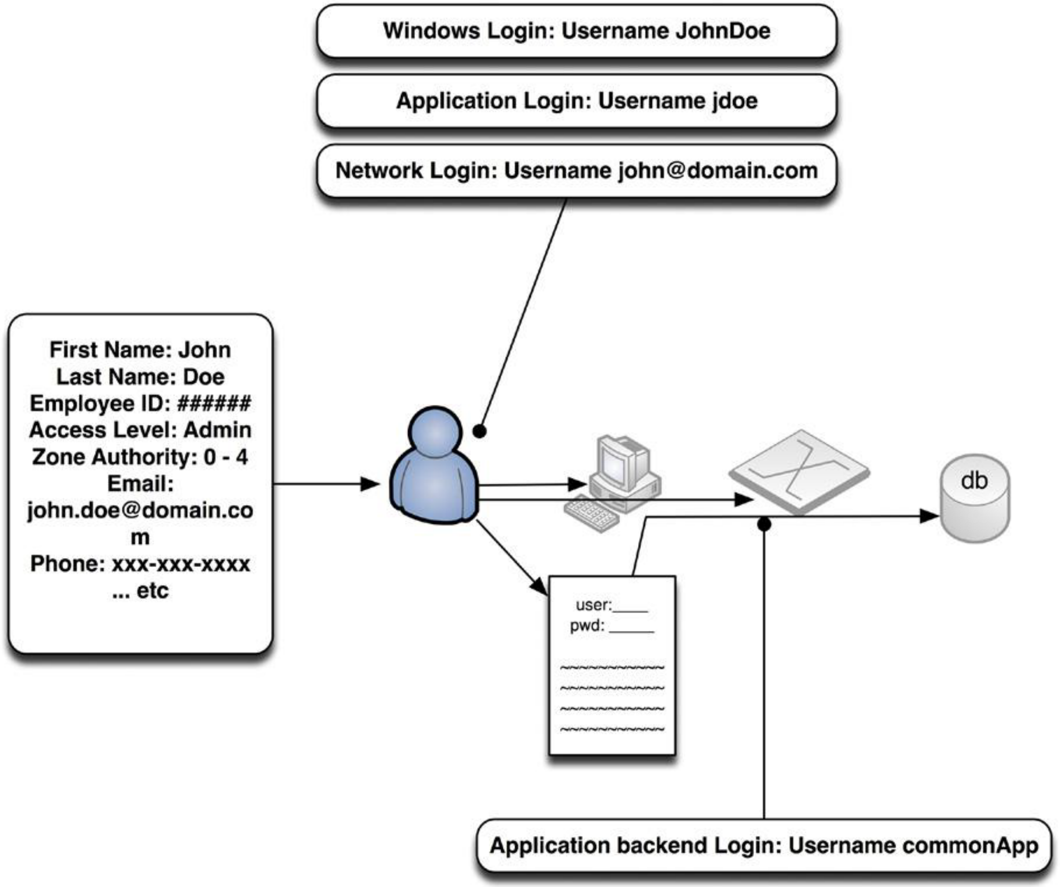
User monitoring is also an important component of compliance management

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

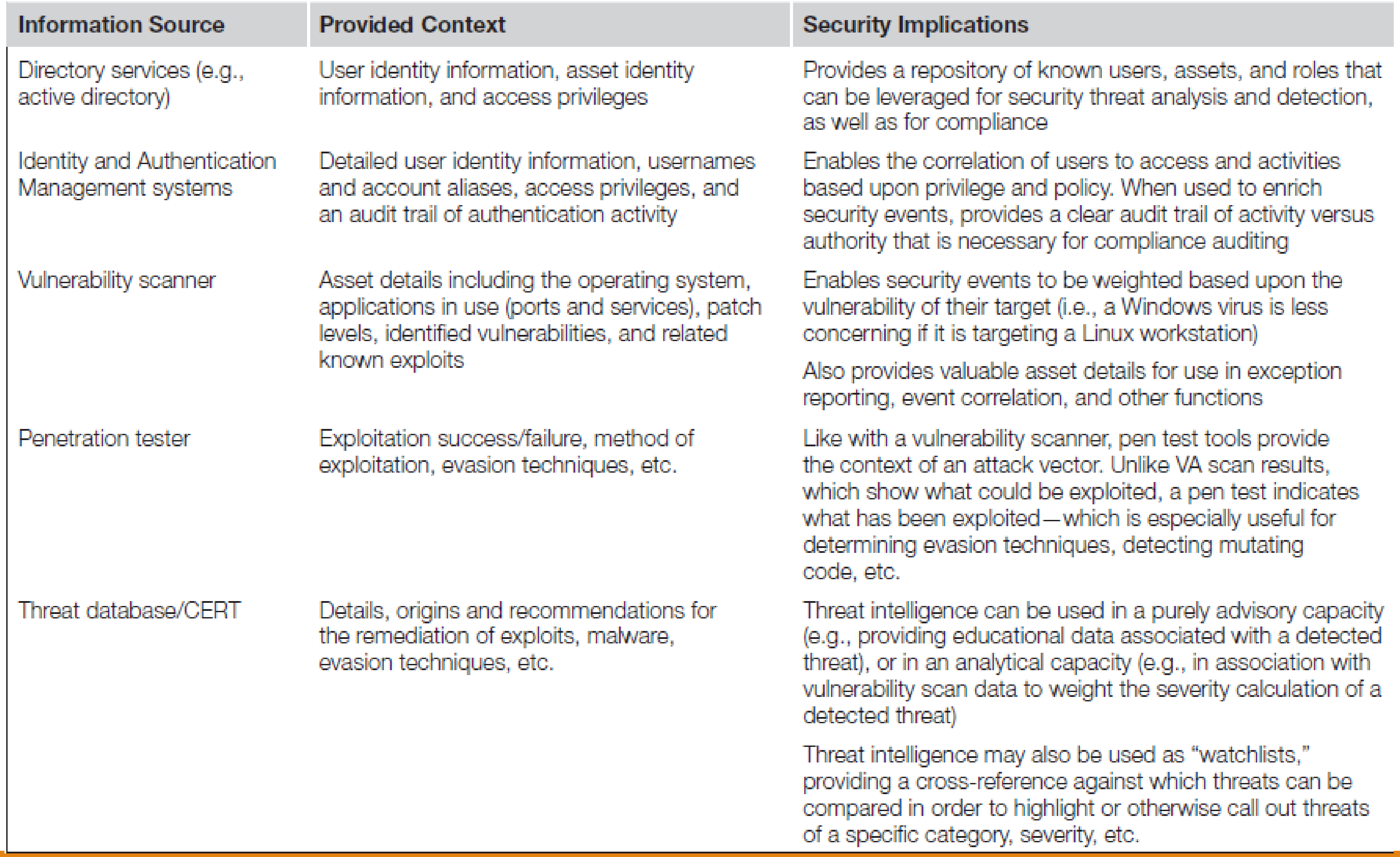
The term “user” is vague

- User account names, domain names, host names, user’s identity, etc.
- Necessary to normalize users to a common identity

User Identities and Authentication

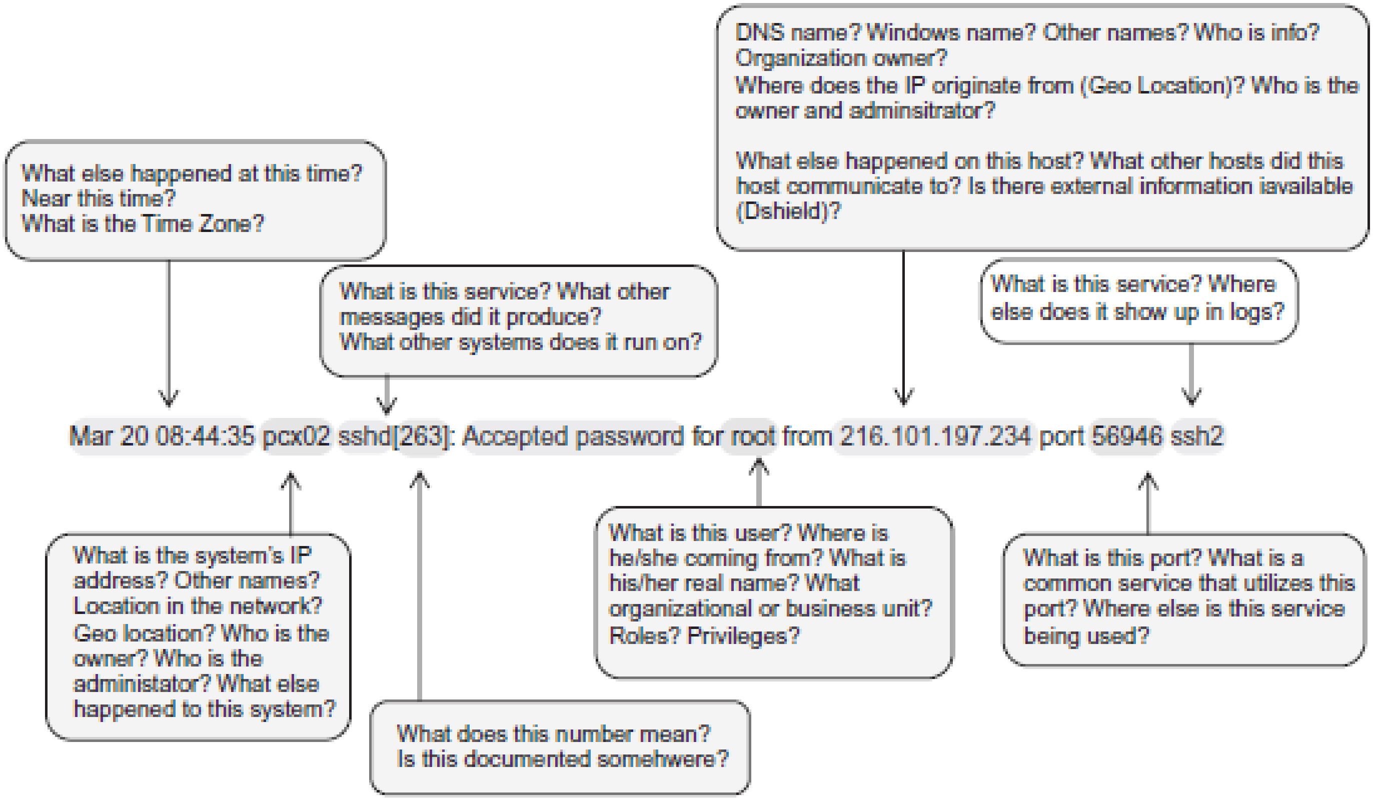

Windows Login: Username JohnDoe
Application Login: Username jdoe
Network Login: Username john@domain.com
First Name: John
Last Name: Doe
Employee ID: ######
Access Level: Admin
Zone Authority: 0 - 4
Email: john.doe@domain.com
Phone: xxx-xxx-xxxx
... etc
db
user:____
pwd: _____
Application backend Login: Username commonApp

Additional Context



Information Source	Provided Context	Security Implications
Directory services (e.g., active directory)	User identity information, asset identity information, and access privileges	Provides a repository of known users, assets, and roles that can be leveraged for security threat analysis and detection, as well as for compliance
Identity and Authentication Management systems	Detailed user identity information, usernames and account aliases, access privileges, and an audit trail of authentication activity	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
Vulnerability scanner	Asset details including the operating system, applications in use (ports and services), patch levels, identified vulnerabilities, and related known exploits	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
Penetration tester	Exploitation success/failure, method of exploitation, evasion techniques, etc.	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.
Threat database/CERT	Details, origins and recommendations for the remediation of exploits, malware, evasion techniques, etc.	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.

Additional Context



What else happened at this time?
Near this time?
What is the Time Zone?

What is this service? What other messages did it produce?
What other systems does it run on?

DNS name? Windows name? Other names? Who is info? Organization owner?
Where does the IP originate from (Geo Location)? Who is the owner and adminsitrator?

What else happened on this host? What other hosts did this host communicate to? Is there external information iavailable (Dshield)?

What is this service? Where else does it show up in logs?

```
Mar 20 08:44:35 pcx02 sshd[263]: Accepted password for root from 216.101.197.234 port 56946 ssh2
```

What is the system's IP address? Other names? Location in the network? Geo location? Who is the owner? Who is the administator? What else happened to this system?

What does this number mean?
Is this documented somehwere?

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

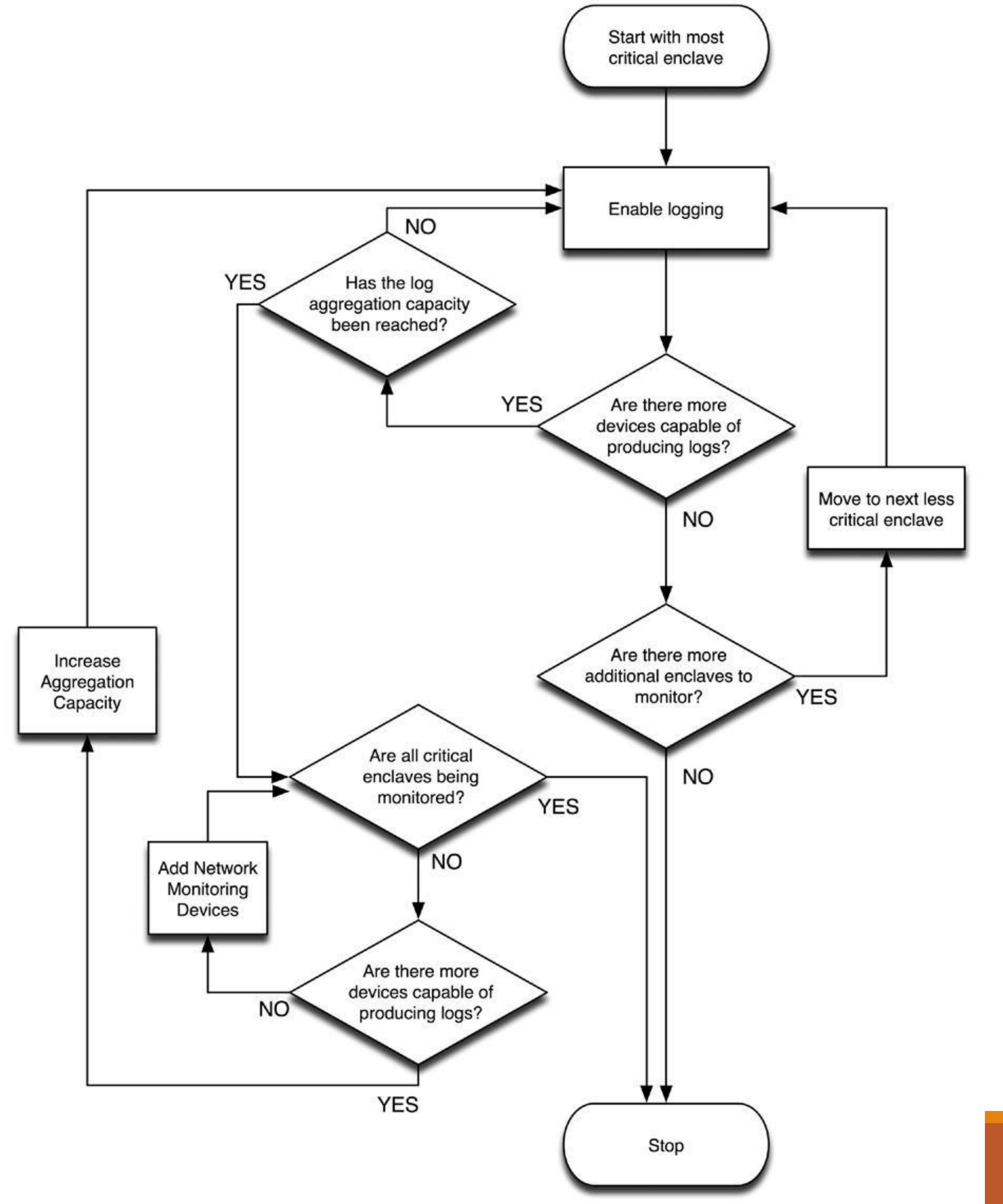
Monitoring Security Zones

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


Start with most critical enclave
Enable logging
NO
YES
Has the log aggregation capacity been reached?
YES
Are there more devices capable of producing logs?
NO
Move to next less critical enclave
Increase Aggregation Capacity
Are there more additional enclaves to monitor?
YES
NO
Are all critical enclaves being monitored?
YES
NO
Add Network Monitoring Devices
NO
Are there more devices capable of producing logs?
YES
Stop

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