HPE ArcSight Activate Framework

Multi-Sensor Data Fusion Model

Deploying SIEM is a cyclical, iterative process

Level 0: Event Generation & Transport

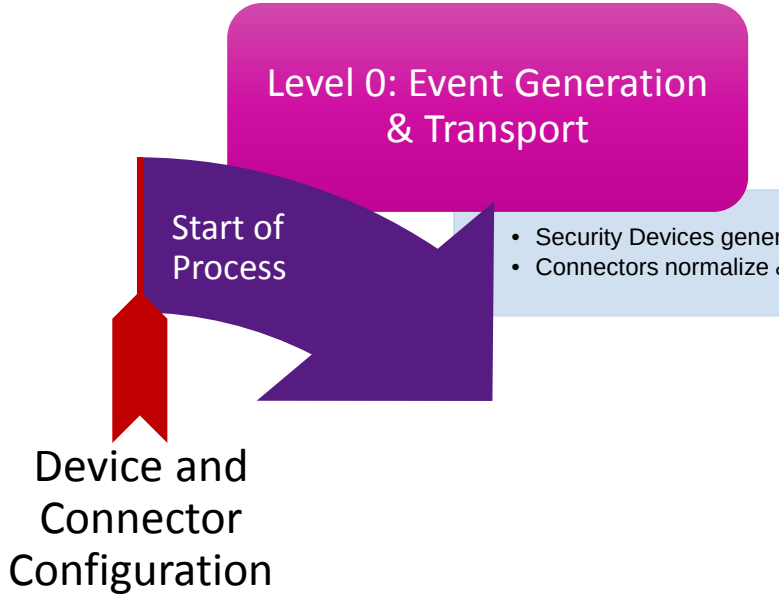
Deploying SIEM is a cyclical, iterative process

Level 0: Event Generation & Transport

- Security Devices generate the logs
- Connectors normalize & categorize the log entries into events

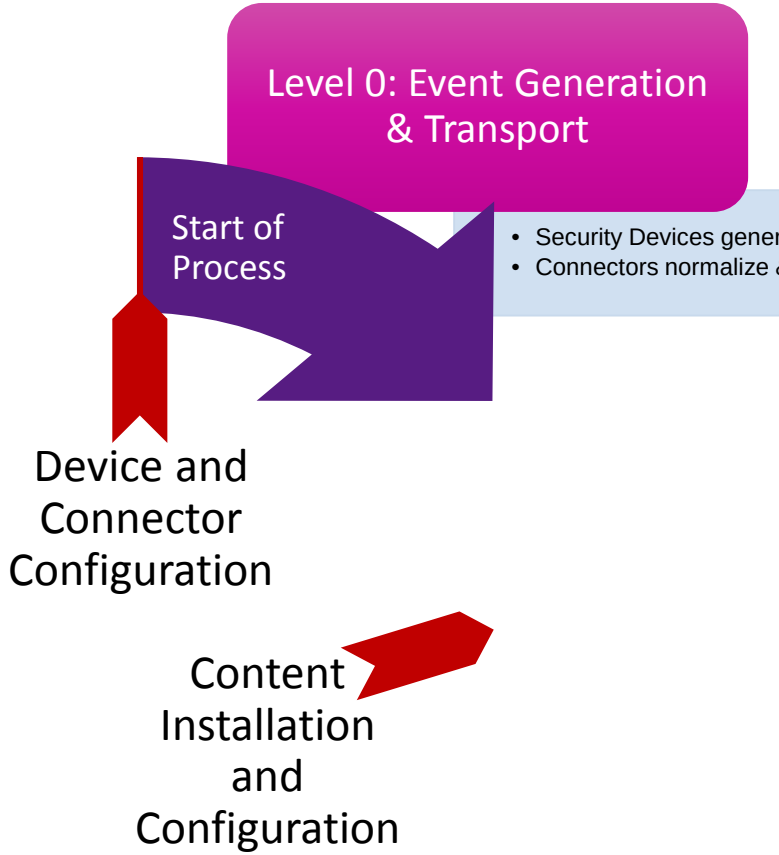
Deploying SIEM is a cyclical, iterative process

Deploying SIEM is a cyclical, iterative process



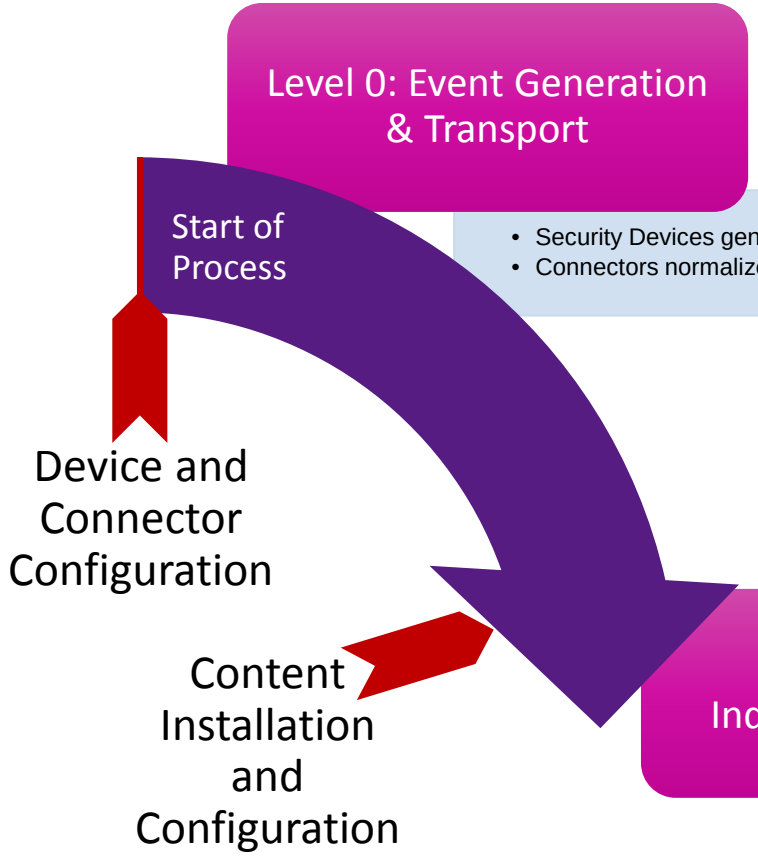
- Security Devices generate the logs
- Connectors normalize & categorize the log entries into events

Deploying SIEM is a cyclical, iterative process



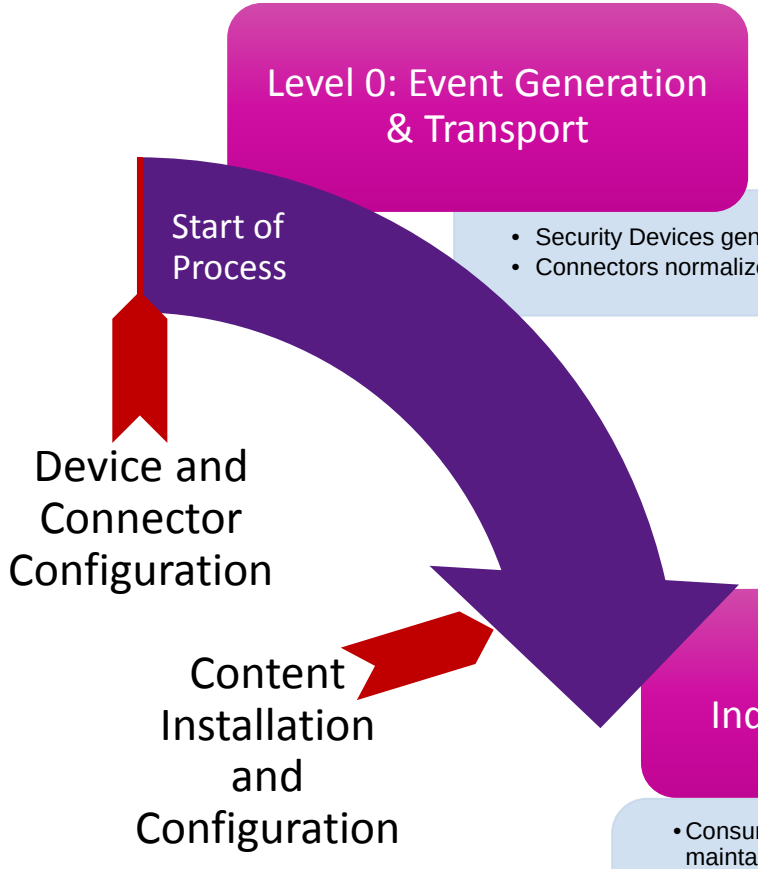
- Security Devices generate the logs
- Connectors normalize & categorize the log entries into events

Deploying SIEM is a cyclical, iterative process



- Security Devices generate the logs
- Connectors normalize & categorize the log entries into events

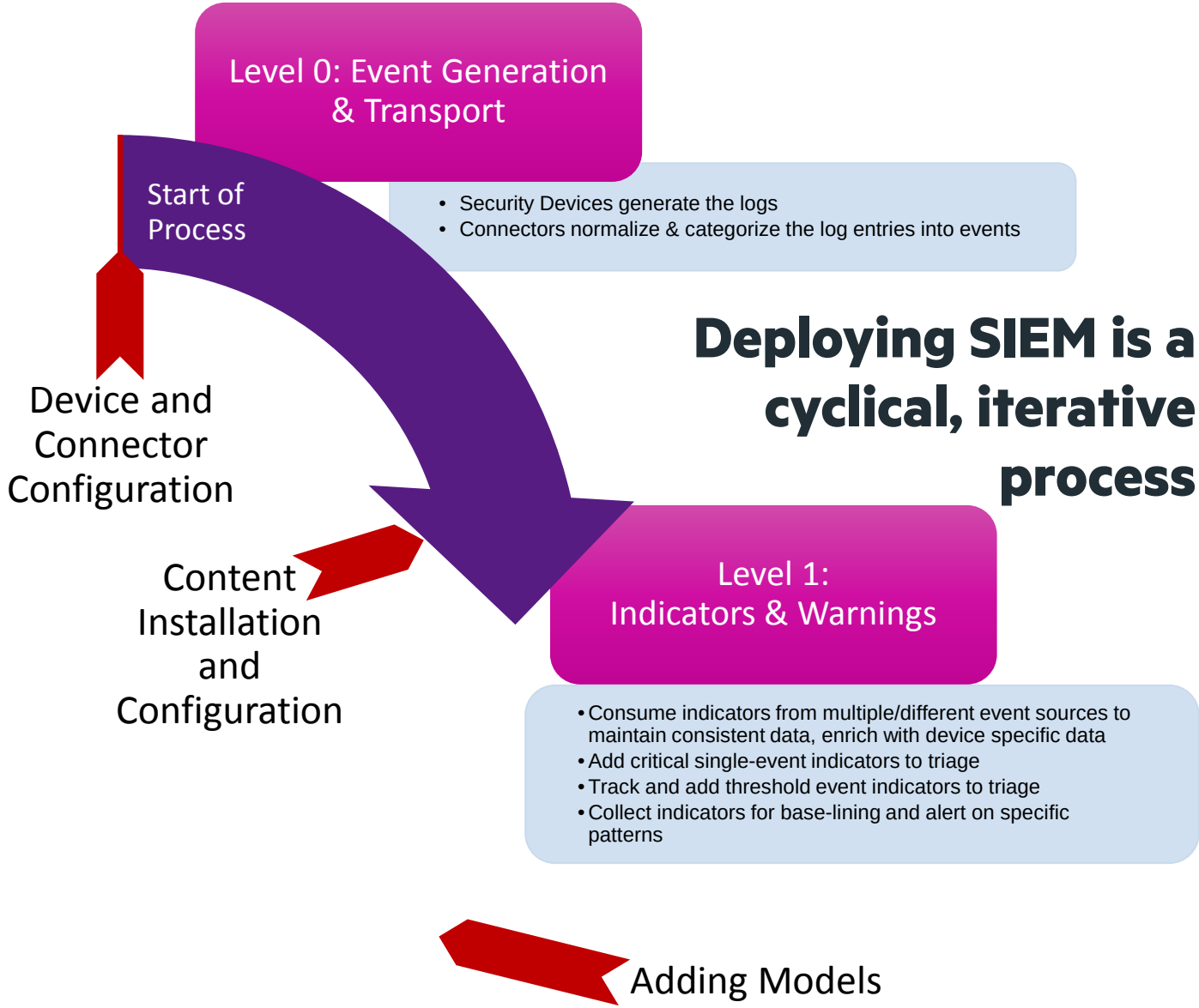
Deploying SIEM is a cyclical, iterative process

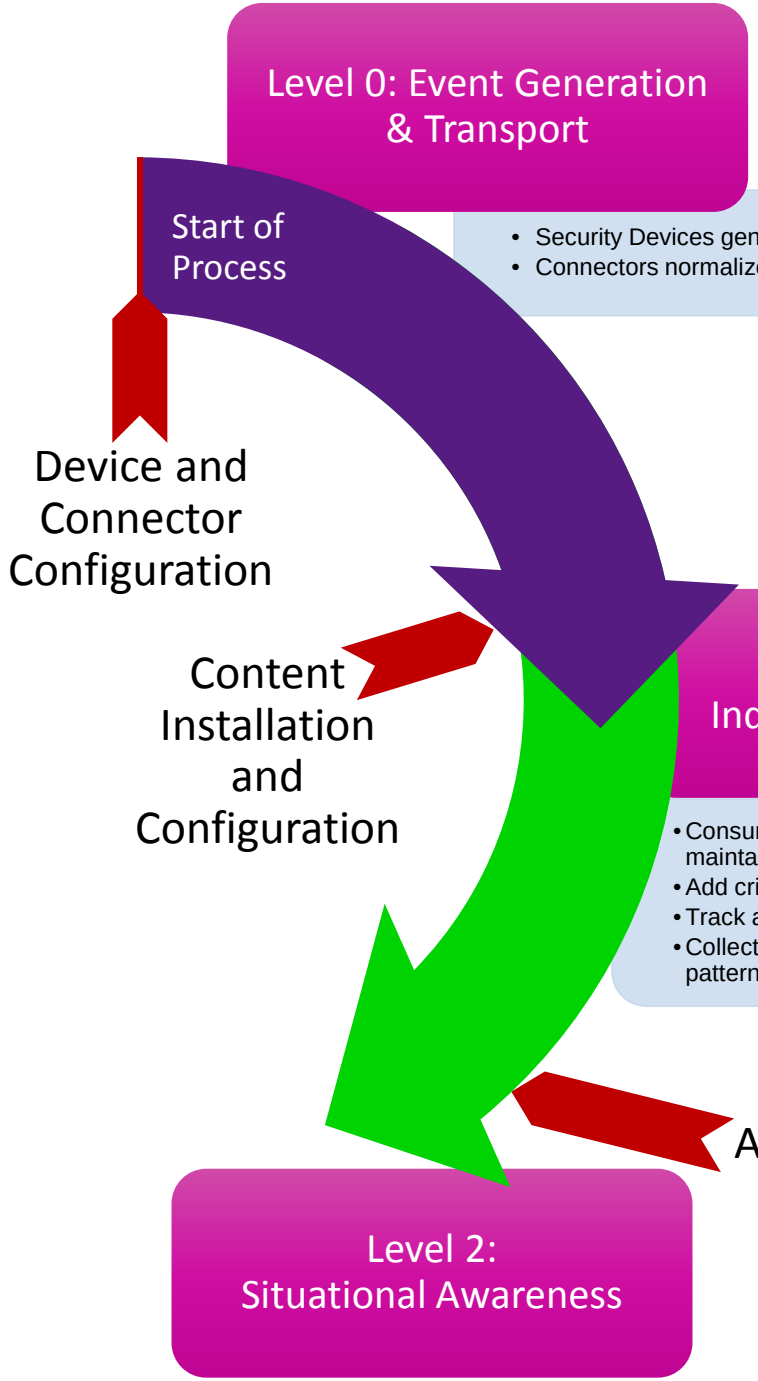


- Security Devices generate the logs
- Connectors normalize & categorize the log entries into events

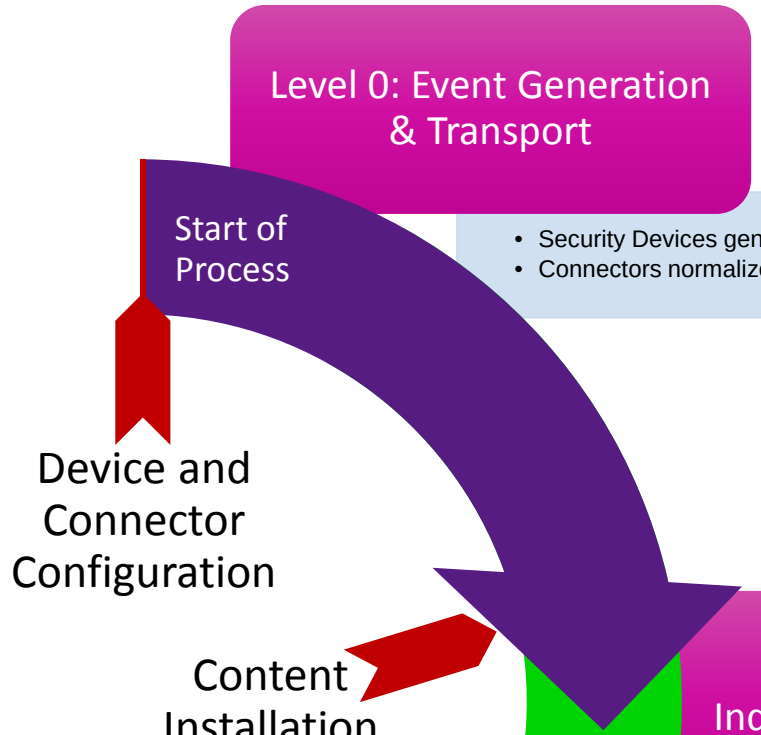
Deploying SIEM is a cyclical, iterative process

- Consume indicators from multiple/different event sources to maintain consistent data, enrich with device specific data
- Add critical single-event indicators to triage
- Track and add threshold event indicators to triage
- Collect indicators for base-lining and alert on specific patterns


Level 0: Event Generation & Transport
Start of Process
Security Devices generate the logs
Connectors normalize & categorize the log entries into events
Deploying SIEM is a cyclical, iterative process
Device and Connector Configuration
Content Installation and Configuration
Level 1: Indicators & Warnings
Consume indicators from multiple/different event sources to maintain consistent data, enrich with device specific data
Add critical single-event indicators to triage
Track and add threshold event indicators to triage
Collect indicators for base-lining and alert on specific patterns
Adding Models



Deploying SIEM is a cyclical, iterative process

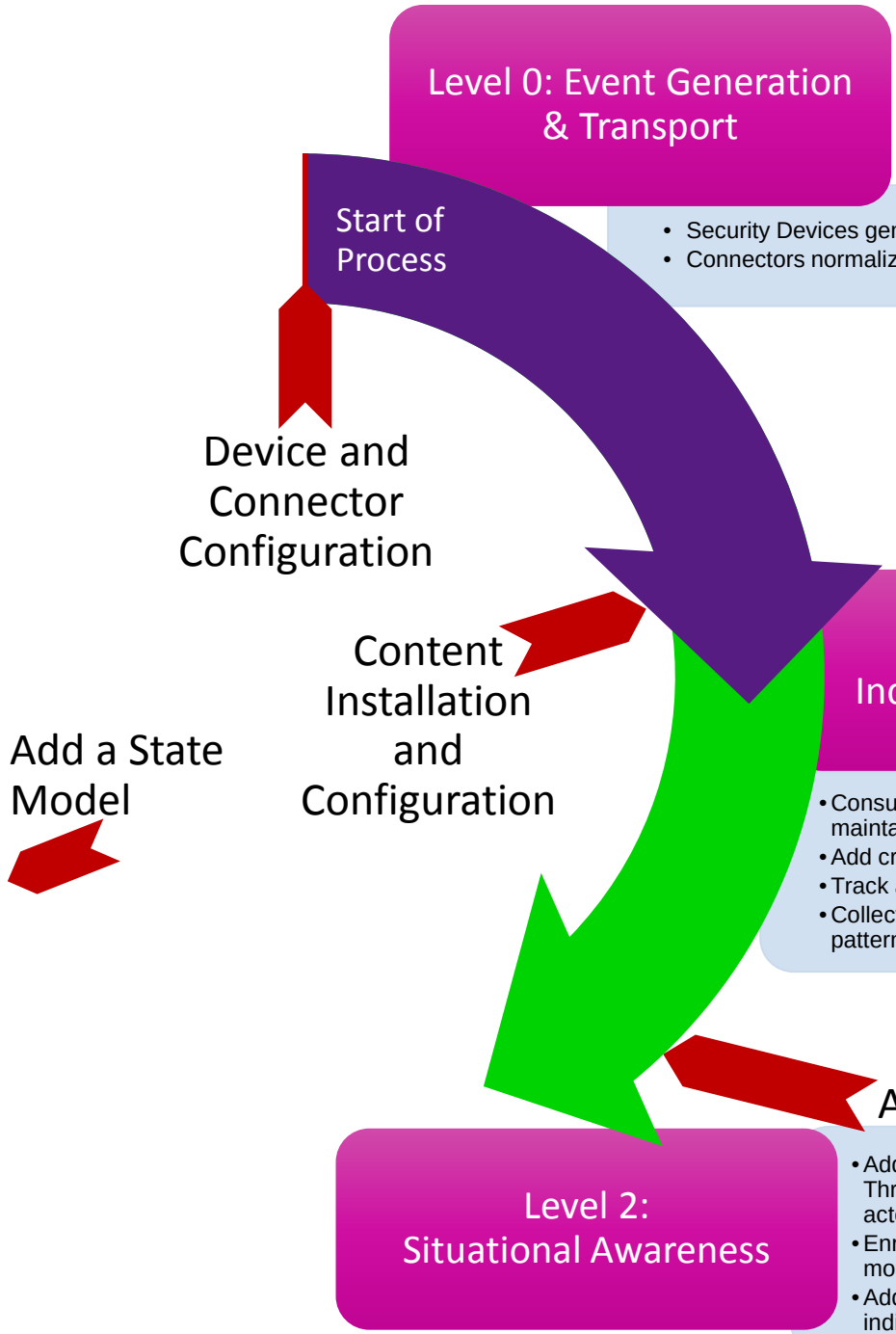


- Security Devices generate the logs
- Connectors normalize & categorize the log entries into events

Deploying SIEM is a cyclical, iterative process

- Consume indicators from multiple/different event sources to maintain consistent data, enrich with device specific data
- Add critical single-event indicators to triage
- Track and add threshold event indicators to triage
- Collect indicators for base-lining and alert on specific patterns

- Add models: Network, Asset (Host, Application), User, Data, Threat Intelligence (modeling of external networks and actors)
- Enrich indicators with situational awareness based on models
- Add critical single-event, threshold and baseline/anomaly indicators to triage



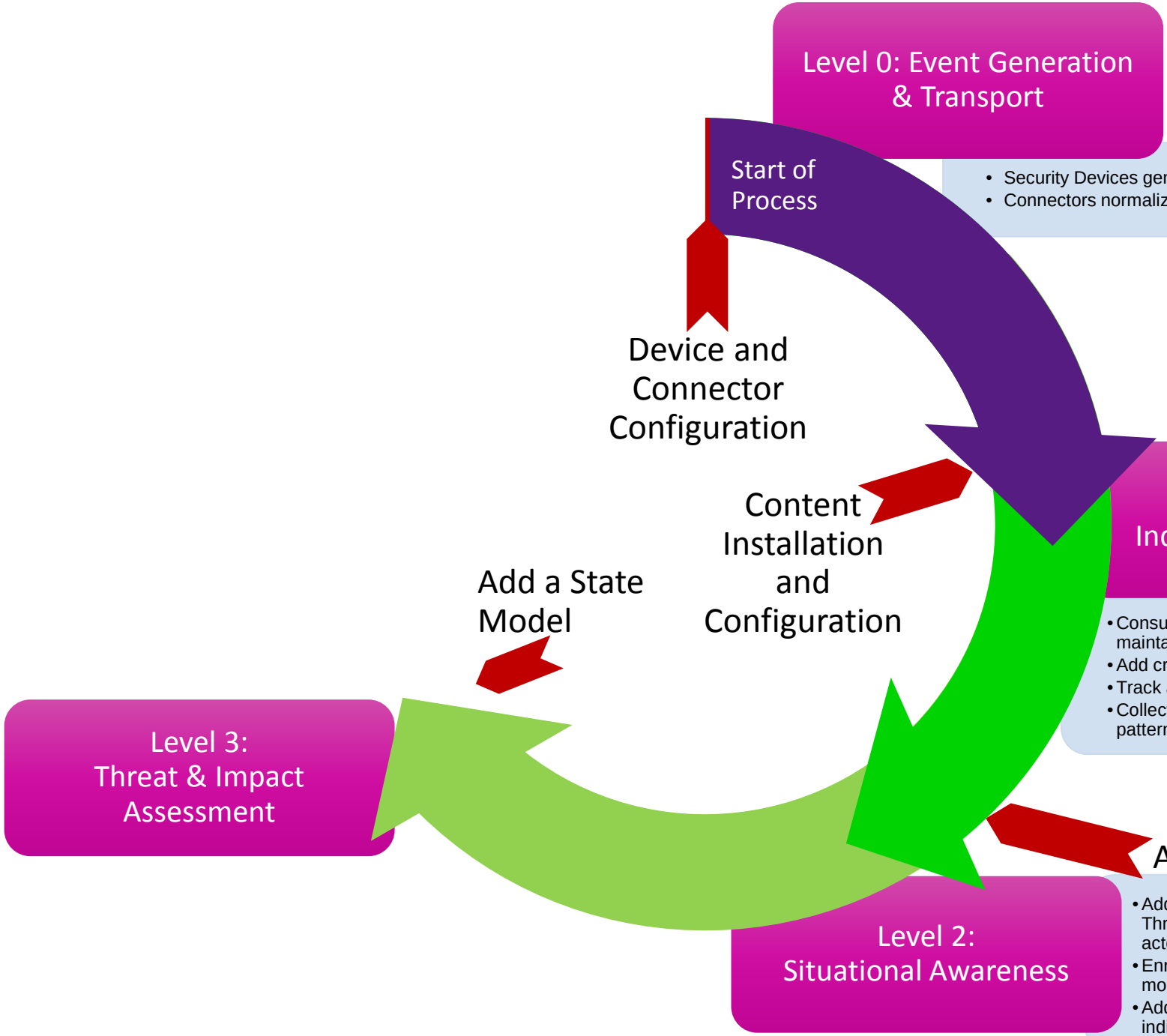
- Security Devices generate the logs
- Connectors normalize & categorize the log entries into events

Deploying SIEM is a cyclical, iterative process

- Consume indicators from multiple/different event sources to maintain consistent data, enrich with device specific data
- Add critical single-event indicators to triage
- Track and add threshold event indicators to triage
- Collect indicators for base-lining and alert on specific patterns

- Add models: Network, Asset (Host, Application), User, Data, Threat Intelligence (modeling of external networks and actors)
- Enrich indicators with situational awareness based on models
- Add critical single-event, threshold and baseline/anomaly indicators to triage

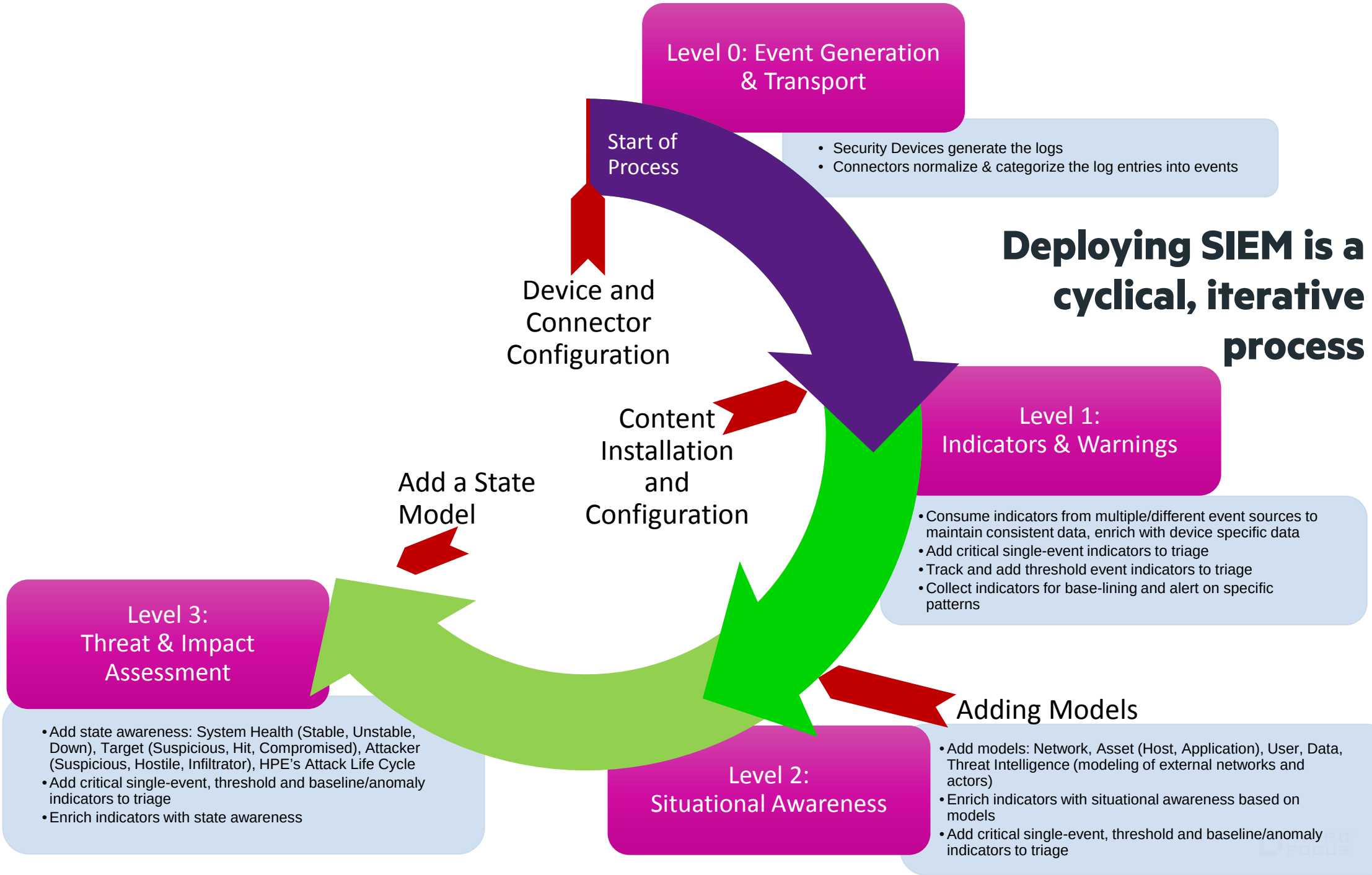
Deploying SIEM is a cyclical, iterative process



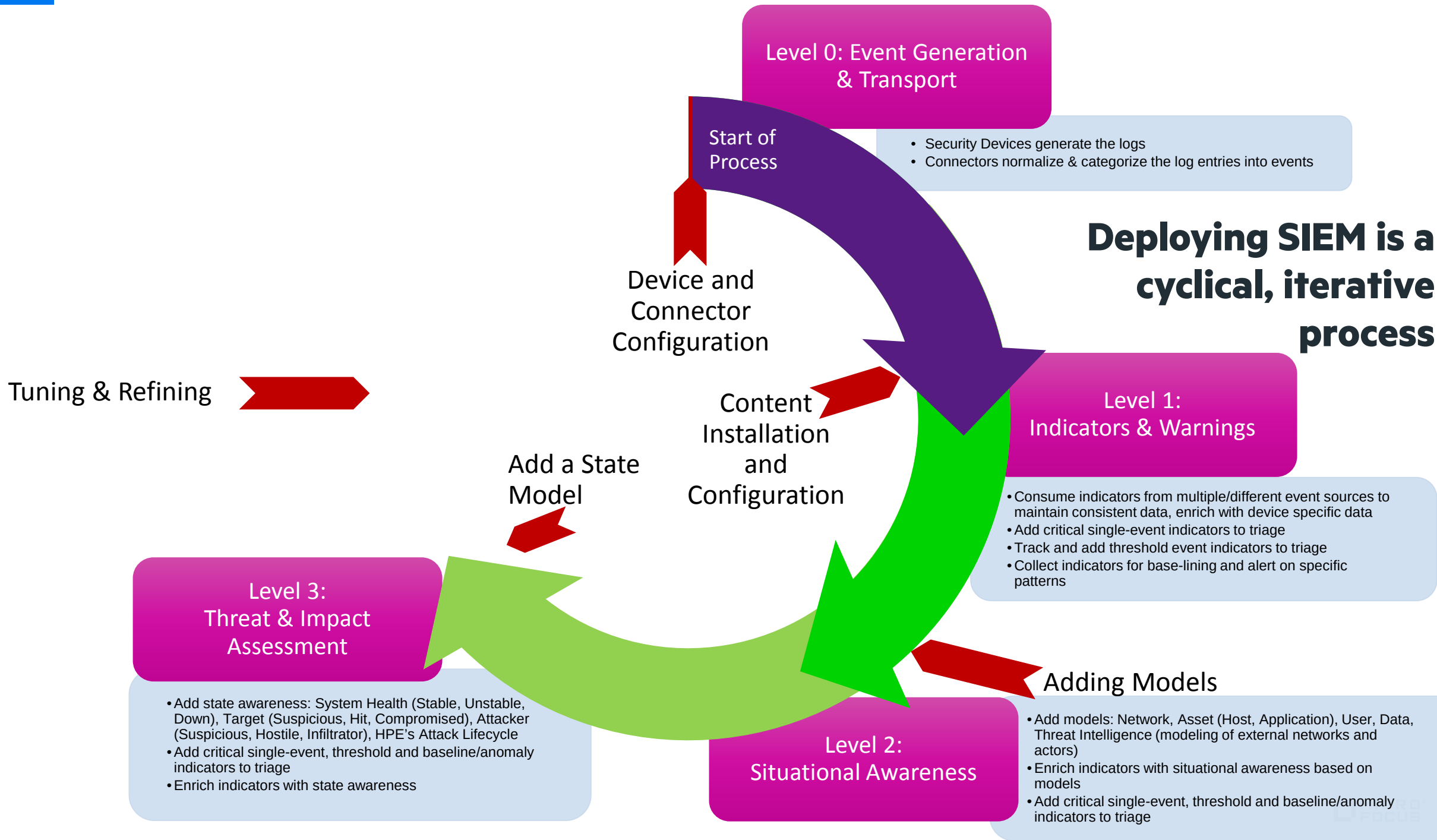
- Security Devices generate the logs
- Connectors normalize & categorize the log entries into events

- Consume indicators from multiple/different event sources to maintain consistent data, enrich with device specific data
- Add critical single-event indicators to triage
- Track and add threshold event indicators to triage
- Collect indicators for base-lining and alert on specific patterns

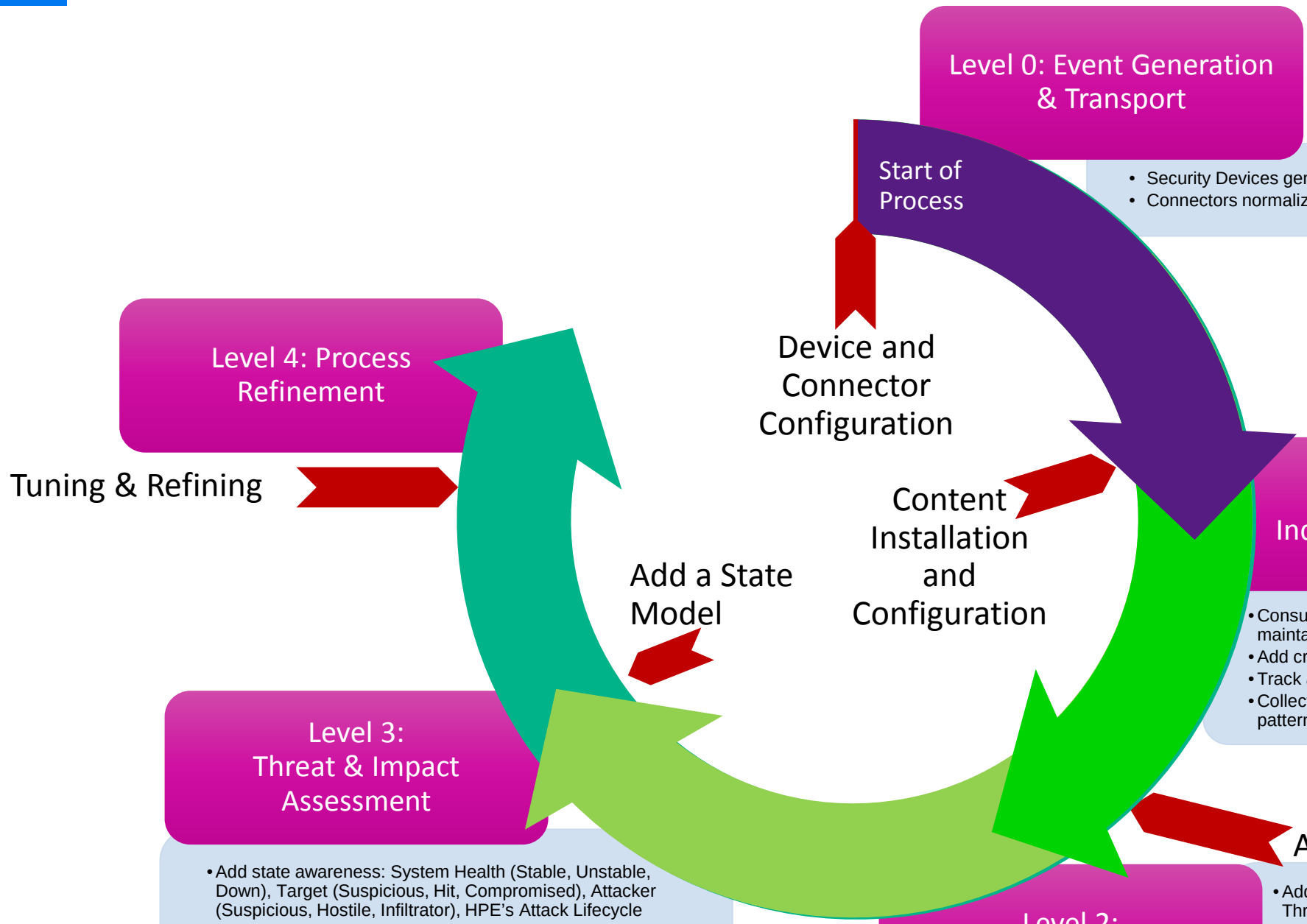
- Add models: Network, Asset (Host, Application), User, Data, Threat Intelligence (modeling of external networks and actors)
- Enrich indicators with situational awareness based on models
- Add critical single-event, threshold and baseline/anomaly indicators to triage


Level 0: Event Generation & Transport
Start of Process
Security Devices generate the logs
Connectors normalize & categorize the log entries into events
Deploying SIEM is a cyclical, iterative process
Device and Connector Configuration
Content Installation and Configuration
Level 1: Indicators & Warnings
Consume indicators from multiple/different event sources to maintain consistent data, enrich with device specific data
Add critical single-event indicators to triage
Track and add threshold event indicators to triage
Collect indicators for base-lining and alert on specific patterns
Adding Models
Level 2: Situational Awareness
Add models: Network, Asset (Host, Application), User, Data, Threat Intelligence (modeling of external networks and actors)
Enrich indicators with situational awareness based on models
Add critical single-event, threshold and baseline/anomaly indicators to triage
Add a State Model
Level 3: Threat & Impact Assessment
Add state awareness: System Health (Stable, Unstable, Down), Target (Suspicious, Hit, Compromised), Attacker (Suspicious, Hostile, Infiltrator), HPE's Attack Life Cycle
Add critical single-event, threshold and baseline/anomaly indicators to triage
Enrich indicators with state awareness

Deploying SIEM is a cyclical, iterative process



Deploying SIEM is a cyclical, iterative process



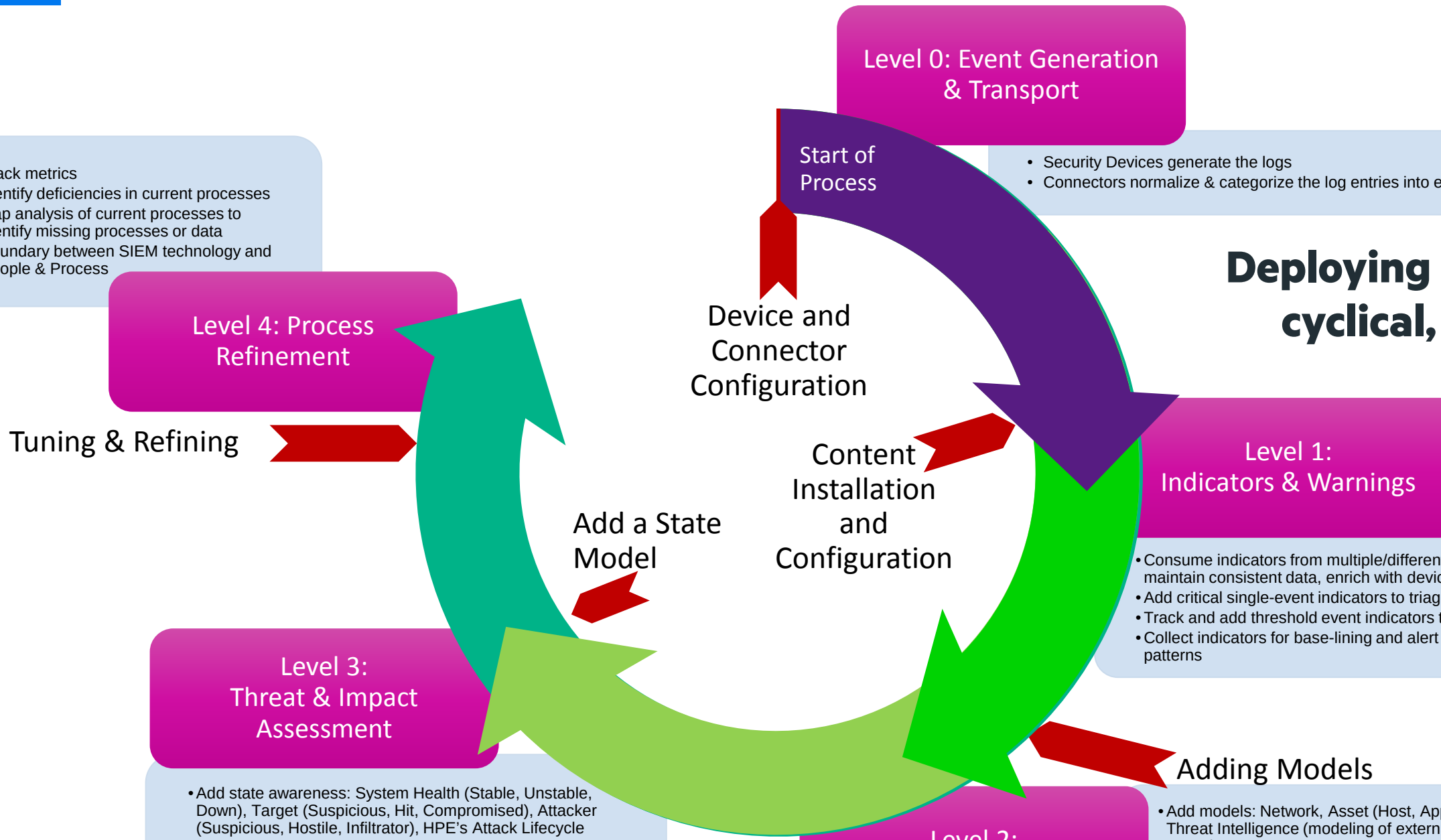
- Security Devices generate the logs
- Connectors normalize & categorize the log entries into events

- Consume indicators from multiple/different event sources to maintain consistent data, enrich with device specific data
- Add critical single-event indicators to triage
- Track and add threshold event indicators to triage
- Collect indicators for base-lining and alert on specific patterns

- Add state awareness: System Health (Stable, Unstable, Down), Target (Suspicious, Hit, Compromised), Attacker (Suspicious, Hostile, Infiltrator), HPE's Attack Lifecycle
- Add critical single-event, threshold and baseline/anomaly indicators to triage
- Enrich indicators with state awareness

- Add models: Network, Asset (Host, Application), User, Data, Threat Intelligence (modeling of external networks and actors)
- Enrich indicators with situational awareness based on models
- Add critical single-event, threshold and baseline/anomaly indicators to triage

Deploying SIEM is a cyclical, iterative process



- Security Devices generate the logs
- Connectors normalize & categorize the log entries into events

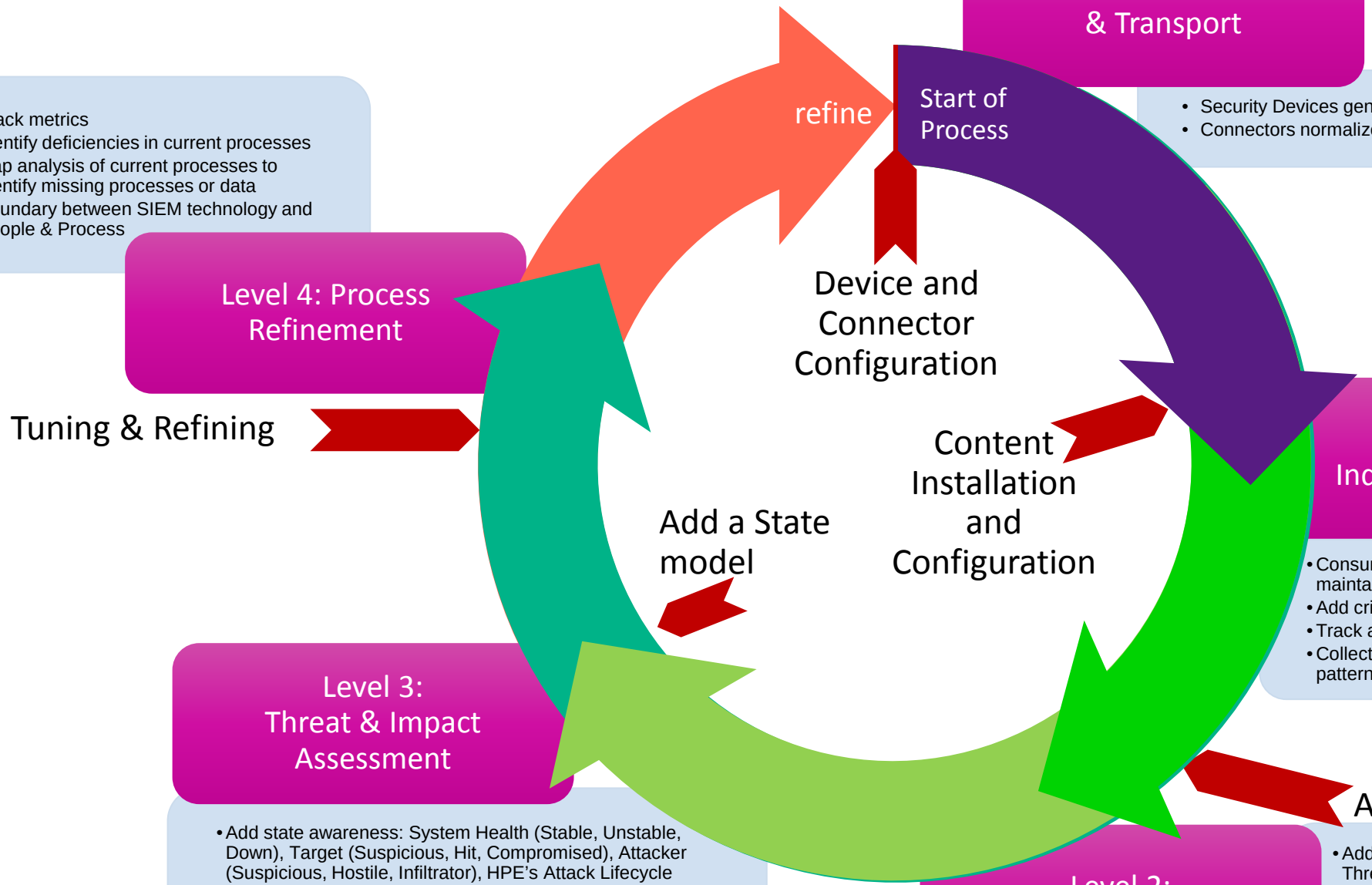
- Consume indicators from multiple/different event sources to maintain consistent data, enrich with device specific data
- Add critical single-event indicators to triage
- Track and add threshold event indicators to triage
- Collect indicators for base-lining and alert on specific patterns

- Add models: Network, Asset (Host, Application), User, Data, Threat Intelligence (modeling of external networks and actors)
- Enrich indicators with situational awareness based on models
- Add critical single-event, threshold and baseline/anomaly indicators to triage

- Add state awareness: System Health (Stable, Unstable, Down), Target (Suspicious, Hit, Compromised), Attacker (Suspicious, Hostile, Infiltrator), HPE's Attack Lifecycle
- Add critical single-event, threshold and baseline/anomaly indicators to triage
- Enrich indicators with state awareness

- Track metrics
- Identify deficiencies in current processes
- Gap analysis of current processes to identify missing processes or data
- Boundary between SIEM technology and People & Process

Deploying SIEM is a cyclical, iterative process



Level 0: Event Generation & Transport

- Security Devices generate the logs
- Connectors normalize & categorize the log entries into events

Level 1: Indicators & Warnings

- Consume indicators from multiple/different event sources to maintain consistent data, enrich with device specific data
- Add critical single-event indicators to triage
- Track and add threshold event indicators to triage
- Collect indicators for base-lining and alert on specific patterns

Level 2: Situational Awareness

- Add models: Network, Asset (Host, Application), User, Data, Threat Intelligence (modeling of external networks and actors)
- Enrich indicators with situational awareness based on models
- Add critical single-event, threshold and baseline/anomaly indicators to triage

Level 3: Threat & Impact Assessment

- Add state awareness: System Health (Stable, Unstable, Down), Target (Suspicious, Hit, Compromised), Attacker (Suspicious, Hostile, Infiltrator), HPE's Attack Lifecycle
- Add critical single-event, threshold and baseline/anomaly indicators to triage
- Enrich indicators with state awareness

Level 4: Process Refinement

- Track metrics
- Identify deficiencies in current processes
- Gap analysis of current processes to identify missing processes or data
- Boundary between SIEM technology and People & Process

The Data Fusion Model

Level 4: Process Refinement	•Track metrics •Identify deficiencies in current processes •Gap analysis of current processes to identify missing processes or data •Boundary between SIEM technology and People & Process
Level 3: Threat & Impact Assessment	•Add state awareness: System Health (Stable, Unstable, Down), Target (Suspicious, Hit, Compromised), Attacker (Suspicious, Hostile, Infiltrator), HPE's Attack Lifecycle •Enrich indicators with state awareness •Add critical single-event, threshold and baseline/anomaly indicators to triage
Level 2: Situational Awareness	•Add models: Network, Asset (Host, Application), User, Data, Threat Intelligence (modeling of external networks and actors) •Enrich indicators with situational awareness based on models •Add critical single-event, threshold and baseline/anomaly indicators to triage
Level 1: Indicators & Warnings	•Consume indicators from multiple/different event sources to maintain consistent data, enrich with device specific data •Add critical single-event indicators to triage •Track and add threshold event indicators to triage •Collect indicators for base-lining and alert on specific patterns
Level 0: Security Devices and Connectors	• Security Devices generate the logs • Connectors normalize & categorize the log entries into events