Attack Trees for Selected Electric Sector High Risk Failure Scenarios

NESCOR

Version 2.0

Annabelle Lee
Sr. Technical Executive

December 2015

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Slide Set Background and Purpose

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

- Contains key results from NESCOR* document: “Analysis of Selected Electric Sector High Risk Failure Scenarios” [2]
  - Failure scenarios selected from the prior NESCOR document “Electric Sector Failure Scenarios and Impact Analyses” [1]
- PowerPoint format supports:
  - Tailoring of information by utilities
  - Use of information in a meeting setting

*NESCOR – National Electric Sector Cybersecurity Organization Resource

Overview of Slide Set

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

- Attack tree notation
- Attack trees for selected failure scenarios, with
  - Short text descriptions
  - Relevant architecture diagrams for some scenarios
- Common sub trees
  - These are modular fragments of attack trees, reused within failure scenario trees
  - Attack sub trees with short text descriptions
- Acronym list

Selected Failure Scenarios

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

- **AMI.1*** - *Mass Meter Disconnect*
- **AMI.9** - *Invalid Disconnect Messages to Meters Impact Customers and Utility*
- **AMI.12** - *Improper Firewall Configuration Exposes Customer Data*
- **AMI.14** - *Breach of Cellular Provider's Network Exposes AMI Access*
- **AMI.16** - *Compromised Head end Allows Impersonation of CA*
- **AMI.27** - *Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control*
- **AMI.29** - *Unauthorized Device Acquires HAN Access and Steals PII*
- **AMI.32* -** *Power Stolen by Reconfiguring Meter via Optical Port*
- **DGM.11*** - *Threat Agent Triggers Blackout via Remote Access to Distribution System*
- **DR.1** - *Blocked DR Messages Result in Increased Prices or Outages*
- **DR.4** - *Improper DRAS Configuration Causes Inappropriate DR Messages*

* For these scenarios, a detailed text format analysis can be found in [2]. For all scenarios, a brief text format analysis can be found in [1].

Selected Failure Scenarios (2)

- **Gen.1*** - *Threat agent adds spurious trip parameters on remotely located plant support equipment and trips unit offline*
- **Gen.15*** - *Plant tripped off-line through access gained through a compromised vendor remote connection*

* For these scenarios, a detailed text format analysis can be found in [2]. For all scenarios, a brief text format analysis can be found in [1].

Attack Tree Notation Quick Start

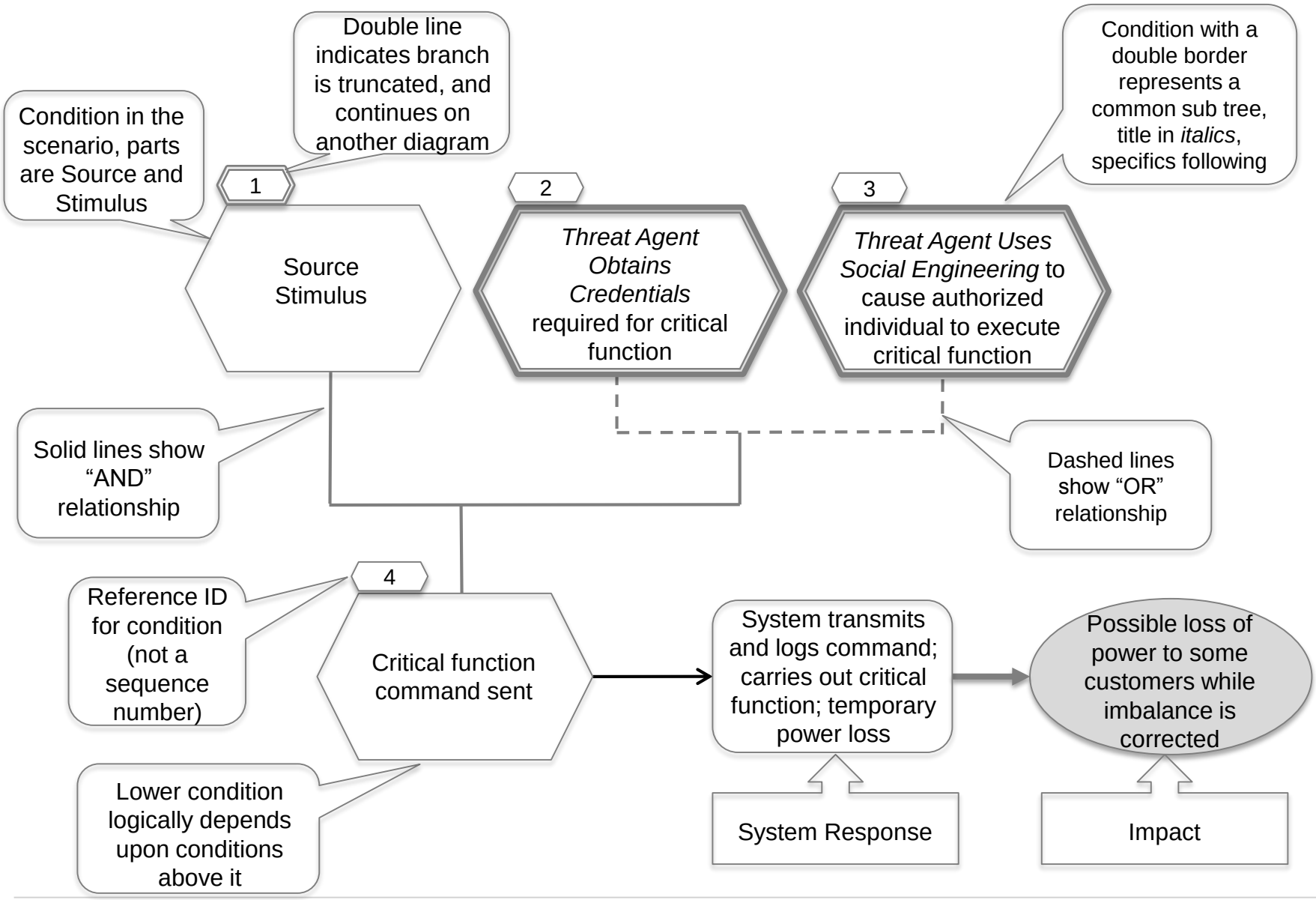
- The generic example on the next slide illustrates how to read an attack tree.
- The tree is shown on each slide, with truncated branches represented by double lines around the numbered small hexagons. These branches are then shown on another slide.
- The *common sub trees* referenced in the attack trees are fragments of attack trees which were found to be repeated across many different trees as well as within attack trees.
  - More appropriate to present them once, and then invoke them using relevant references.
  - The large hexagon that names the common sub tree has a double outline.
- *Common mitigations* are in italics, followed by specifics for the failure scenario.

Common Sub Trees

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

- Threat Agent Gains Capability to Reconfigure <firewall>
- Threat Agent Blocks Wireless Communication Channel Connecting <x and y>
- Authorized Employee Brings Malware into <system or network>
- Threat Agent Obtains Credentials for <system or function>
- Threat Agent Uses Social Engineering to <desired outcome>
- Threat Agent Exploits Firewall Gap <specific firewall>
- Threat Agent Exfiltrates <data>
- Threat Agent Gains Access to <network>

Attack Tree Notation Icons



AMI.1 Mass Meter Remote Disconnect by Authorized Individual

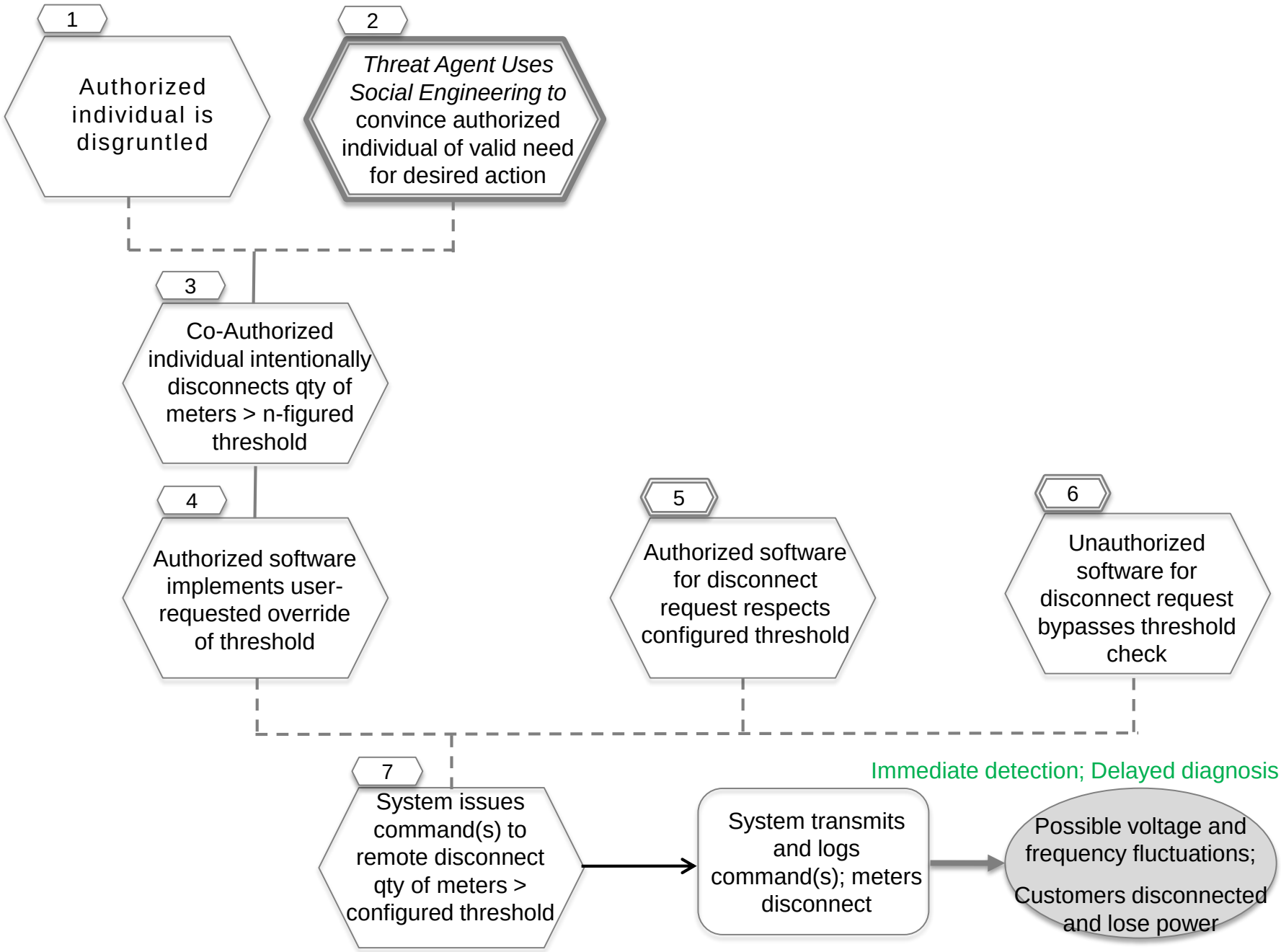
Description

An authorized individual (defined as an individual who legitimately has privileges to remotely disconnect meters) issues a command or commands that causes disconnect of a massive number of meters within a short time period.

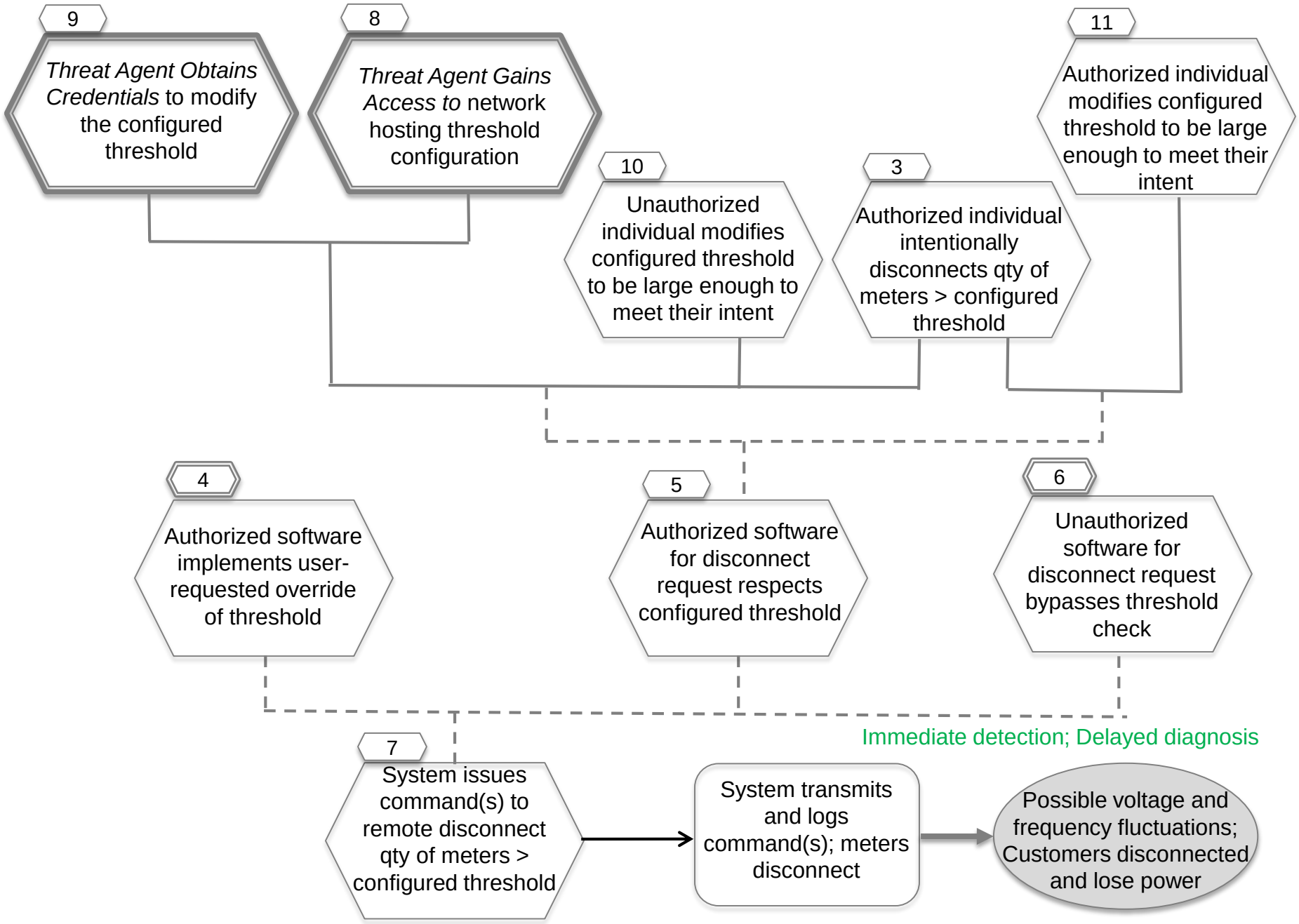
Assumptions

- Two stage disconnect process – request and implement
- Authentication and roles in place for disconnect request
- Implement stage warns when meter quantity threshold exceeded (stronger enforcement not assumed)
- Implement stage verifies business rules such as critical service, billing status
- Remote install of software requires VPN connection and strong authentication
- Requests for disconnect are logged with user name, log strongly protected.

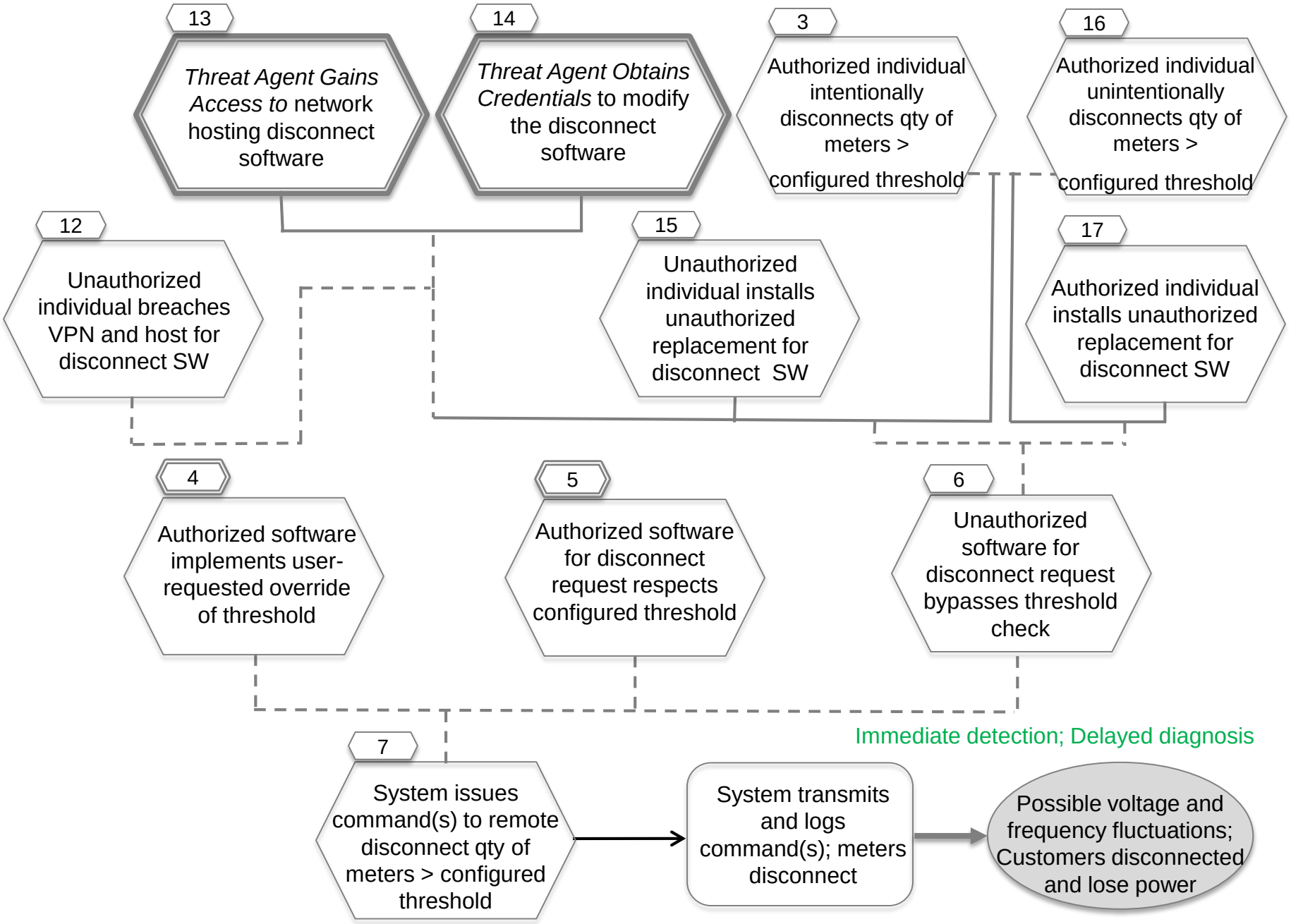
AMI.1 Authorized Individual Issues Unauthorized Mass Remote Disconnect (1/3)



AMI.1 Authorized Individual Issues Unauthorized Mass Remote Disconnect (2/3)



AMI.1 Authorized Individual Issues Unauthorized Mass Remote Disconnect (3/3)



AMI.1 Authorized Individual Issues Unauthorized Mass Remote Disconnect

Potential Mitigations

1 – *Verify personnel* using background checks

2 – See common sub tree *Threat Agent Uses Social Engineering to* <desired outcome>

3 – *Limit events:* do not support override of number of disconnects*; require two-person rule* for override

6 - *Require application whitelisting*

8 – See common sub tree *Threat Agent Gains Access to <network >*

9 – See common sub tree *Threat Agent Obtains Credentials* for <system or function>

10 ,11 – *Require 2 person rule*; *generate alert* for change to threshold setting or file

12 – *Create policy* for changing passwords, *maintain patches* in VPN SW

12 – *require strong host password* or other credentials; *harden platform* of host

AMI.1 Authorized Individual Issues Unauthorized Mass Remote Disconnect

Potential Mitigations (2)

13 – See common sub tree *Threat Agent Gains Access to <network >*

14 – See common sub tree *Threat Agent Obtains Credentials* for <system or function>

15 – *check SW file integrity*

16 – none

15, 17 – *generate alert* on changes to critical files

AMI.9 Invalid Disconnect Messages to Meters Impact Customers and Utility

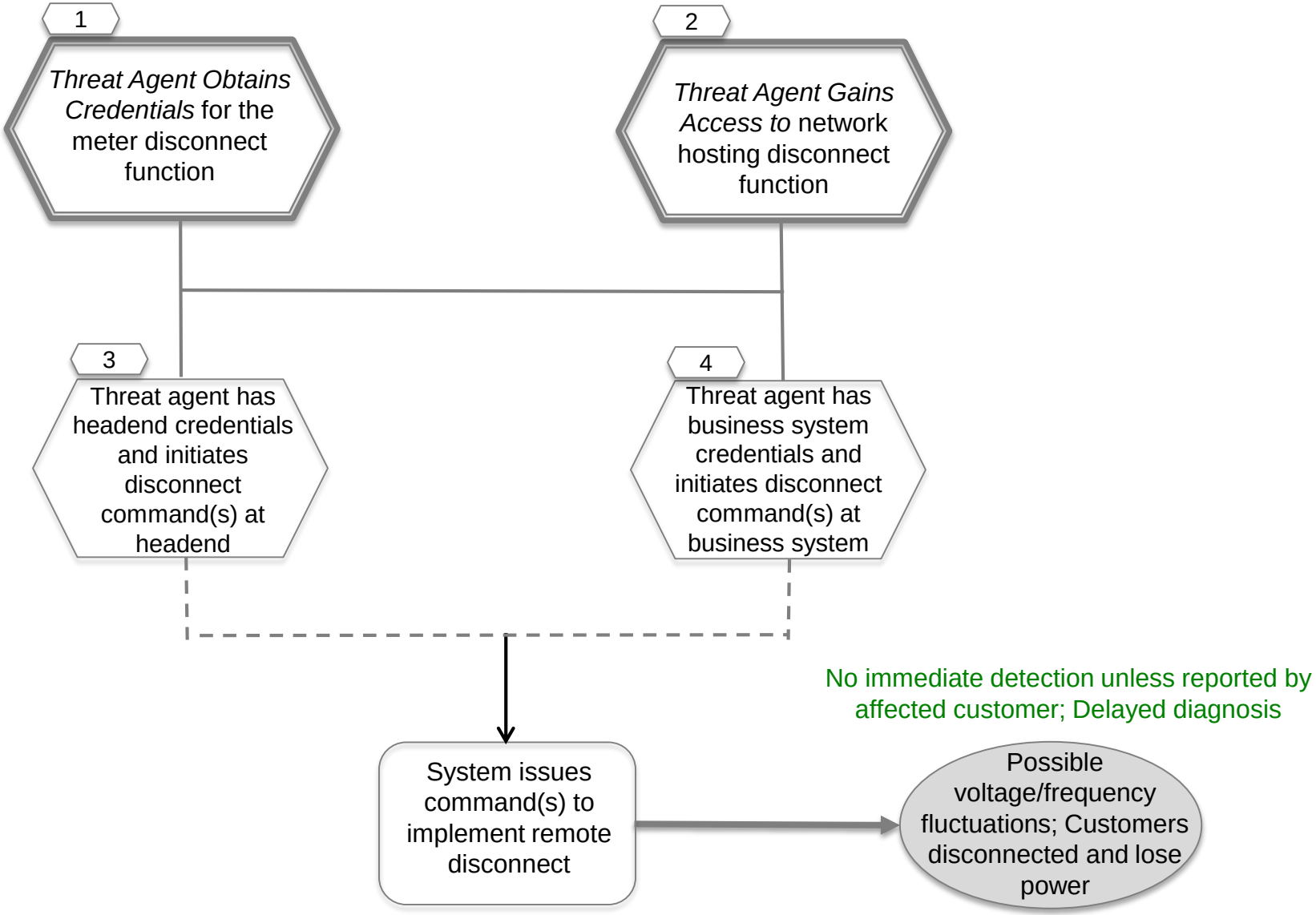
Description

A threat agent obtains legitimate credentials to the AMI system via social engineering. The threat agent may already have access to the network on which this system resides or may succeed in reaching the network from another network. The threat agent issues a disconnect command for one or more target meters. Alternatively, a disconnect may be placed in a schedule and then occur automatically at a later time.

Assumptions

- No Internet access from AMI headend
- A limited number of individuals have privilege to do disconnects

AMI.9: Invalid Disconnect Messages to Meters Impact Customers and Utility



AMI.9: Invalid Disconnect Messages to Meters Impact Customers and Utility

Potential Mitigations

1 - *Verify personnel* using background checks

1 - See common sub tree *Threat Agent Obtains Credentials* for <system or function>

2 - See common sub tree *Threat Agent Gains Access to <Network >*

3 - *Design for security* by not permitting disconnects originating from headend (For example, require meter to verify signature by business system)

4 - *Cross check* payment status and critical service against business rules

4 - *Enforce least privilege* to a minimum number of individuals requiring MDMS access

4 - *Generate alerts* for users to another instance of their account in use (if they are logged in), and time of last login

4 - *Detect unusual patterns* of disconnects on smart meters

AMI.12: Improper Firewall Configuration Exposes Customer Data

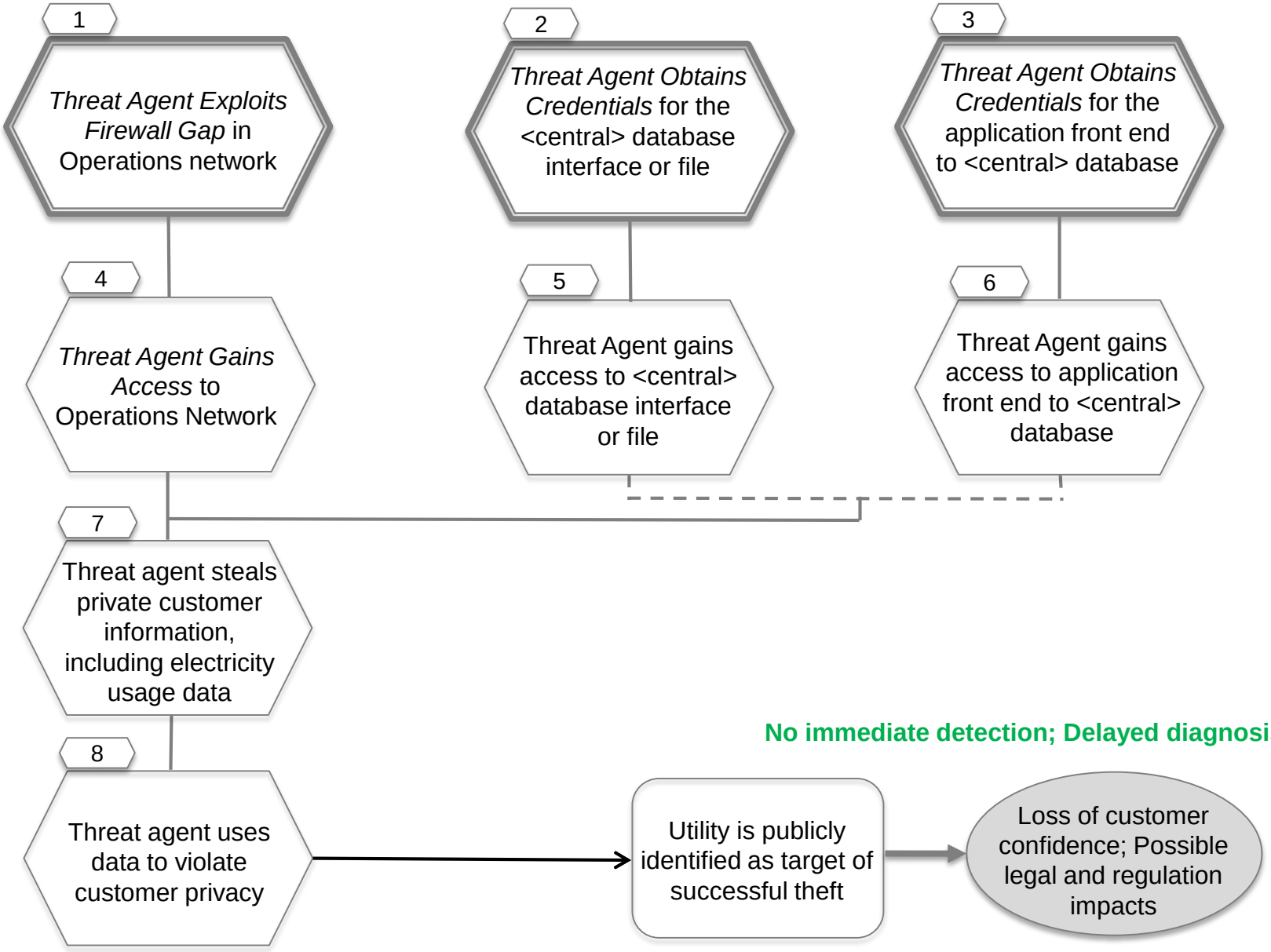
Description

A firewall rule is intentionally or unintentionally created allowing direct access from another network. Taking advantage of this rule, a threat agent subsequently gains access to the [central] database that receives data from the customer accounts database, [and from the energy usage application]. This enables the threat agent to steal customer identifiable information, including electricity usage data.

Assumptions

- Authentication and roles in place for access to customer data
- Operations network hosts customer private data

AMI.12: Improper Firewall Configuration Exposes Customer Data



AMI.12: Improper Firewall Configuration Exposes Customer Data

Potential Mitigations

1 – See common sub tree *Threat Agent Finds Firewall Gap in* <specific firewall>

2, 3 – See common sub tree *Threat Agent Obtains Credentials for* <system or function>

4 – *Require authentication* to the network

4 – *Enforce least privilege* for individuals with access to hosts on the network

4 – *Detect unusual patterns* of usage on hosts and network

5, 6 - Enforce least privilege to limit central database/application access to authorized applications and/or locally authenticated users

AMI.14 Breach of Cellular Provider's Network Exposes AMI Access

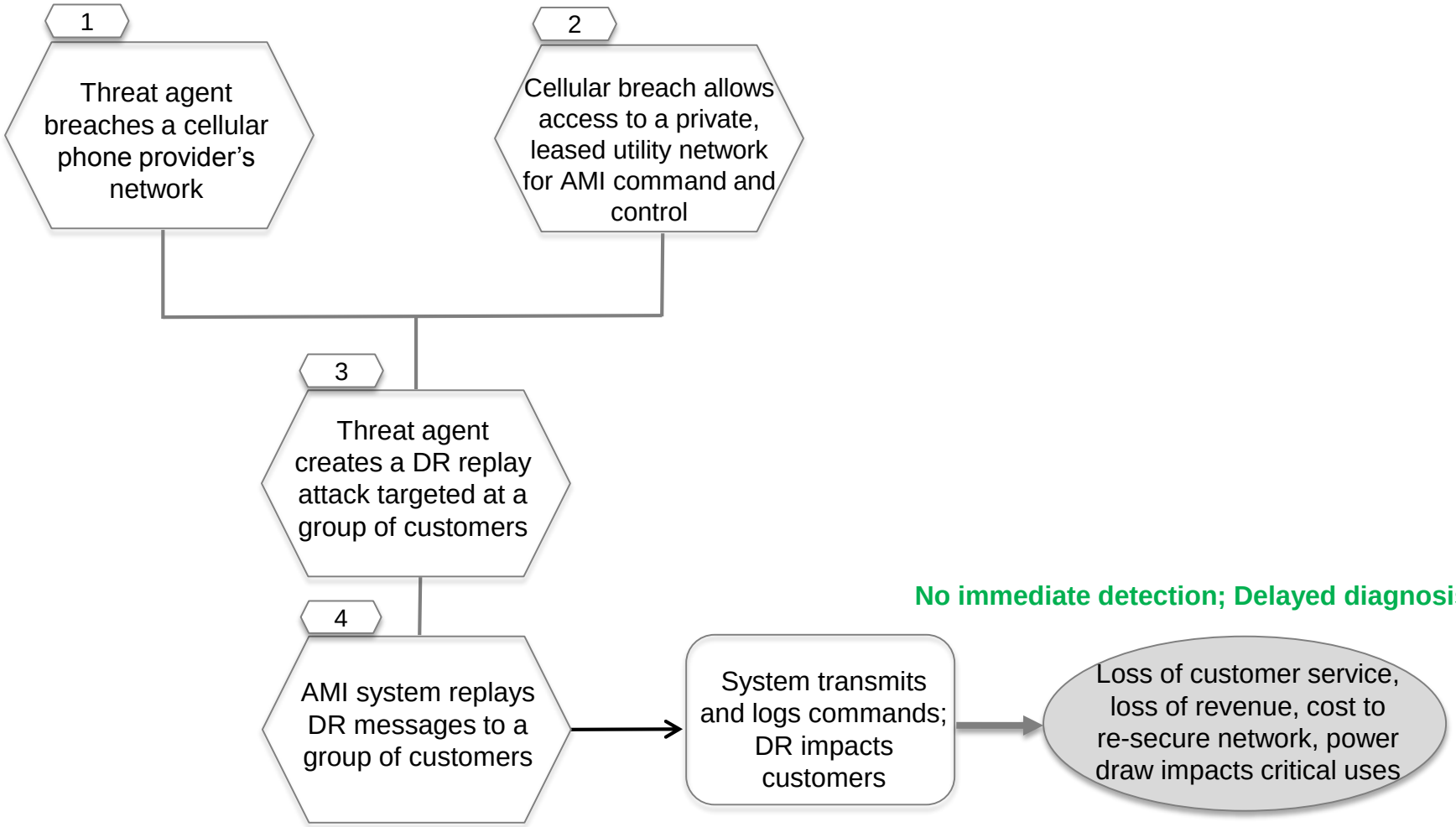
Description

A cellular phone provider's network is breached, allowing access to a private network leased to a utility for AMI command and control. The AMI implementation is vulnerable to replay attacks and DR messages are replayed to a group of customers.

Assumptions

- Inadequate separation of private leased networks between cellular phone provider and leased utility network for AMI
- Weak or no cryptography for network access
- Replay ability for commands

AMI.14: Breach of Cellular Provider's Network Exposes AMI Access



AMI.14 Breach of Cellular Provider's Network Exposes AMI Access

Potential Mitigations

1, 2 - *Isolate networks* using different encryption keys to prevent a breach in one network from affecting another network

2 - Require approved cryptographic algorithms at the link layer to prevent a threat agent from being able to affect the confidentiality and integrity on the AMI network if a breach should occur

3 - Protect against replay using time-stamping or other methods

AMI.16: Compromised Headend Allows Impersonation of CA

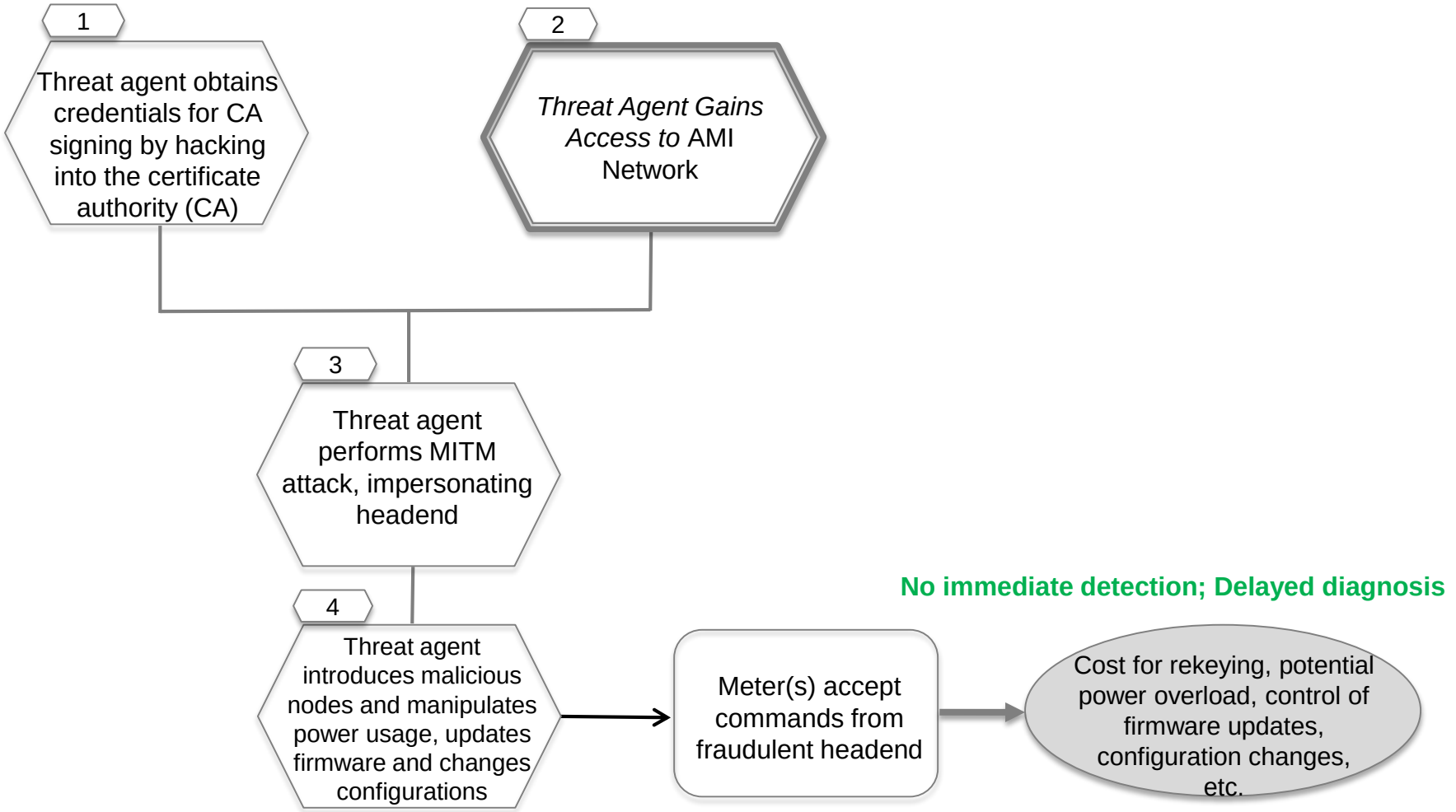
Description

The private key for the certificate authority (CA) used to set up a Public Key Infrastructure (PKI) at the head end is compromised, which allows a threat agent to impersonate the CA.

Assumptions

- No cryptography for AMI network access
- PKI is used on the AMI network

AMI.16: Compromised Headend Allows Impersonation of CA



AMI.16: Compromised Headend Allows Impersonation of CA

Potential Mitigations

1 – *Require approved key management* including secure generation, distribution, storage, and update of cryptographic keys

2 – See common sub tree *Threat Agent Gains Access to* <network>

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

AMI.27: Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control

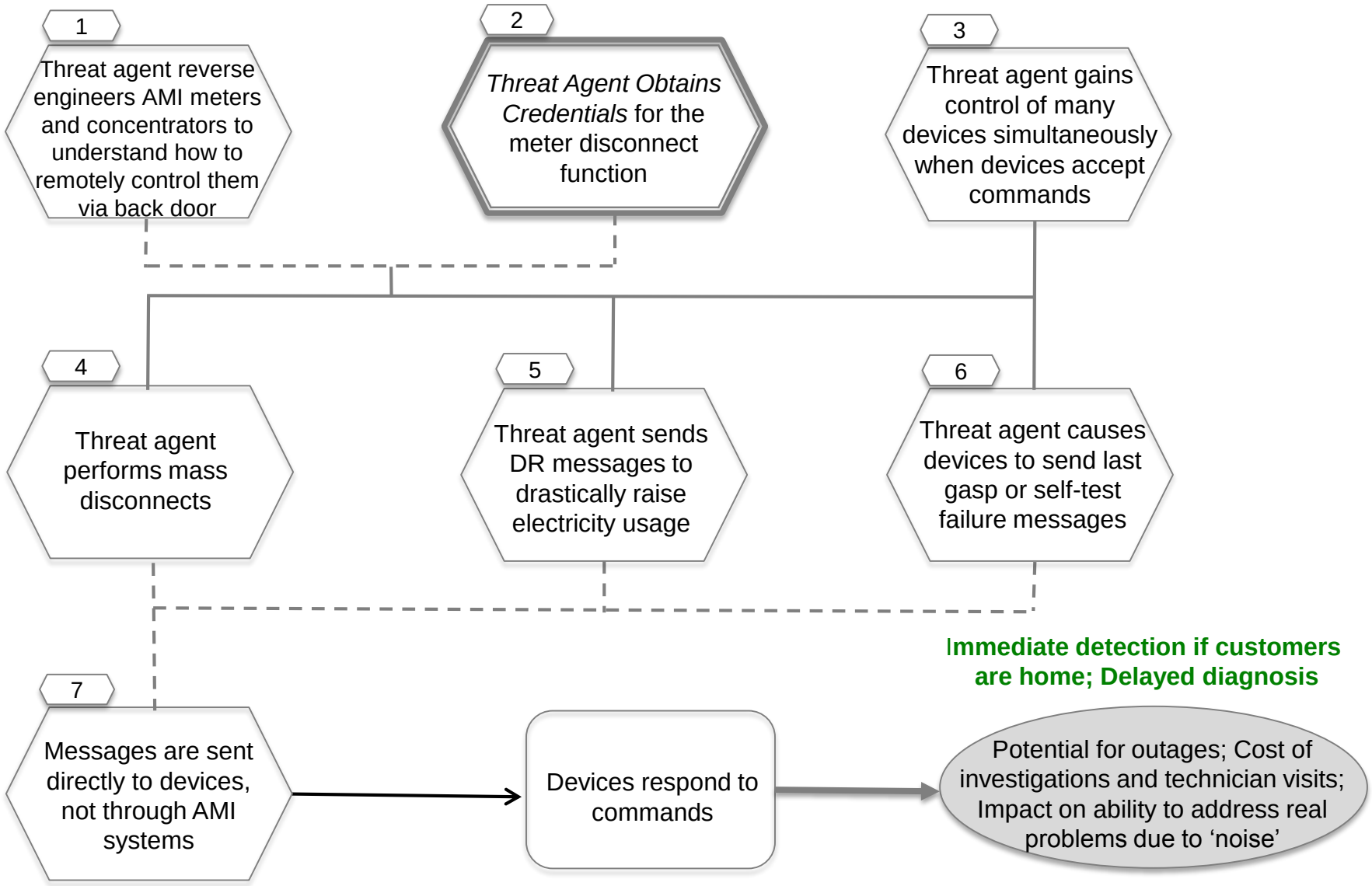
Description

A threat agent is able to reverse engineer AMI equipment (meters and concentrators) to determine how to remotely control them. This allows the threat agent to control many devices simultaneously, and, for example, to perform a simultaneous mass disconnect, send DR messages that cause consumption of electricity to go up dramatically, or cause devices to send out last gasp or self-test failed messages.

Assumptions

- Devices are not built with adequate security
- Backdoors and unprotected interfaces remain on production equipment

AMI.27: Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control



AMI.27: Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control

Potential Mitigations

1 – *Design for security* to identify and remove unsecure development features and nonstandard" interfaces from production devices

2 – See common tree *Threat Agent Obtains Credentials for* <system or function>

3 - Design for security in equipment such that knowledge alone should not allow a threat agent to access a device without knowledge of keys and other credentials in equipment design

3 - Configure for least functionality by removing unnecessary interfaces and labeling from production devices

AMI.29: Unauthorized Device Accesses HAN and Steals Private Information

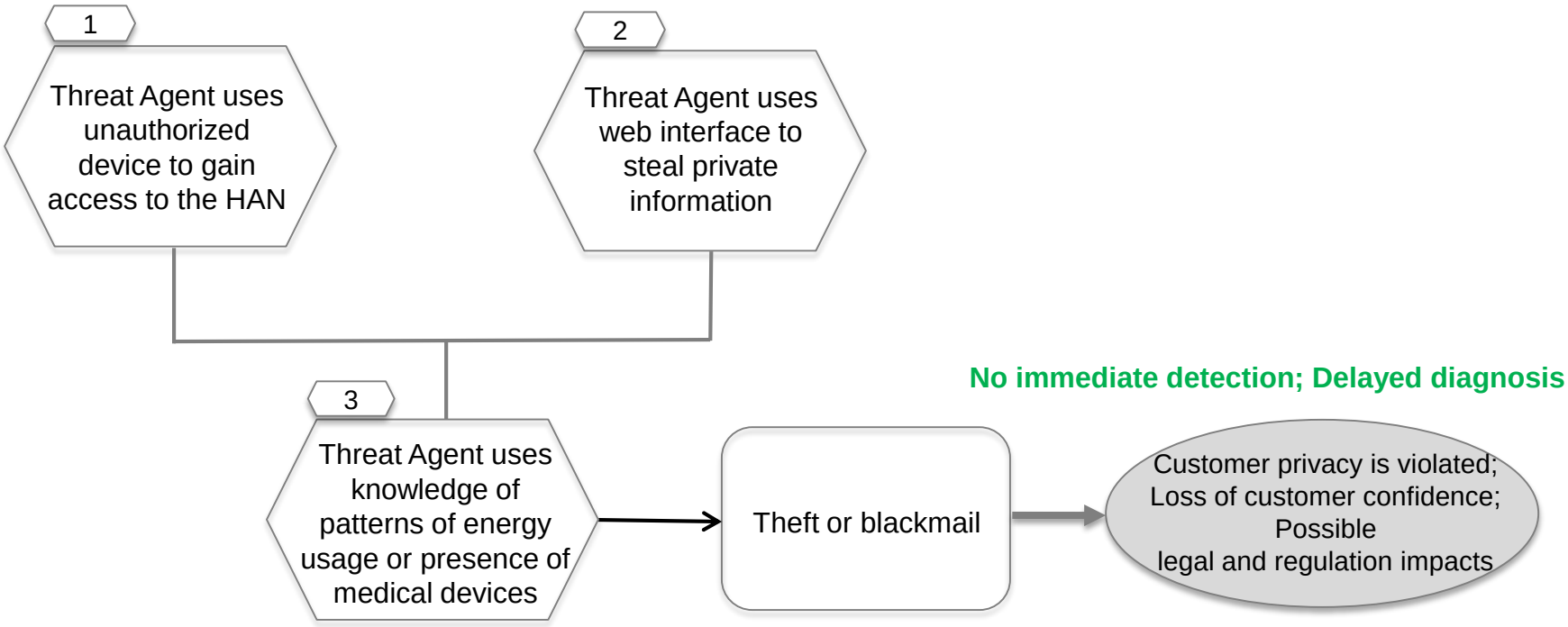
Description

An unauthorized device gains access to the HAN and uses the web interface to obtain private information. Examples of such information are patterns of energy usage and the presence of medical devices.

Assumptions

- Weak or no authentication required for HAN access

AMI.29: Unauthorized Device Acquires HAN Access and Steals Private Information



AMI.29: Unauthorized Device Accesses HAN and Steals Private Information

Potential Mitigations

1 - Restrict network access to the HAN

2 - Minimize private information in HAN systems and devices

AMI.32:Power Stolen by Reconfiguring Meter via Optical Port

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

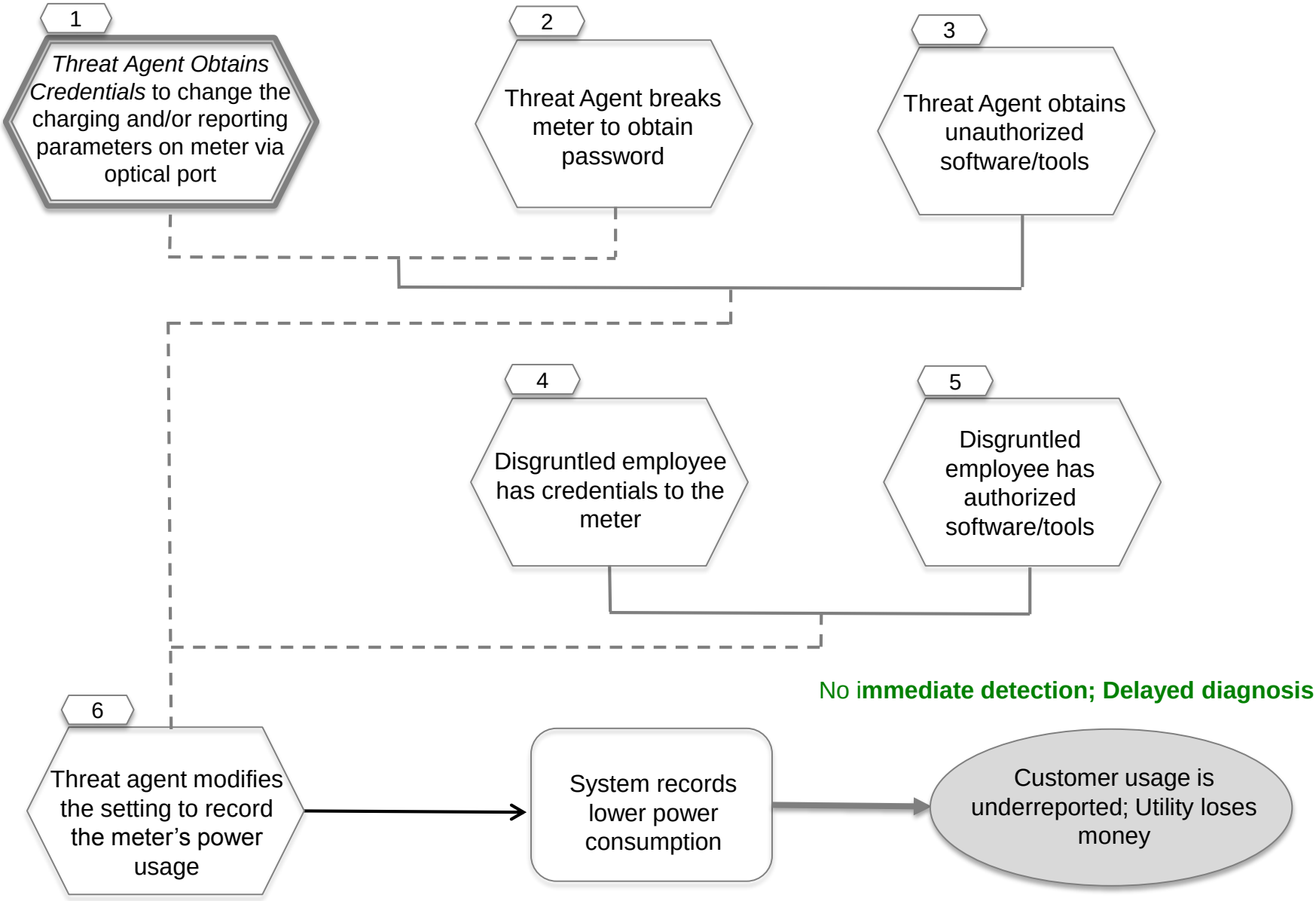
Description

Many smart meters provide the capability of re-calibrating the settings via an optical port, which is then misused by economic thieves who offer to alter the meters for a fee, changing the settings for recording power consumption and often cutting utility bills by 50-75%. This requires collusion between a knowledgeable criminal and an electric customer, and will spread because of the ease of intrusion and the economic benefit to both parties.

Assumptions

- Weak or no authentication required for HAN access
- Meters have an optical port, and a re-configuration function accessible from the optical port
- Both insiders and outsiders have a strong motivation in financial gain
- There is sufficient information and tools available to teach outsiders how to do this attack
- Threat agent has physical access to meter

AMI.32: Power Stolen by Reconfiguring Meter via Optical Port



AMI.32: Power Stolen by Reconfiguring Meter via Optical Port

Potential Mitigations

1 - See common sub tree *Threat Agent Obtains Credentials for* <system or function>

2, 4, 5 - Require multi-factor authentication for firmware updates

6 - Detect unusual patterns of energy usage on smart meters (all utilities have some type of revenue protection scheme, but these may not be sufficient)

6 - Check software file integrity (digital signatures) on code files to validate firmware updates before installation

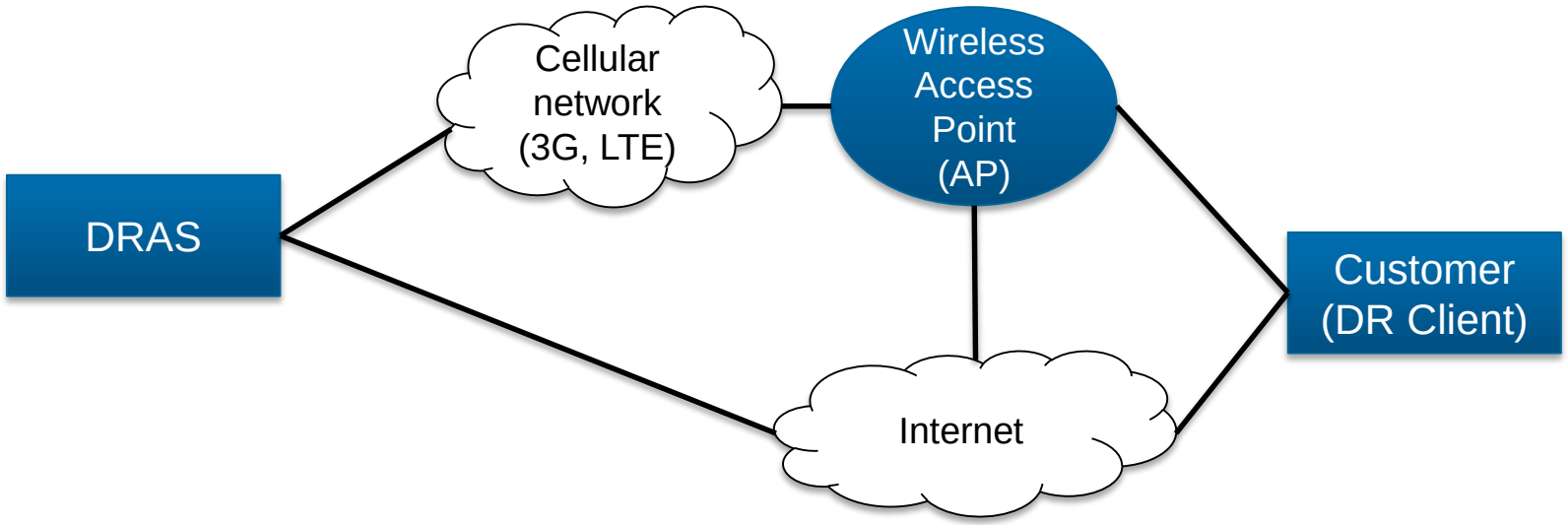
DR.1 Blocked DR Messages Result in Increased Prices or Outages

Description

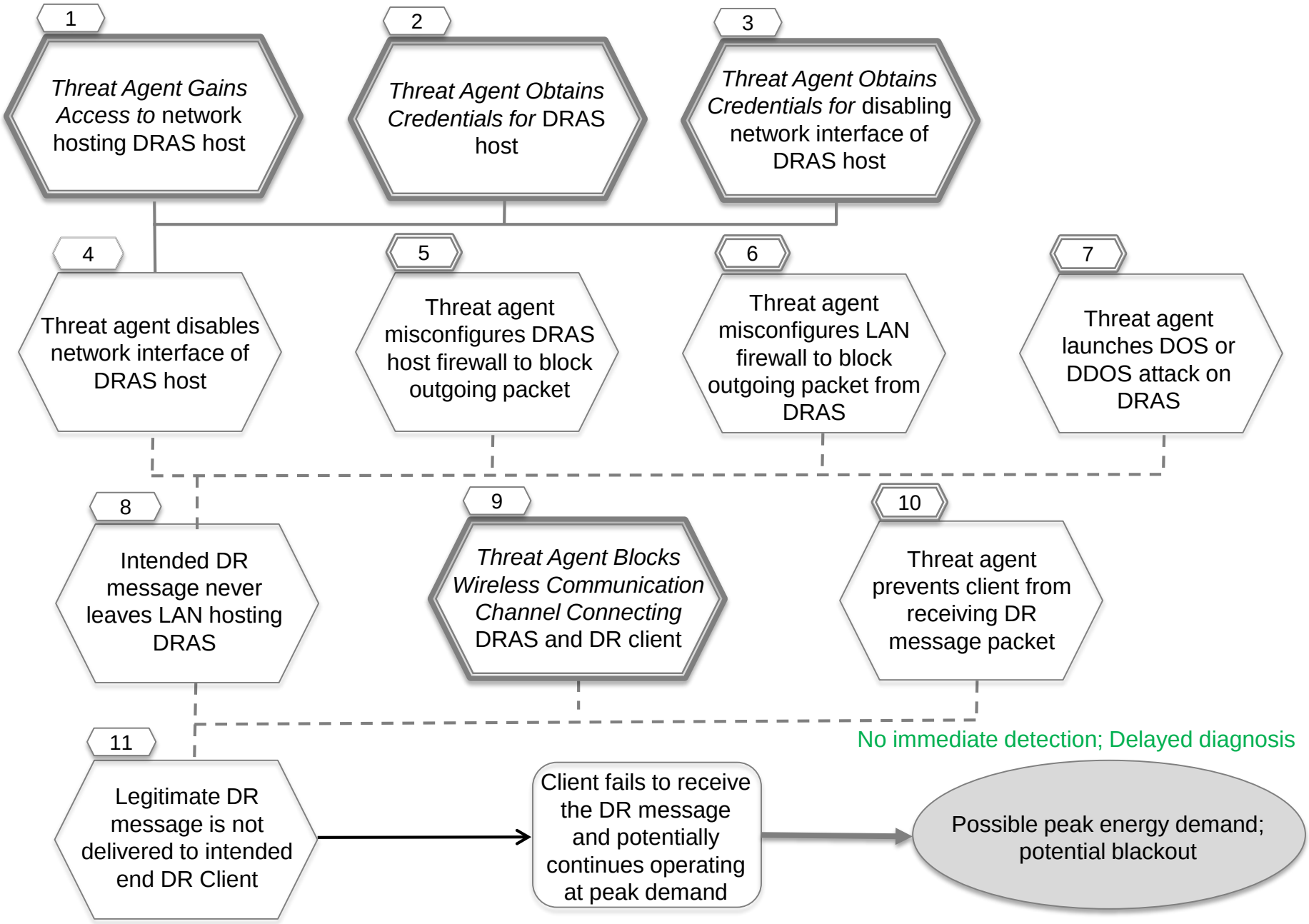
A threat agent blocks communications between a demand response automation server (DRAS) and a customer system (smart meters or customer devices). This could be accomplished by flooding the communications channel with other messages, or by tampering with the communications channel. These actions could prevent legitimate DR messages from being received and transmitted. This can occur at the wired or the wireless portion of the communications channel.

DR.1 Blocked DR Messages Result in Increased Prices or Outages

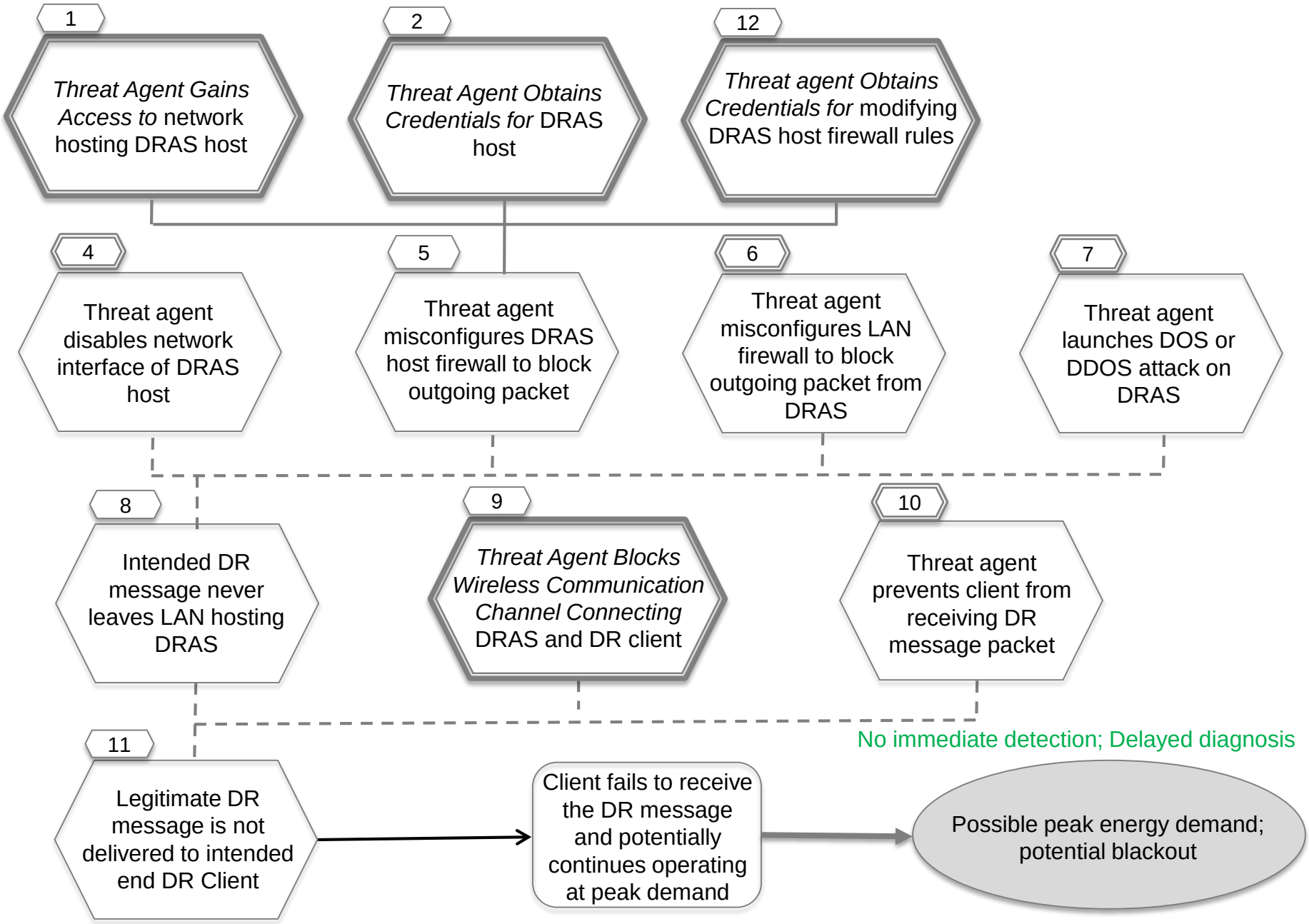
Related Architecture



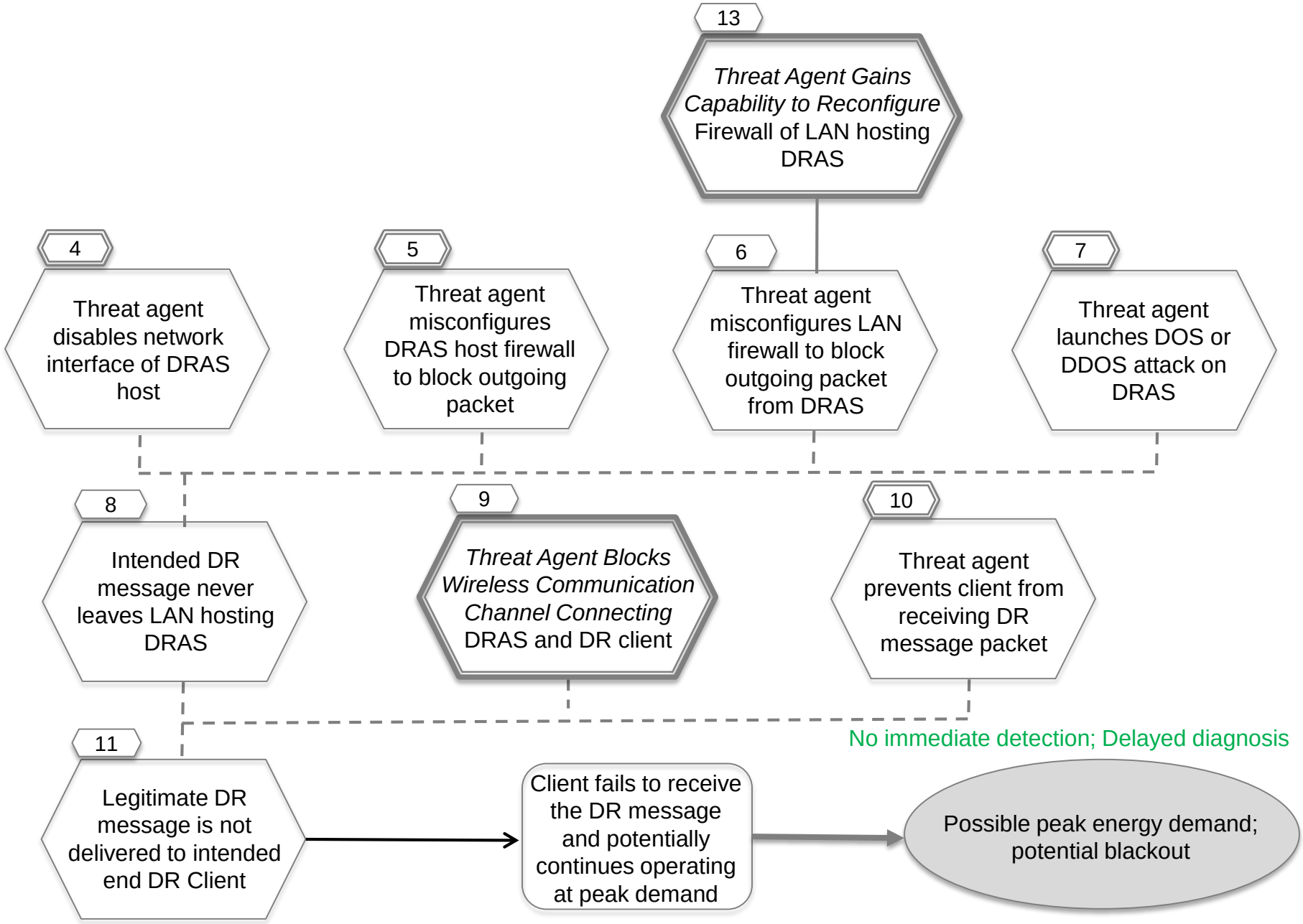
DR.1 Blocked DR Messages Result in Increased Prices or Outages (1/8)



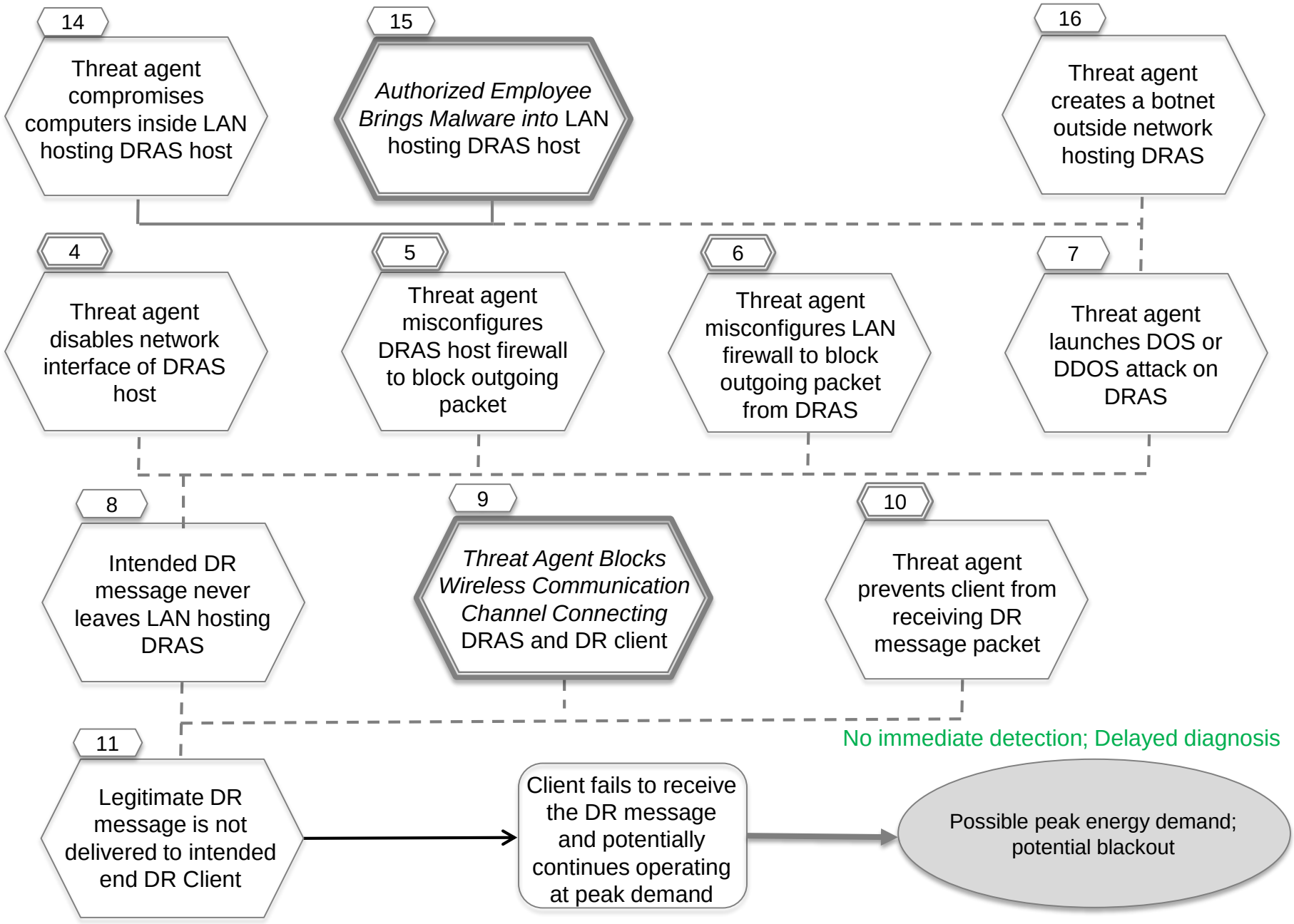
DR.1 Blocked DR Messages Result in Increased Prices or Outages (2/8)



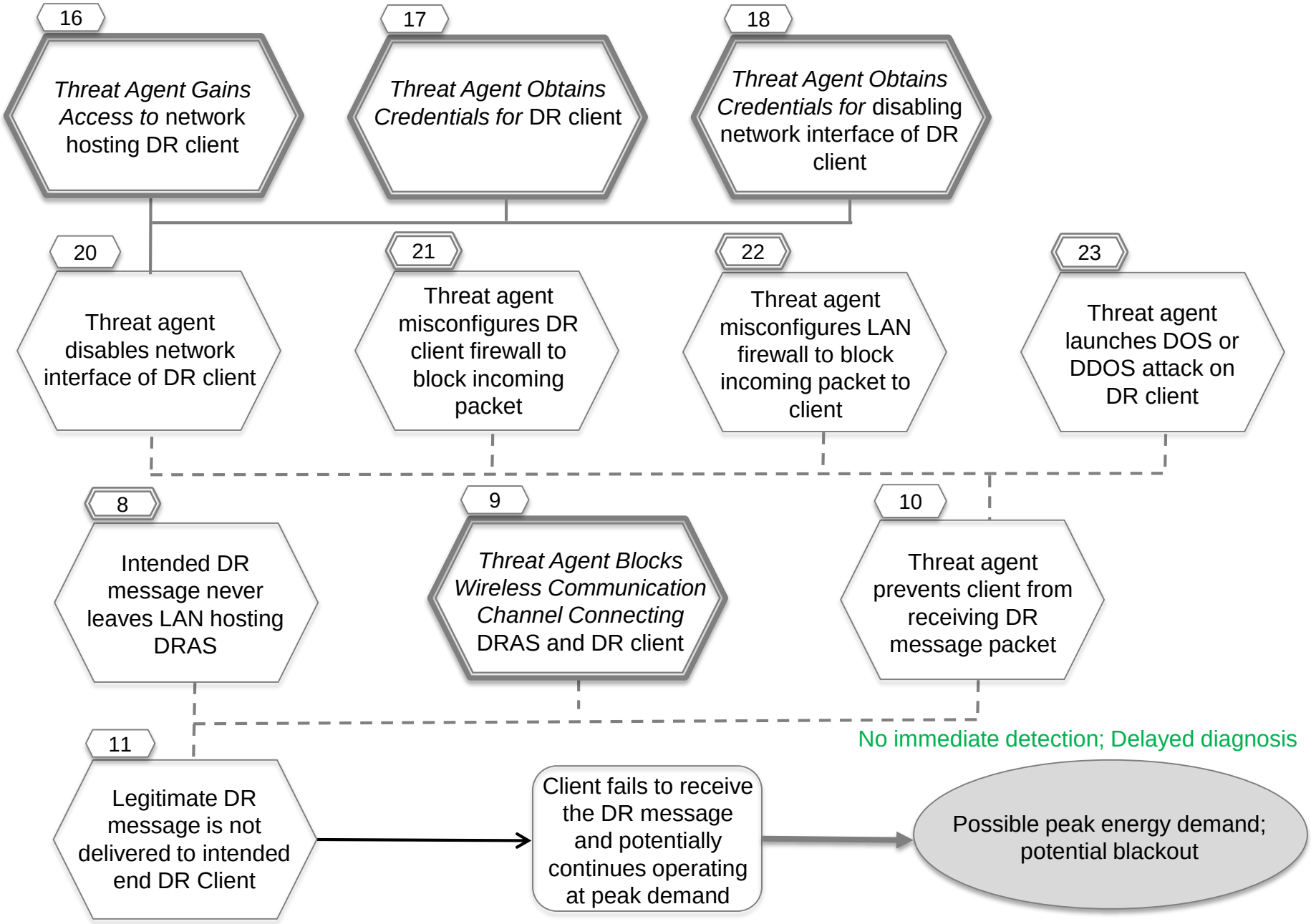
DR.1 Blocked DR Messages Result in Increased Prices or Outages (3/8)



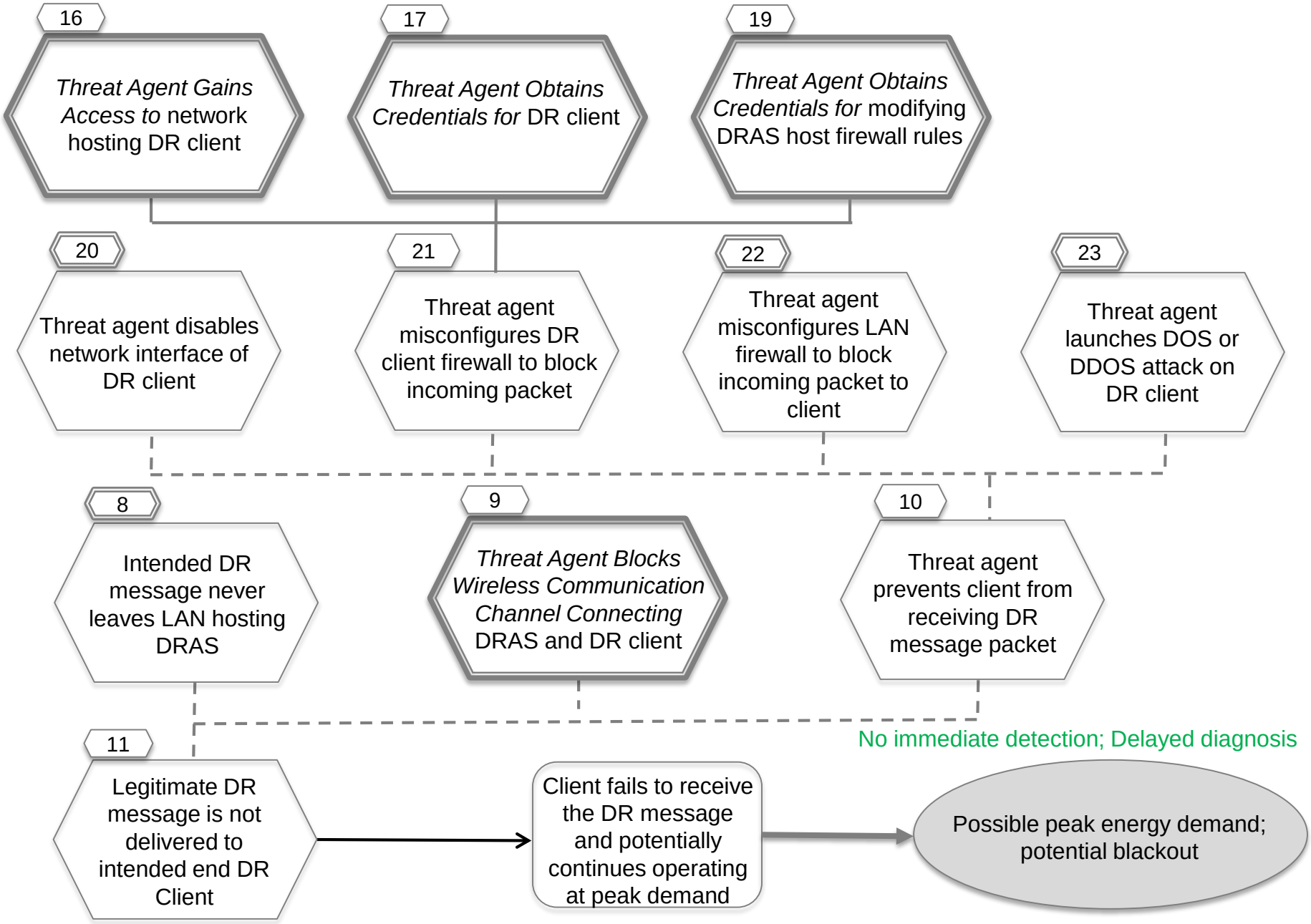
DR.1 Blocked DR Messages Result in Increased Prices or Outages (4/8)



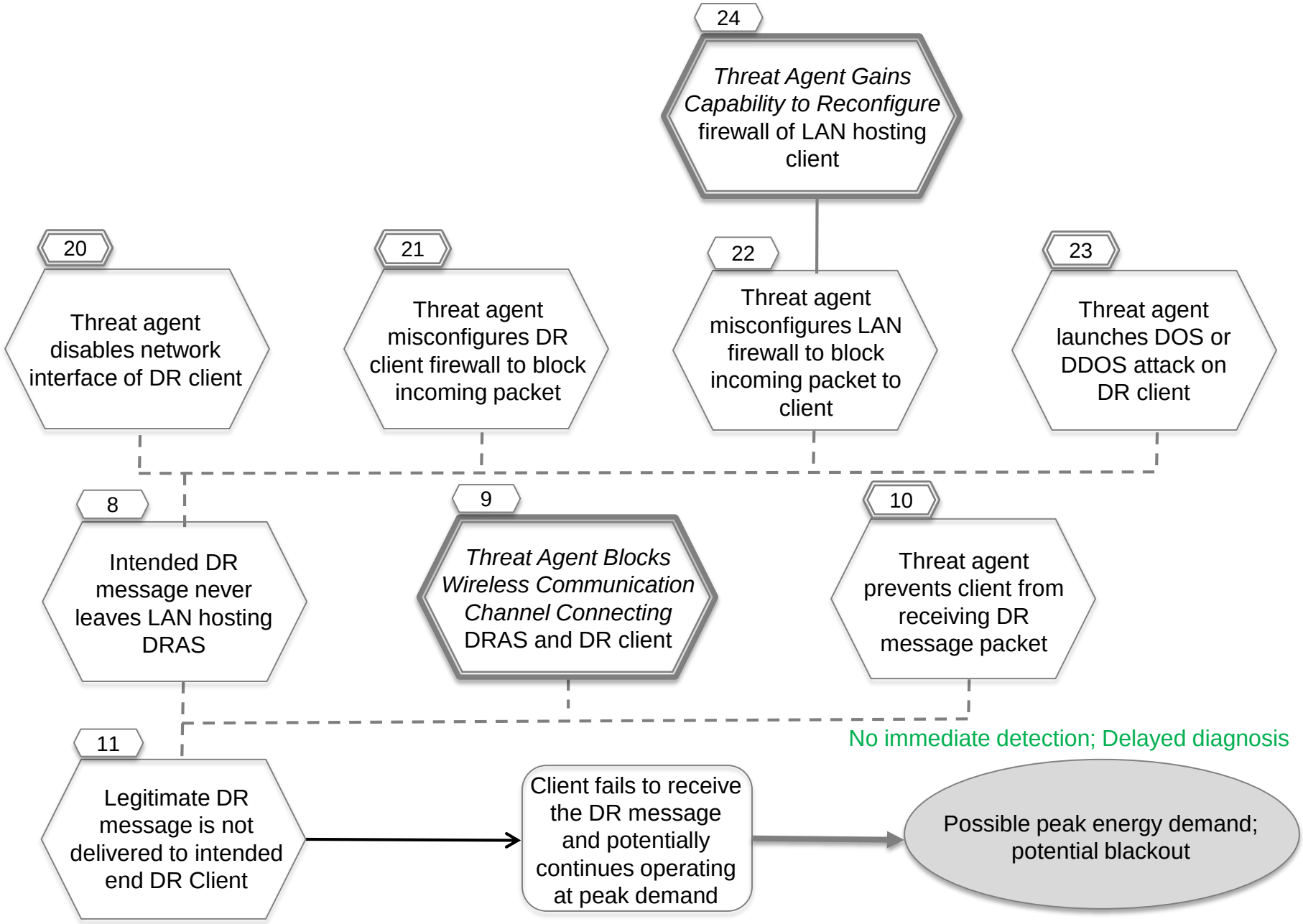
DR.1 Blocked DR Messages Result in Increased Prices or Outages (5/8)



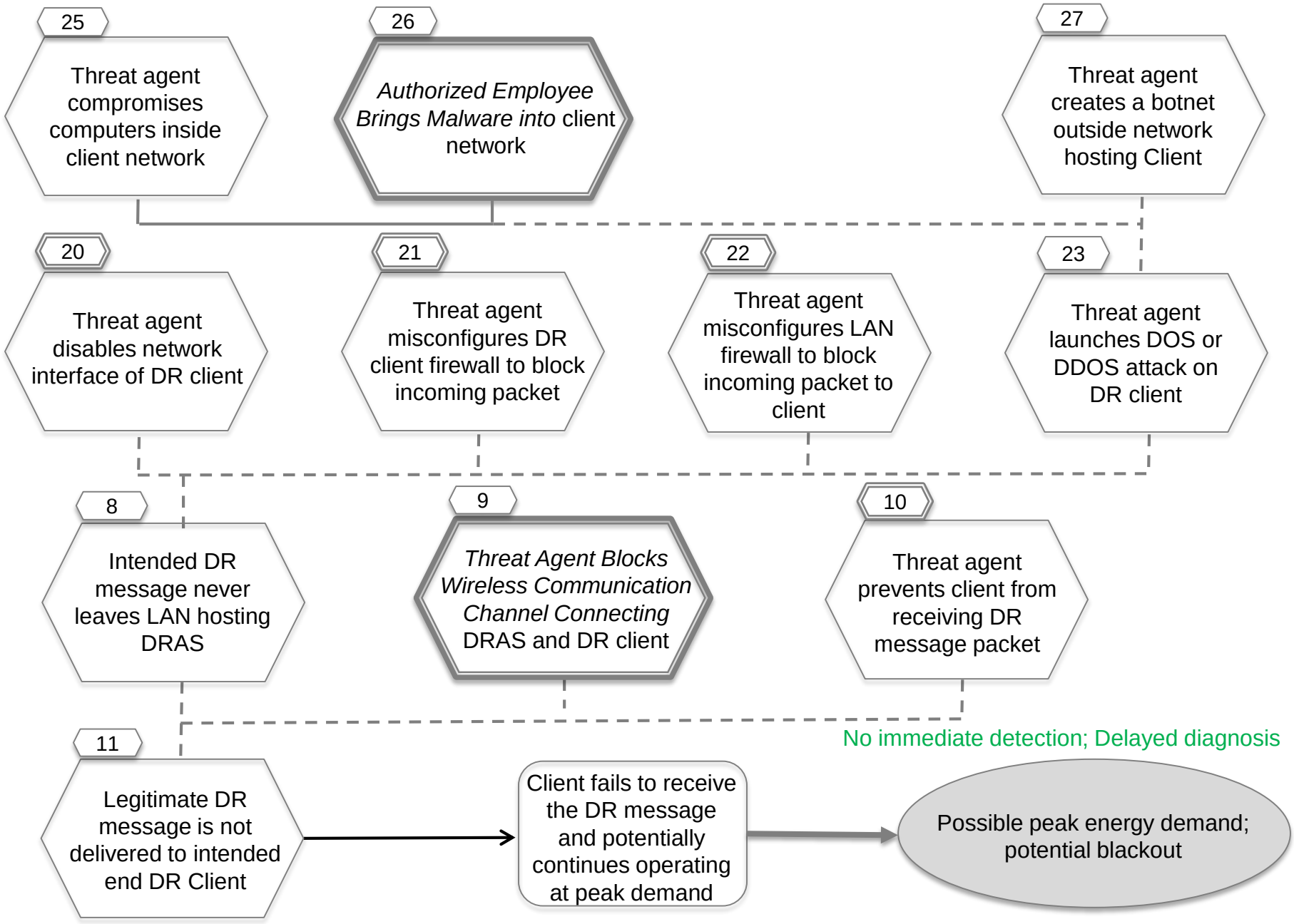
DR.1 Blocked DR Messages Result in Increased Prices or Outages (6/8)



DR.1 Blocked DR Messages Result in Increased Prices or Outages (7/8)



DR.1 Blocked DR Messages Result in Increased Prices or Outages (8/8)



DR.1 Blocked DR Messages Result in Increased Prices or Outages

Potential Mitigations

1 - See common sub tree *Threat Agent Gains Access to* <network>

2, 3 - See common sub tree *Threat Agent Obtains Credentials for* <system or function>

4 - *Generate alerts* on changes to device configurations on DRAS host; *Require acknowledgement* of link status to ensure network connectivity; *Detect unauthorized configuration changes*

6 - *Generate alerts* on changes to rules on LAN firewall; *Detect unauthorized changes; Create audit log* of packet filtering rule changes

7 - *Require intrusion detection and prevention*; *Detect unusual patterns* of network traffic; *Enforce restrictive firewall rules* for DRAS LAN access

9 - See common sub tree *Threat Agent Blocks Wireless Communication Channel Connecting* <x and y>

12 - See common sub tree *Threat Agent Obtains Credentials for* <system or function>

DR.1 Blocked DR Messages Result in Increased Prices or Outages

Potential Mitigations (2)

13 - See common sub tree *Threat Agent Gains Capability to Reconfigure <firewall >*

14 - *Maintain patches* in all computers; *Maintain anti-virus; Test for malware*; *Restrict remote access* to internal computers

15 - See common sub tree *Authorized Employee Brings Malware into* <system or network>

16 - See common sub *tree Threat Agent Gains Access to* <network>

17, 18, 19 - See common sub tree *Threat Agent Obtains Legitimate Credentials for* <system or function>

20 – *Generate alerts* on changes to device configurations on DR client; *Require acknowledgement* of link status to ensure network connectivity; *Detect unauthorized configuration changes*

21 – *Generate alerts* on changes to configurations on DR client; *Require acknowledgement* of link status to ensure network connectivity; *Detect unauthorized configuration changes*

DR.1 Blocked DR Messages Result in Increased Prices or Outages

Potential Mitigations (3)

22 – *Generate alerts* on changes to rules on LAN firewall; *Detect unauthorized configuration changes; Create audit log* of packet filtering rule changes

23 – *Require intrusion detection and prevention*; *Detect unusual patterns* of network traffic; *Enforce restrictive firewall rules* for Client LAN access

24 – See common sub tree *Threat Agent Gains Capability to Reconfigure* <firewall >

25 – *Maintain patches* in all computers; *Maintain anti-virus*; *Test for malware*; *Restrict remote access* to internal computers

26 – See common sub tree *Authorized Employee Brings Malware into* <system or network>

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages

Description

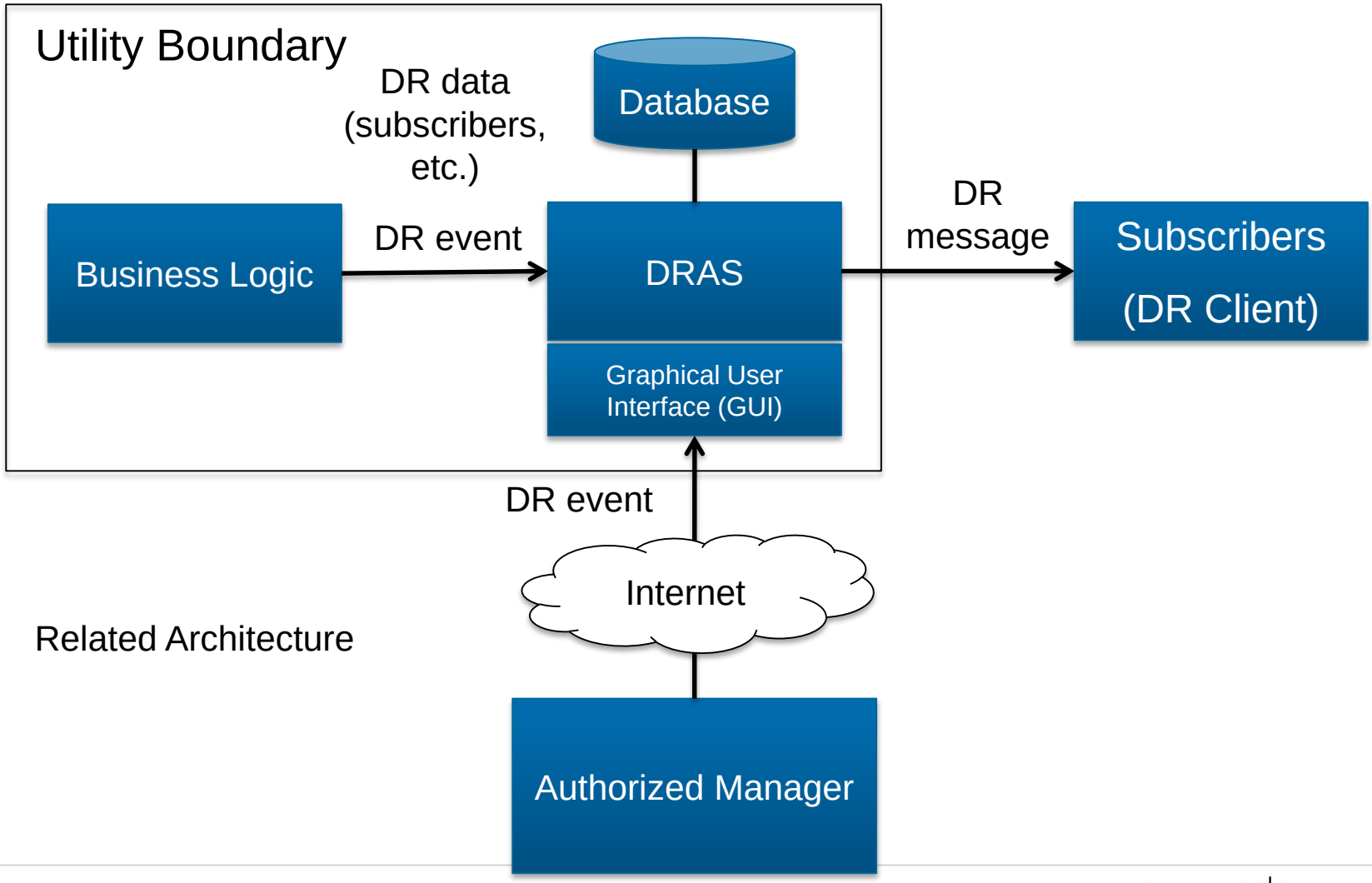
A threat agent unintentionally or maliciously modifies the DRAS configuration to send (or not send) DR messages at incorrect times and to incorrect devices. This could deliver a wrong, but seemingly legitimate set of messages to the customer system.

Assumptions

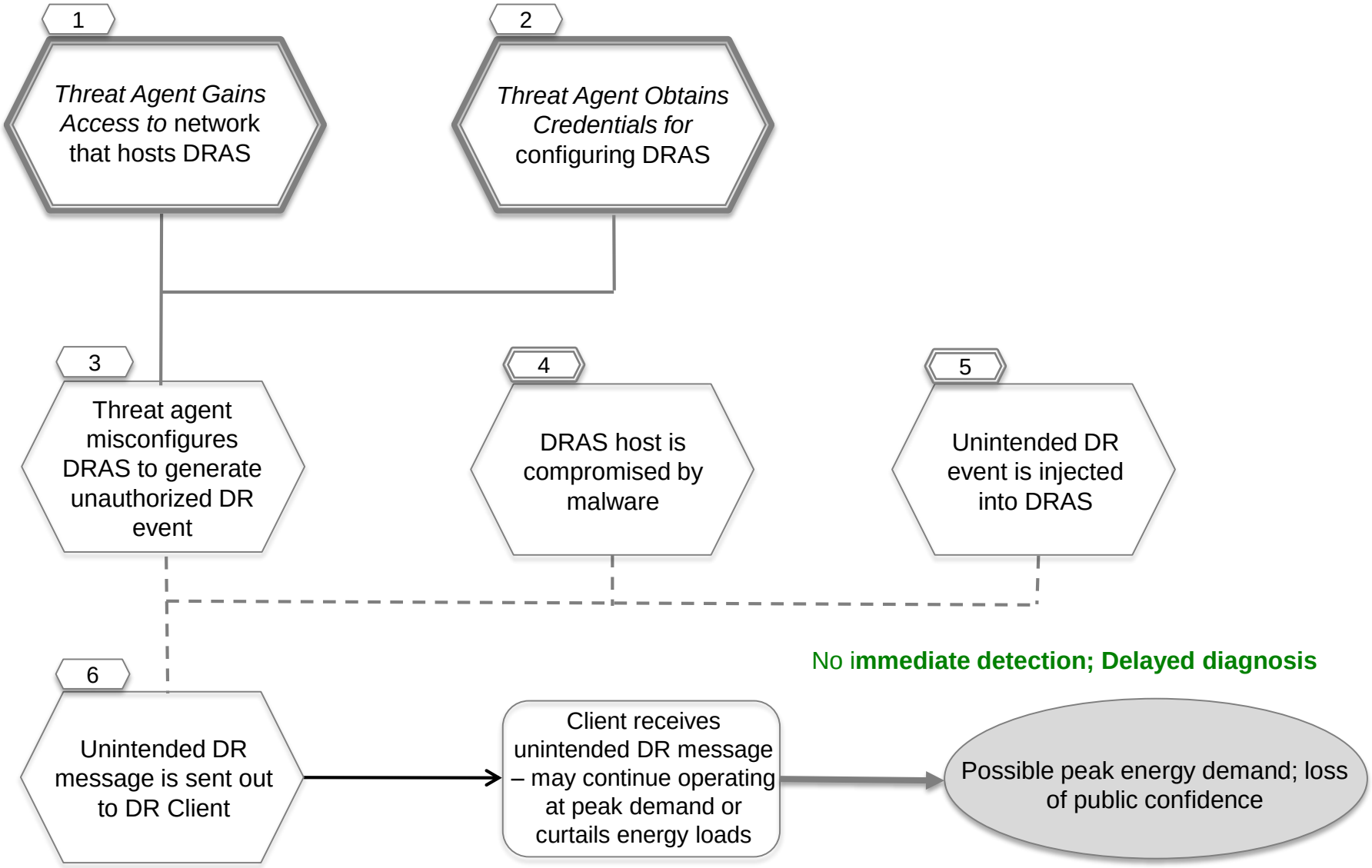
- DRAS issues a DR message when receiving DR event information in the following ways:
  (1) Business Logic feeds DR event to DRAS automatically based on its analysis;
  (2) Authorized manager manually generates and feeds DR event to DRAS through management GUI.

DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages

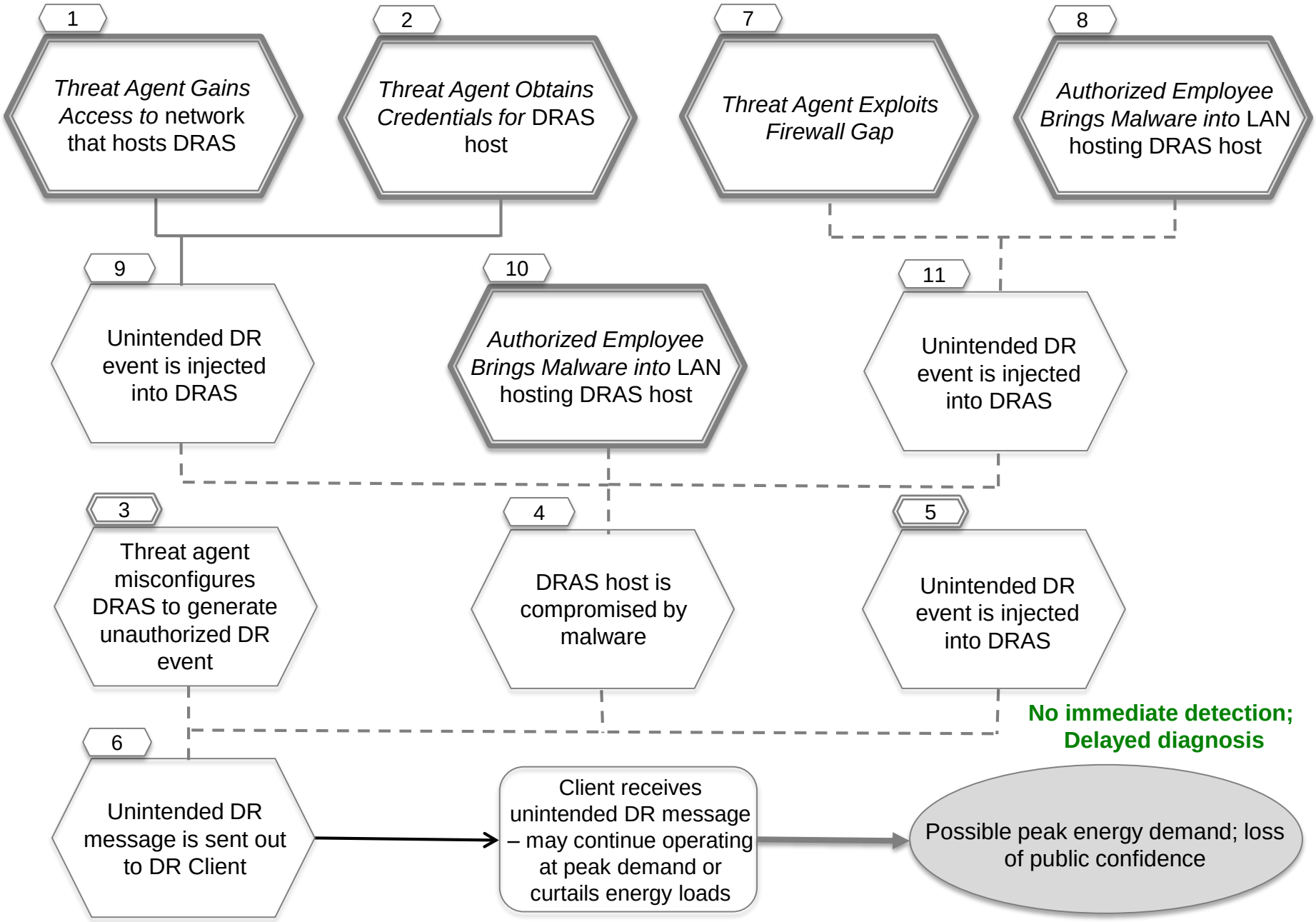
Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership



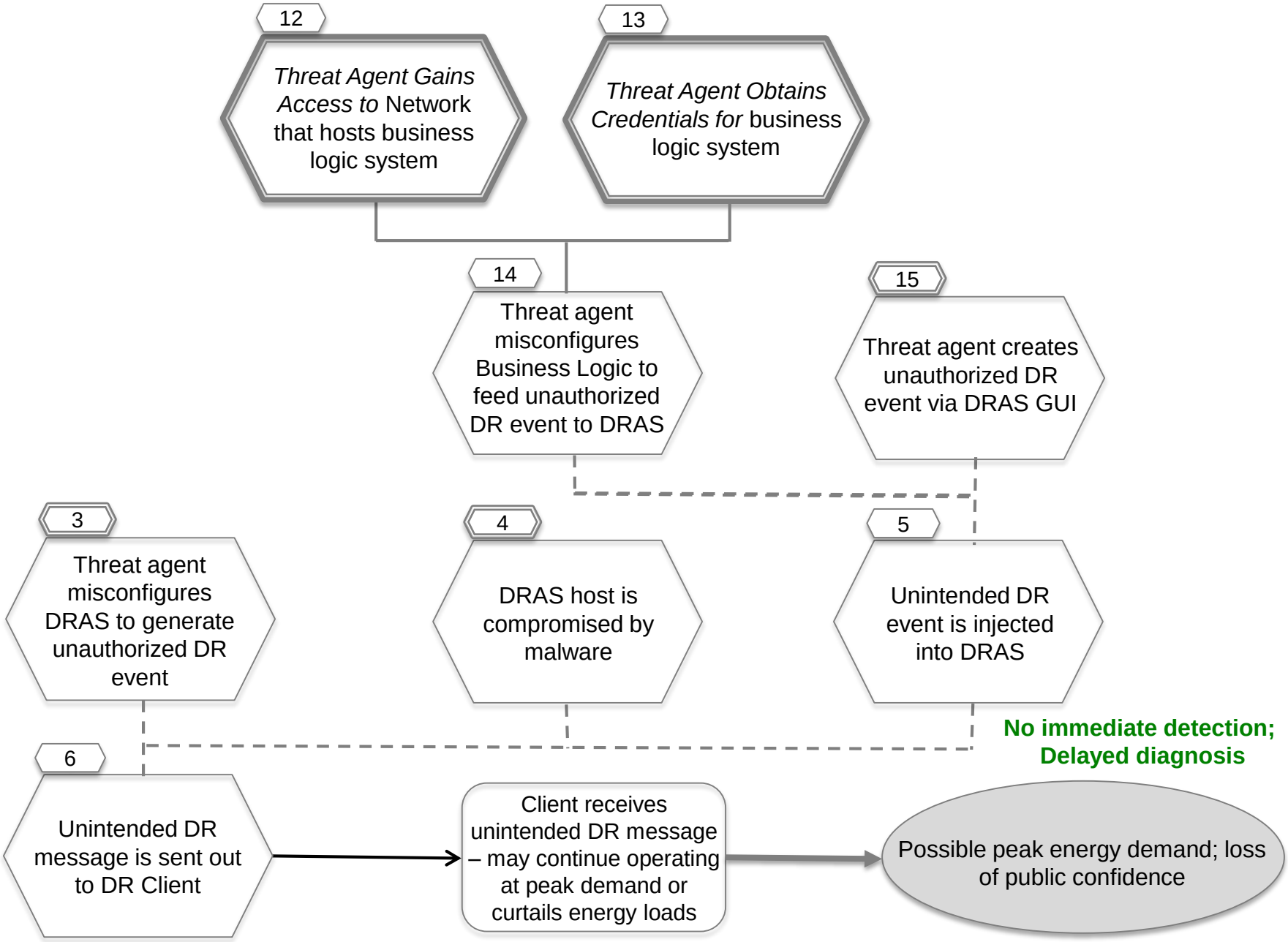
DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages (1/4)



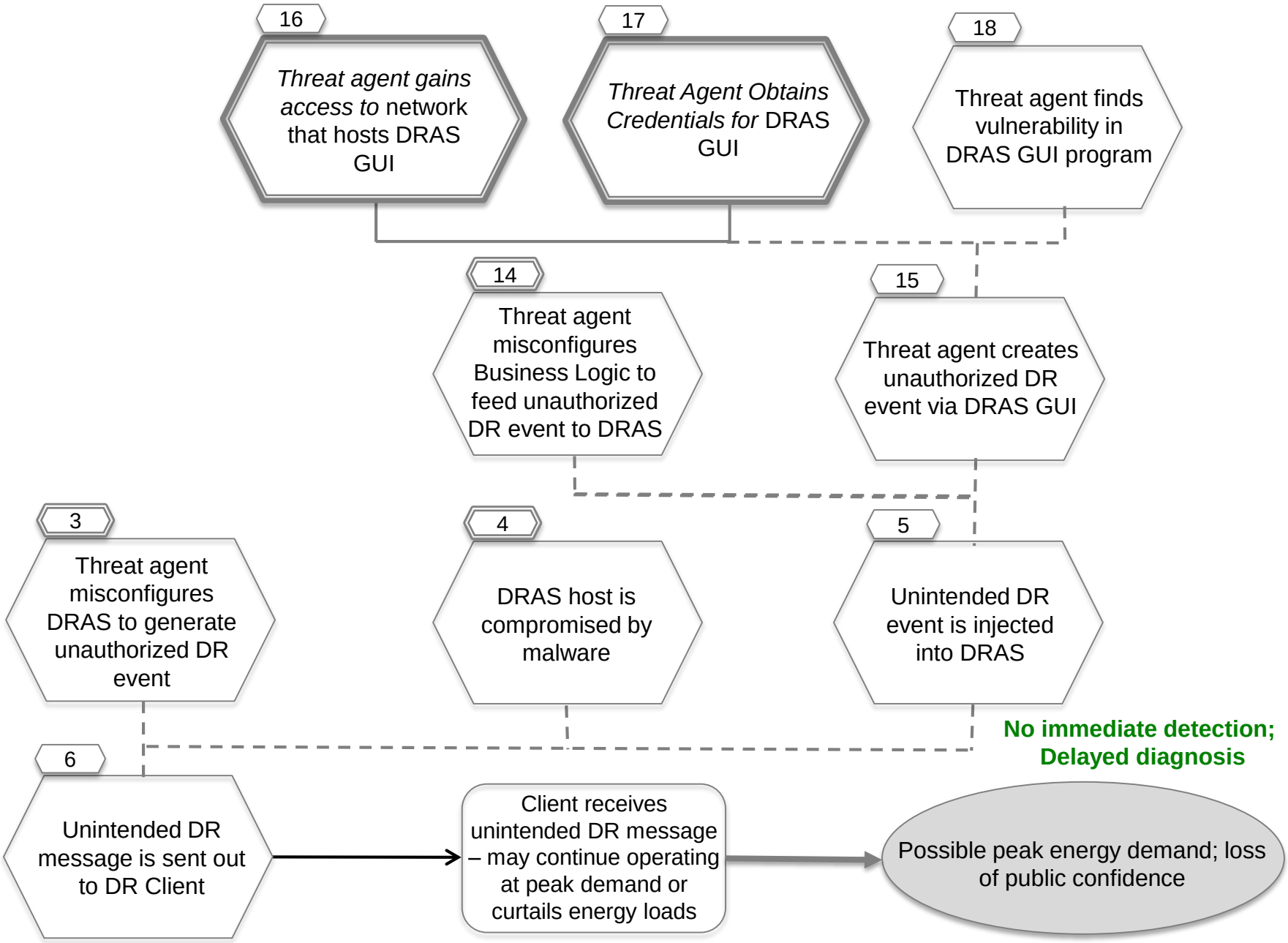
DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages (2/4)



DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages (3/4)



DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages (4/4)



DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Potential Mitigations

1 - See common sub tree *Threat Agent Gains Access to* <specific network>
2 - See common sub tree *Threat Agent Obtains Credentials for* <system or function>
3 - *Generate alerts* on changes to configurations on DRAS; *Detect unauthorized configuration changes*; *Create audit log* of DR messages generated; *Require second-level authentication* to change configuration
5, 6 - *Validate inputs*, specifically the reasonableness of DR event
7 - See common sub tree *Threat Agent Exploits Firewall Gap in* <specific firewall>
8 - See common sub tree *Authorized Employee Brings Malware into* <system or network>
9, 11 - *Require application whitelisting*
11 - *Conduct penetration testing*; *Perform security testing*; *Maintain patches* in DRAS host; *Maintain anti-virus*

DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Potential Mitigations (2)

13 - See common sub tree *Threat Agent Obtains Credentials for* <system or functions>

14 - *Use RBAC* to limit generation of DR event; *Generate alerts* on changes to configurations on Business Logic; *Detect unauthorized configuration changes*; *Create audit log* of DR events generated

15 - *Create audit log* of DR events generated; *Generate alarm* on unexpected DR event generation

18 - *Maintain patches* in DRAS GUI host; *Maintain anti-virus*; *Detect unauthorized connections* to DRAS GUI; *Restrict Internet access* to DRAS GUI

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System

Description

A threat agent gains access to selected elements of the utility DMS system - which includes all distribution automation systems and equipment in control rooms, substations, and on pole tops - via remote connections. After gaining the required access, the threat agent manufactures an artificial cascade through sequential tripping of select critical feeders and components, causing automated tripping of generation sources due to power and voltage fluctuations.

Assumptions

- Remote connections for vendor access are tightly controlled and physically disconnected when not in use, but inadvertent connections sometimes occur
- DMS/SCADA network segregated from corporate, public networks, no air gap
- Data logging is performed on DMS system, recording logins, breaker trips, capacitor bank switching, configuration changes, etc.

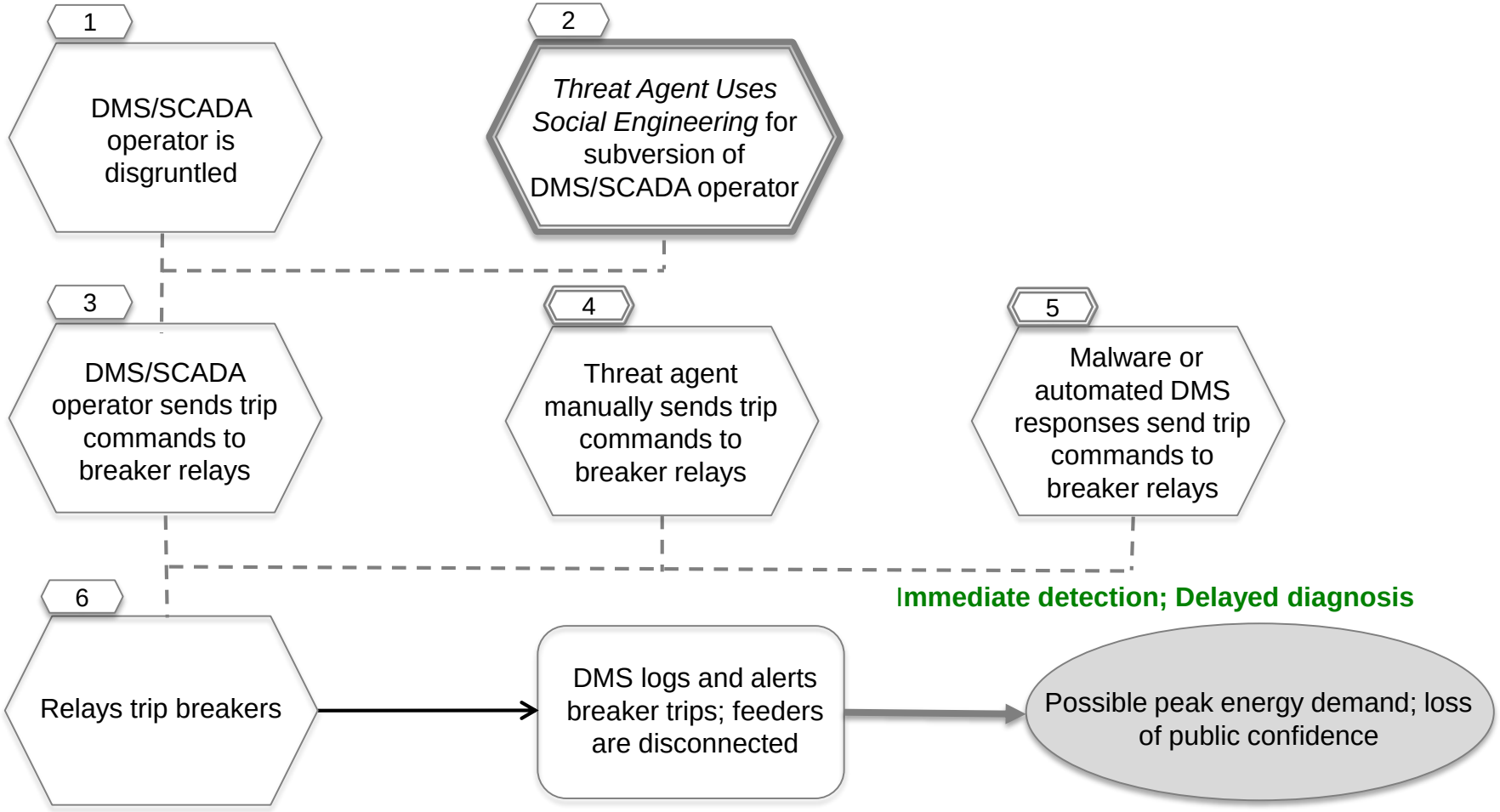
DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

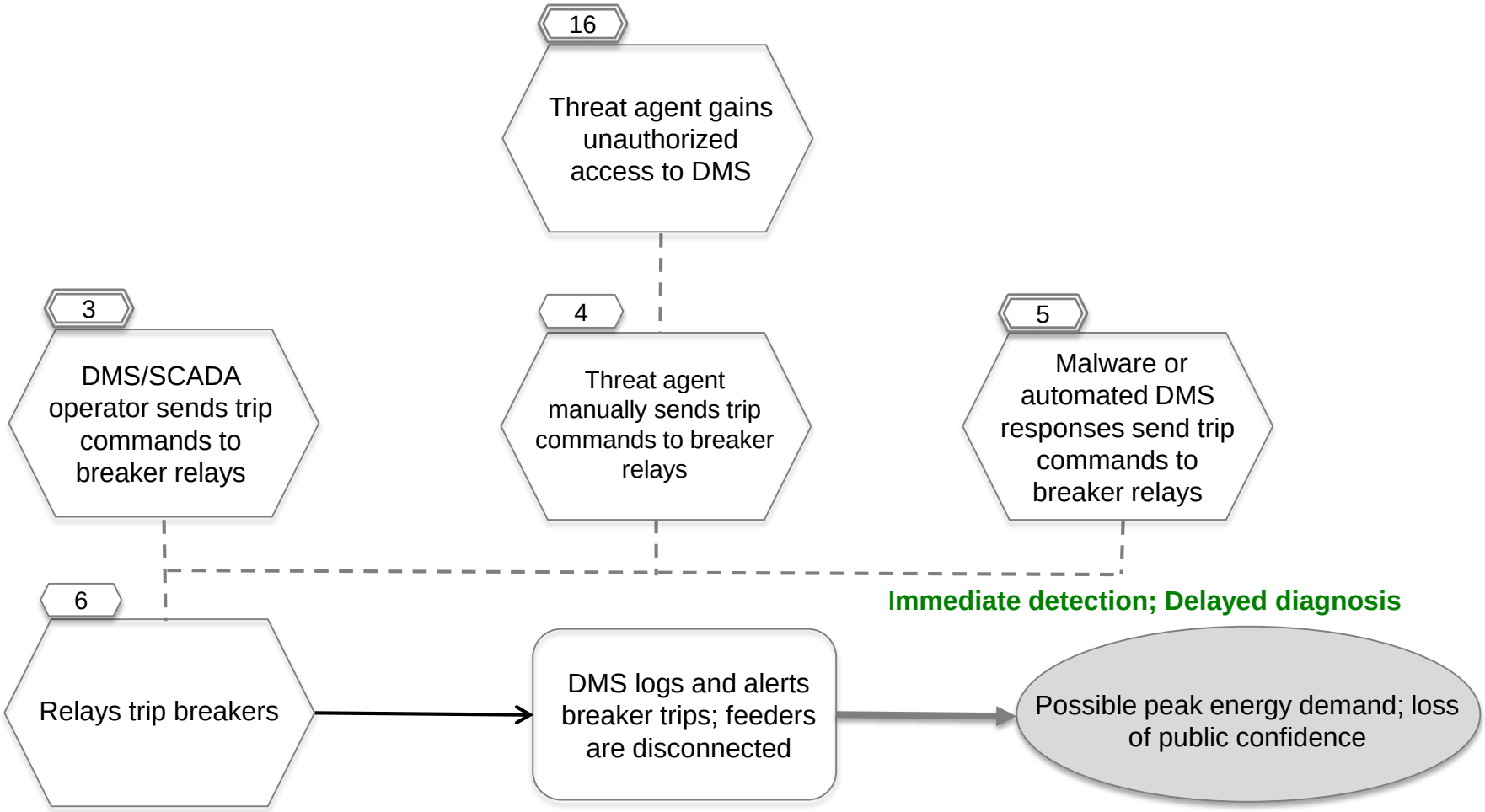
Assumptions (2)

- Some DMS communications are run over leased fiber lines where some communication's equipment is shared with other entities
- Intrusion detection systems are not present on DMS network
- Electrical infrastructure information resides on corporate networks as well as the control network
- Distribution communications do not employ encryption and defense in depth
- Moderate complexity password authentication, no two-factor authentication
- DMS/SCADA system is monitored 24/7 by dedicated control personnel
- Some utility linemen and communication personnel carry laptops that permit connections to DMS/SCADA field equipment, communication devices, and the DMS system over the control system network
- Control system network is flat
- Distribution system is largely radial with tie lines at the end of some laterals

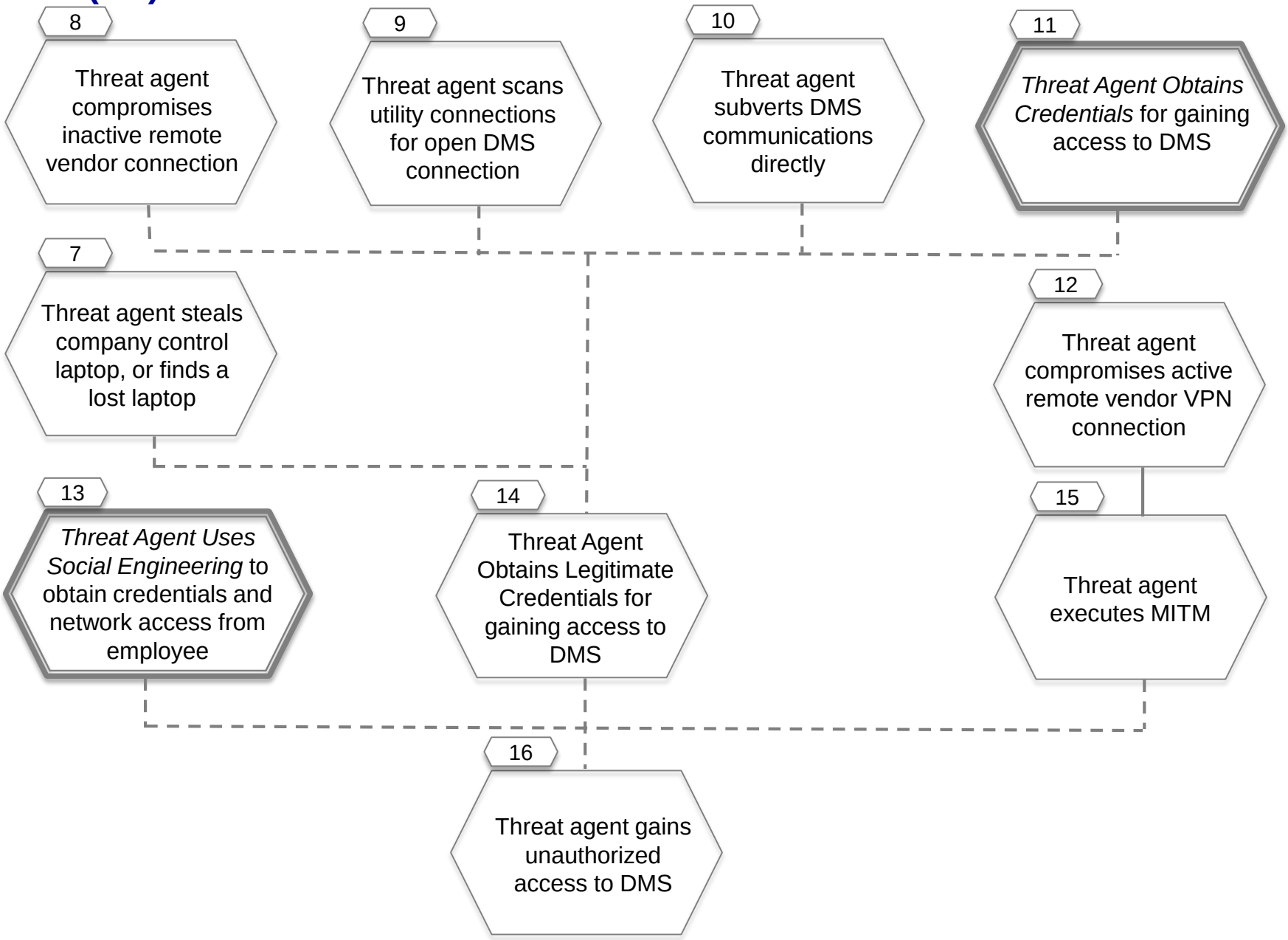
DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System (1/4)



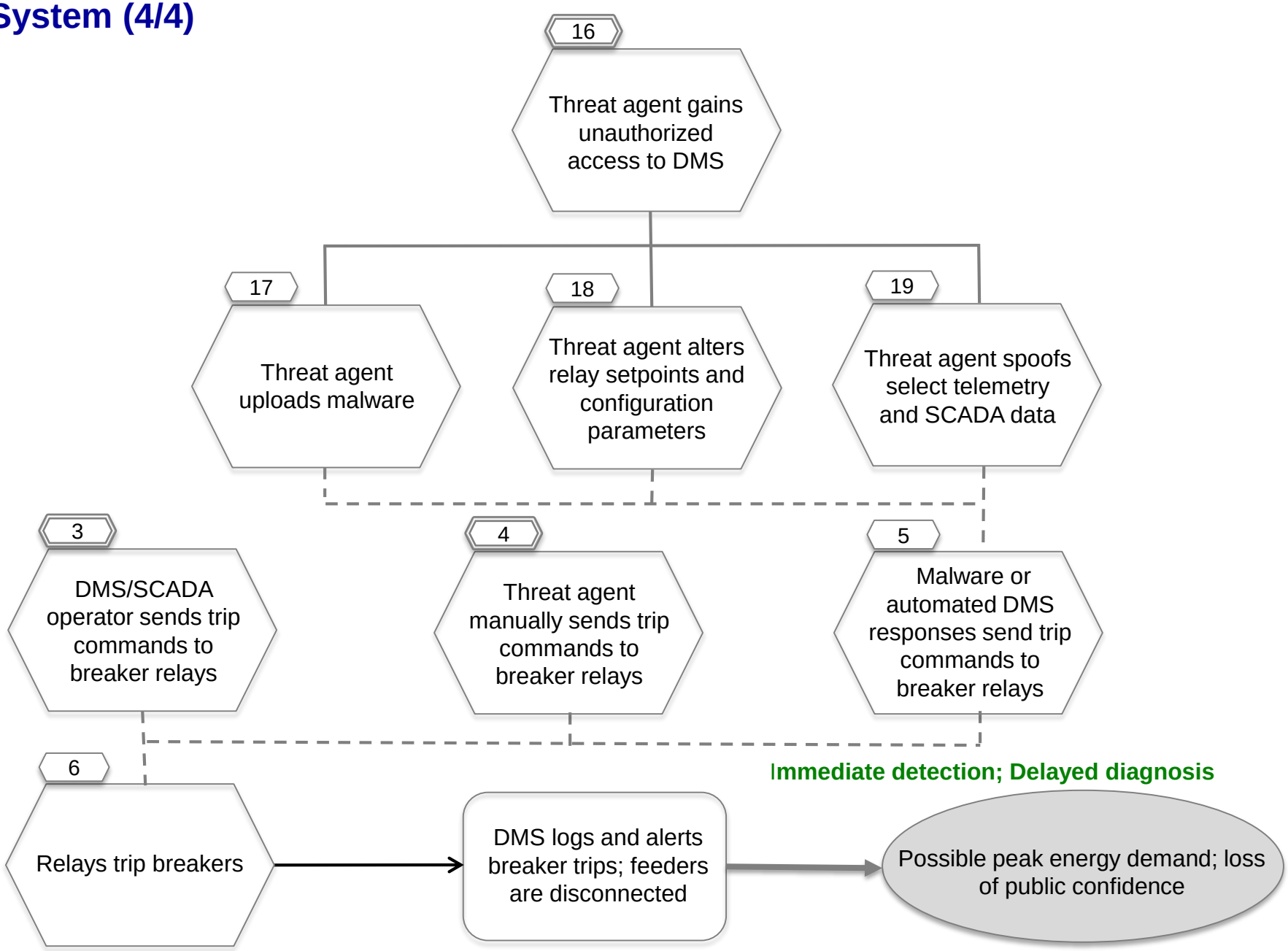
DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System (2/4)



DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System (3/4)



DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System (4/4)



DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System

Potential Mitigations

1 - *Verify personnel* by performing thorough background checks

2 - See common sub tree *Threat Agent Uses Social Engineering to* <desired outcome>

7 - Training on security for portable devices

7, 10 - *Restrict physical access* to DMS equipment

8 - *Restrict remote access* of vendor connections

8, 10, 11, 14 - *Encrypt* all DMS/SCADA communications

9, 10 - *Minimize functions* on control system equipment by disabling all unused ports

11 - See common sub tree *Threat Agent Obtains Credentials for* <system or function>

14 - *Require strong passwords* or *two-factor authentication*

16 - *Require intrusion detection* on DMS networks/hosts

DGM.11 Threat Agent Triggers Blackout via Remote Access to Distribution System

Potential Mitigations (2)

16 - *Restrict remote access* (vendors) by installing patches and updates via physical media mailed by vendor instead of allowing remote vendor access

16, 19 - *Encrypt* and authenticate all DMS/SCADA communications

17 - *Check integrity* of firmware, applications, patches, and updates

18 - *Authenticate users* of relays using strong passwords that are different for each relay

19 - *Restrict physical access* to telemetry and communication equipment

GEN.1 Threat Agent Adds Spurious Trip Parameters on Remotely Located Plant Support and Trips Unit Offline

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Description

A threat agent gains physical access to a river water pump house, connects a laptop to the local controls network, and adds a time-delay trip to the circulating water pumps triggered off of a normal value. This causes loss of cooling water flow resulting in the loss of condenser vacuum tripping the turbine and causing the plant to be tripped offline.

Assumptions

- The pump house equipment utilizes a local networked, microprocessor-based relay control system to control pump house equipment – including trips.
- The threat actor has knowledge of power plant operations and knowledge of the access parameters.
- The time-delay is triggered off of an intake level transmitter value within normal limits that adds a random factor to the trip frequency.

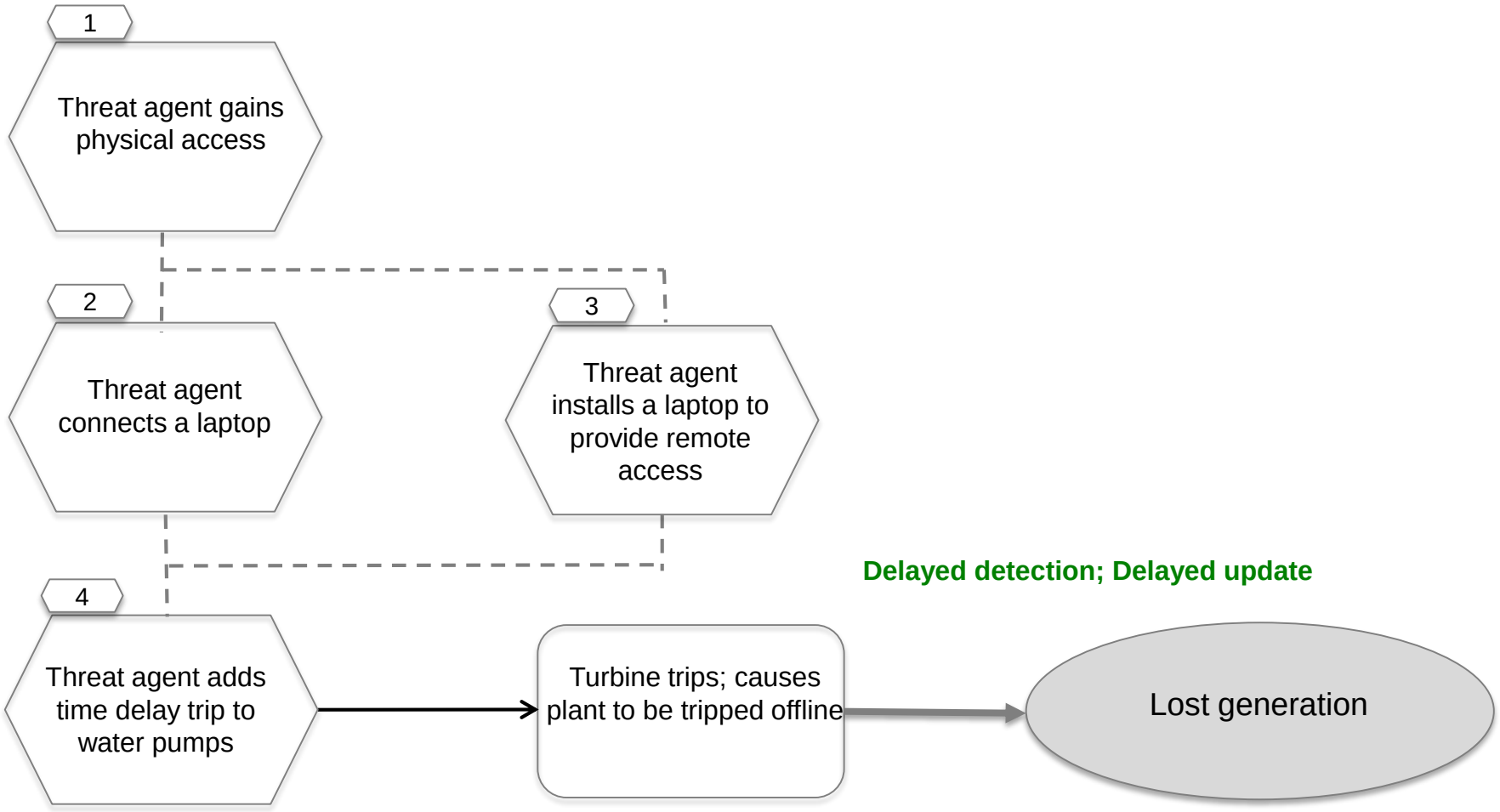
GEN.1 Threat Agent Adds Spurious Trip Parameters on Remotely Located Plant Support and Trips Unit Offline

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Assumptions (2)

- The main control room system access to the pump house is limited by design to only allow start and stop commands to equipment and to receive generic trouble alarms (e.g., motor trouble, high or low water levels, high differential pressure).
- The pump house is located outside of the inner security perimeter of the plant and it not actively guarded.
- Surveillance is limited to periodic spot checks once-per-shift to check for leaks and obvious mechanical issues.
- Pumps are single speed pumps in standard configuration.
- Equipment controls use no passwords or default passwords.
- A backup copy of the pump house controls logic has been kept off-site, but it may not include all the tuning and setpoint adjustments.

GEN.1 Threat Agent Adds Spurious Trip Parameters on Remotely Located Plant Support and Trips Unit Offline



GEN.1 Threat Agent Adds Spurious Trip Parameters on Remotely Located Plant Support and Trips Unit Offline

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Potential Mitigations

1 - Restrict physical access to pump house using, for example, card swipes, pin codes, etc.

1 - Require video surveillance of the human interfaces to the pump house equipment

1 - Require periodic physical surveillance of intake structures and equipment (new common mitigation)

1 - Restrict physical access by implementing personnel security control procedures

2, 3 - Authenticate users so that physical access to the system(s) does not automatically grant logical access

2 - Restrict configuration access to limit who has access and can make configuration changes

GEN.1 Threat Agent Adds Spurious Trip Parameters on Remotely Located Plant Support and Trips Unit Offline

Potential Mitigations (2)

4 - Define procedures to evaluate the credibility of high intake level readings from a pump house. For a spurious reading, other plant indications related to open loop cooling system would not be consistent

2, 3 - Authenticate users for all user interface interactions

4 - Generate alarms on remote equipment when there is evidence of tampering of controls and instrumentation

GEN.15 Plant Tripped Off-Line Through Access Gained Through a Compromised Vendor Remote Connection

Description

The threat agent, a disgruntled or compromised vendor employee, uses the authorization credentials and verification procedure to a secure remote maintenance solution. The remote access solution involves a vendor-maintained asset on the DCS network that prompts the utility to grant the asset access to the DCS network. In addition to the prompt, the procedure requires a separate call from the vendor to the utility describing the need to remotely connect before the utility will complete the connection. The threat agent calls the utility and claims the need to collect routine system performance information. The utility connects the vendor maintained computer to the DCS network, giving the threat agent access. The payload delivered by the threat agent is a modified system file that starts polling networked assets sending commands that cause a flood of traffic in the DCS network. The commands overwhelm the processing ability of the network causing loss of DCS control of the plant. On loss of plant control, the assigned operator initiates an immediate unit trip.

GEN.15 Plant Tripped Off-Line Through Access Gained Through a Compromised Vendor Remote Connection

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Assumptions

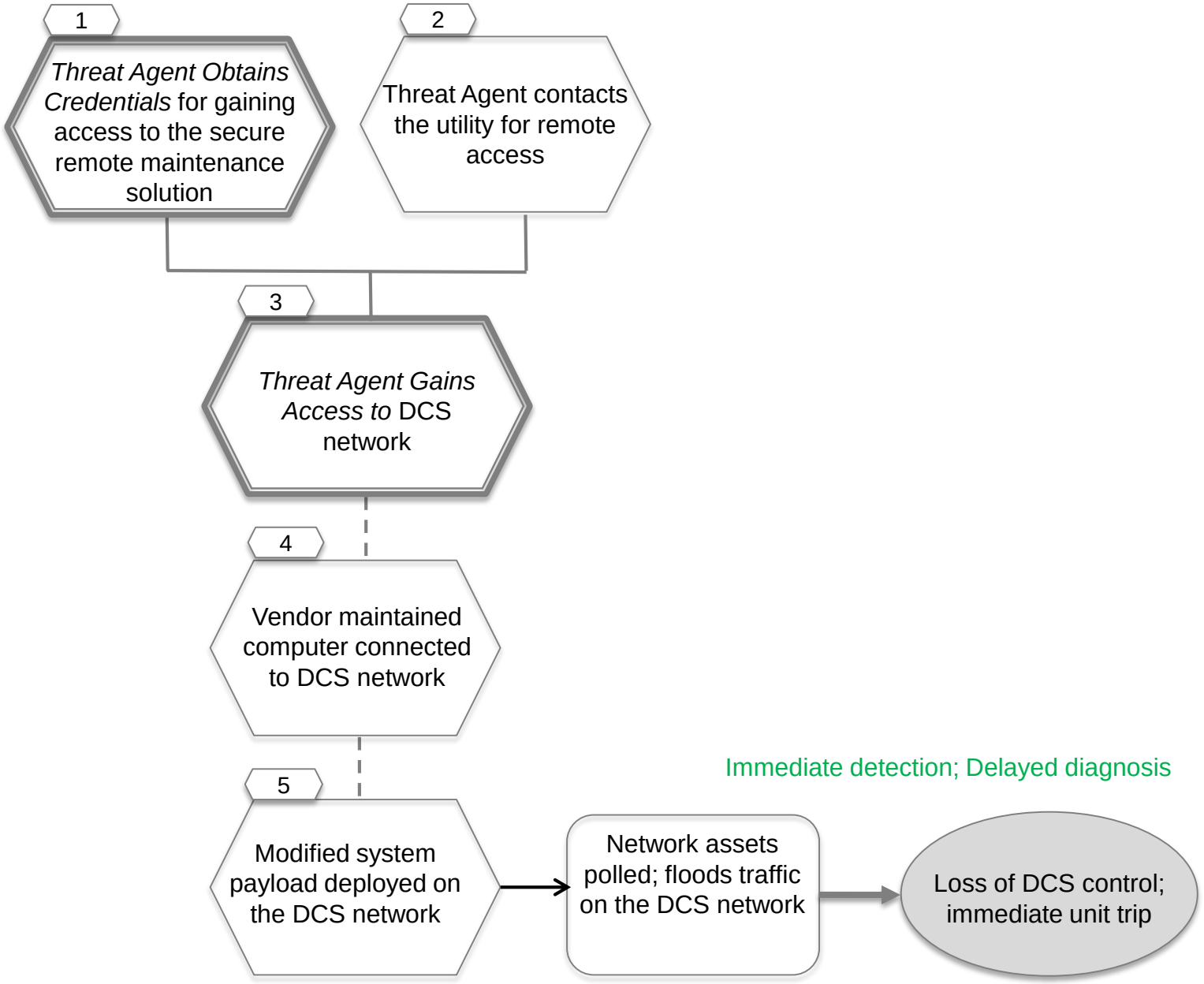
- The attacker has detailed knowledge of the system to develop and execute the attack.
- The attacker is employed by the vendor at the time of the attack.
- The equipment supported by the vendor, if disrupted, has immediate impact on operations.
- The vendor remote access solution is authorized though the DMZ and firewalls.
- The remote access solution allows administrative access to the control system or DCS. This allows the attacker to carry out the full scope of the attack.
- The vendor remote solution offers access to the balance-of-plant controls.
- The affected computer is centrally connected within the DCS network with connection to the systems required for operation.
- The vendor is not actively monitored when provided remote access through the vendor remote access solution.

GEN.15 Plant Tripped Off-Line Through Access Gained Through a Compromised Vendor Remote Connection

Assumptions (2)

- Utility employees follow all appropriate procedures when granting remote access, but those do not include control room notification.
- Vendor remote access to the utility network is not limited to the IP range of the vendor.
- The vendor uses a single support team to support all customers.
- The DCS does not employ an active configuration change detection solution.
- The backup system is in place and the files being backed up are sufficient for recovery. This has been confirmed by testing.
- The hardware is not damaged and does not require replacement parts to be shipped.

GEN.15 Plant Tripped Off-Line Through Access Gained Through a Compromised Vendor Remote Connection



Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Potential Mitigations

- *Train personnel* in proper configuration requirements for assets connected to the DCS system,
- *Enforce least privilege* for access to the DCS by limiting remote administrative access through vendor monitoring employee sessions for cases of configuration and file system changes,
- *Restrict remote access* to not allow direct file transfer as a default privilege,
- *Require second-level authentication* that includes:
  - management authorization for configuration changes and file transfers and
  - "Escorted remote access" requiring live monitoring of vendor access for potentially damaging actions.
- *Restrict configuration access* to limit who has access and can make configuration changes,
- *Create audit logs* that record the remote access sessions,

GEN.15 Plant Tripped Off-Line Through Access Gained Through a Compromised Vendor Remote Connection

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

- **Potential Mitigations**

  Detect unauthorized configuration changes to the asset,

  Automated *configuration change detection*,

  Detect unauthorized access in network traffic between the vendor and the DCS device,

  Require intrusion detection,

  Detect abnormal behavior in machines and flag this behavior,

  Require application whitelisting on the DCS network.

Common Sub Trees

- Threat Agent Gains Capability to Reconfigure <firewall>
- Threat Agent Blocks Wireless Communication Channel Connecting <x and y>
- Authorized Employee Brings Malware into <system or network>
- Threat Agent Obtains Credentials for <system or function>
- Threat Agent Uses Social Engineering to <desired outcome>
- Threat Agent Exploits Firewall Gap in <specific firewall>
- Threat Agent Exfiltrates <data>
- Threat Agent Gains Access to <network>

Common Tree: Threat Agent Gains Capability to Reconfigure <firewall>

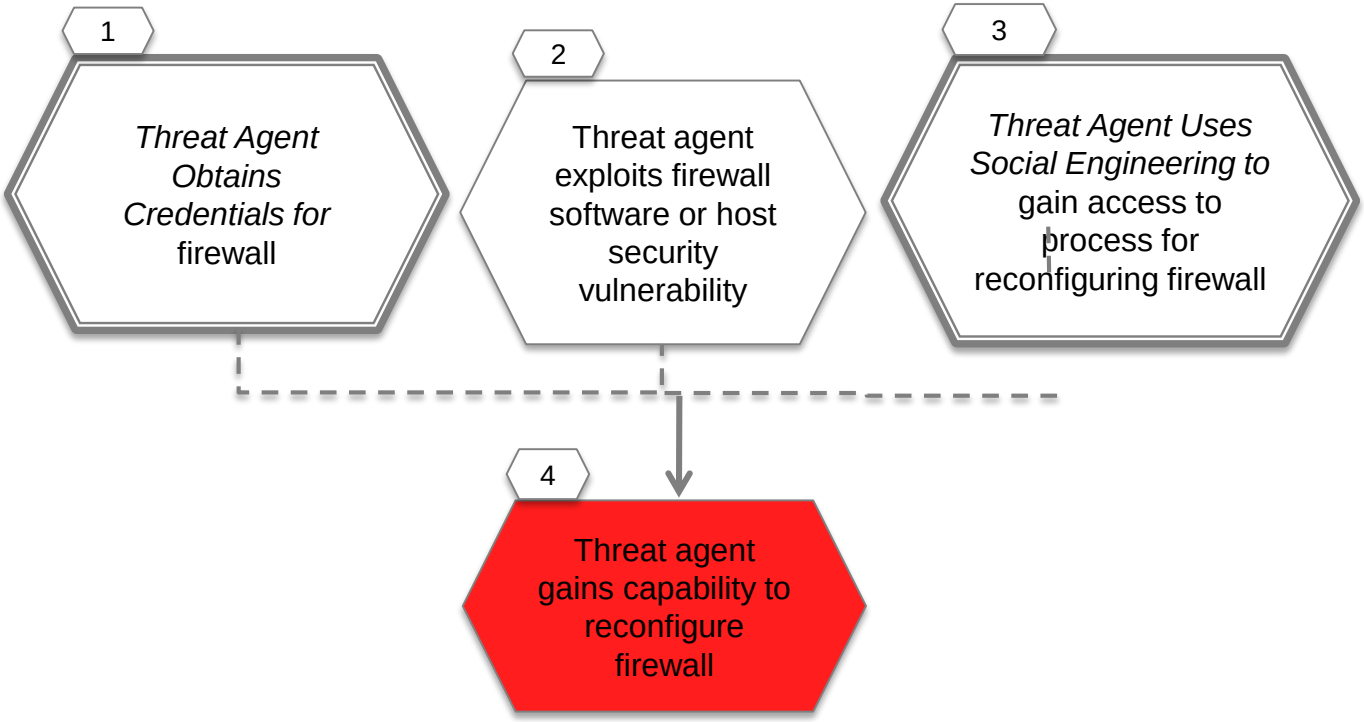
Description

A threat agent gains the capability to change firewall rules on a specific firewall to permit types of traffic to flow through the firewall that will enable future attacks.

Assumptions

- Threat agent has access to a network with a firewall interface

Common Tree: Threat Agent Gains Capability to Reconfigure <firewall>



Common Tree: Threat Agent Gains Capability to Reconfigure <firewall>

Potential Mitigations

1 - See mitigations for common sub tree *Threat Agent Obtains Credentials for* <system or function>

2 - Conduct penetration testing to uncover firewall vulnerabilities

2 - Implement configuration management for the firewall system

2 - Maintain patches on firewall system

2 - Detect unauthorized access through traffic monitoring, specifically to detect reconnaissance; *Generate alarm* on detection

2 - Require intrusion detection and prevention

2 - Create audit log of attempts to access firewall host

2 - Require authentication for system and database access to firewall

2 - Restrict database access on firewall to authorized applications and/or locally authenticated users

3 - See mitigations for common sub tree *Threat Agent Uses Social Engineering to* <desired outcome>

Common Tree: Threat Agent Blocks Wireless Communication Channel Connecting <x and y>

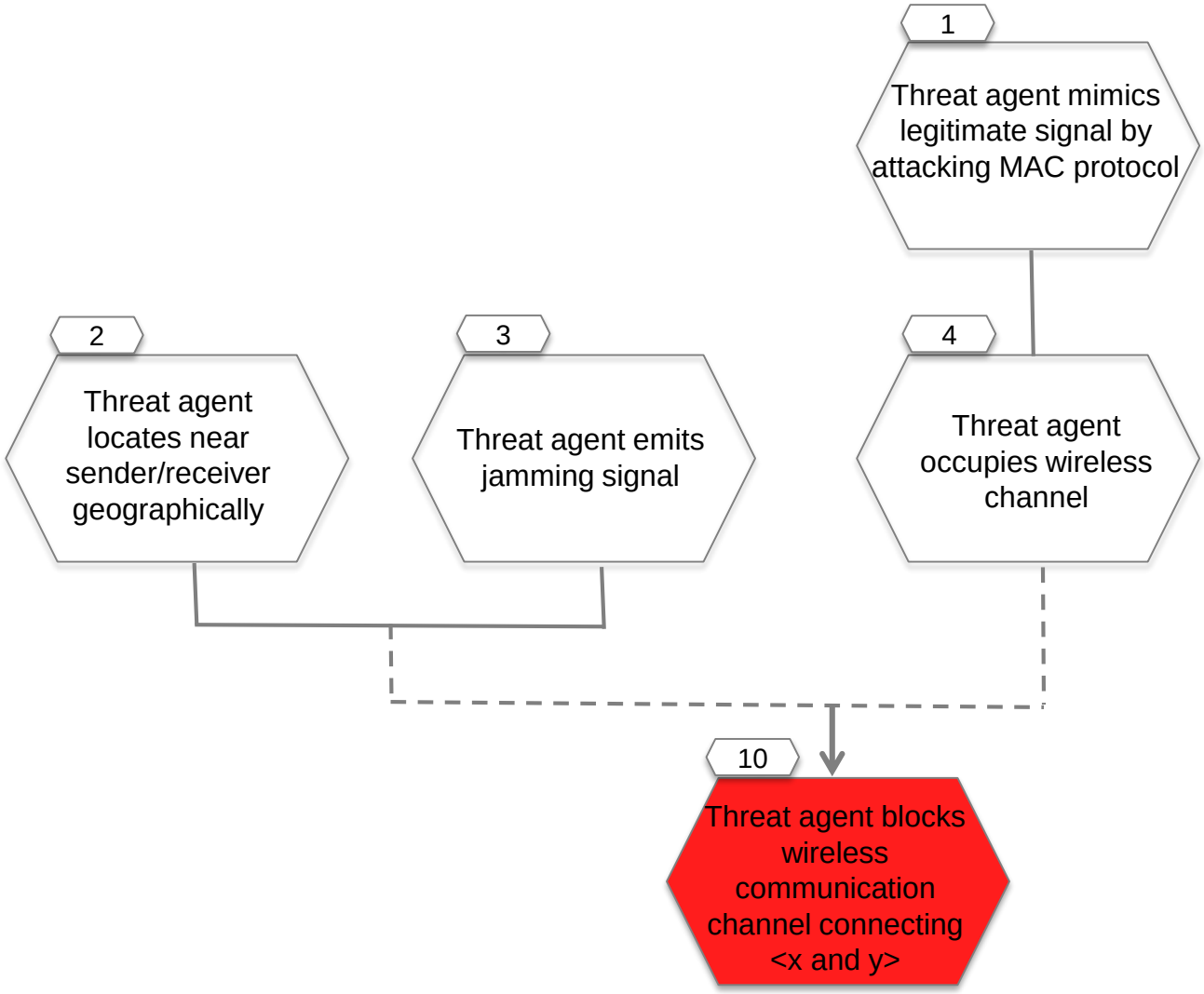
Description

The threat agent stops the flow of messages on a wireless communication channel connecting two entities, or slows it down to a point that it is essentially stopped.

Assumptions

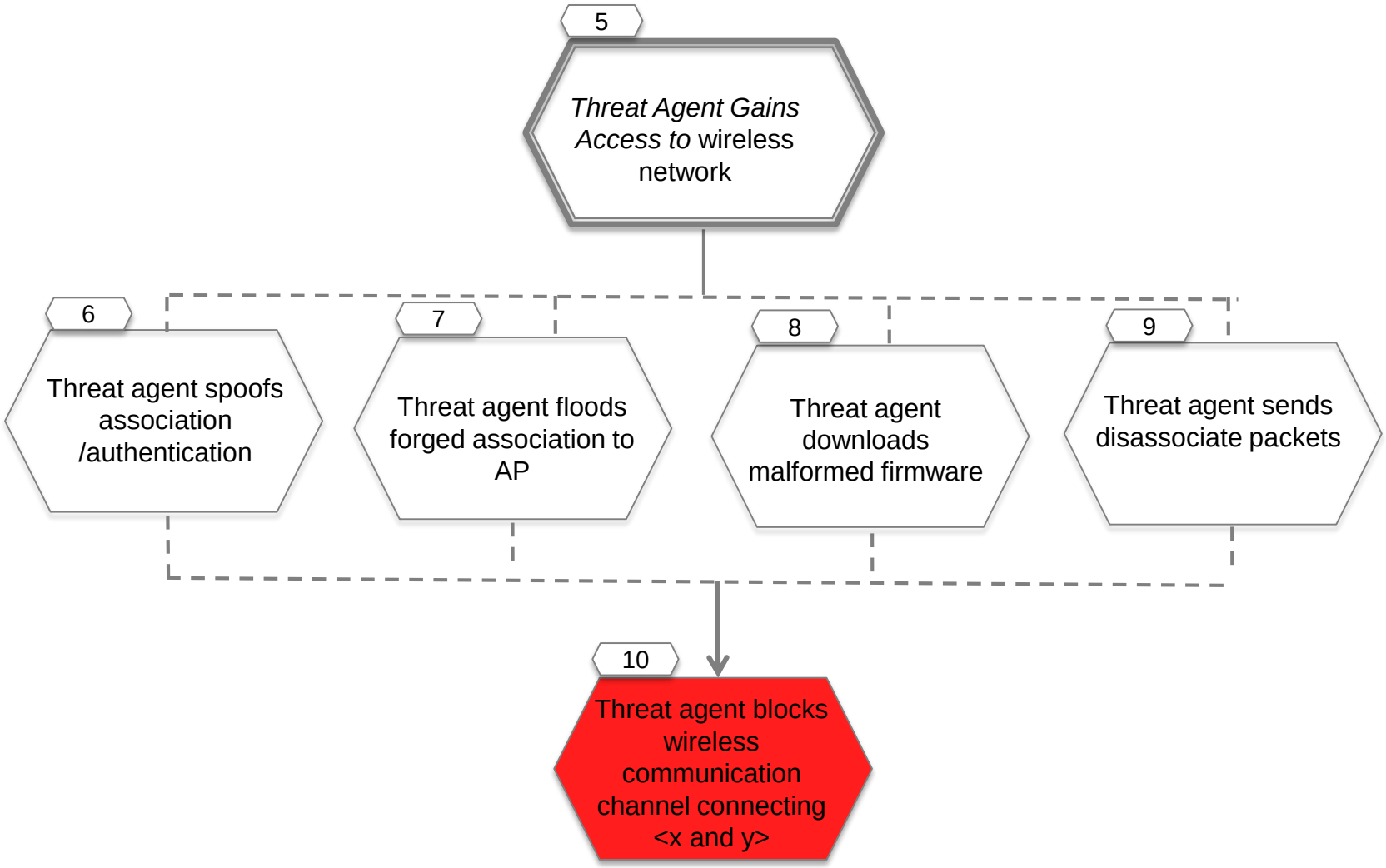
The backbone network for this wireless channel is wired, e.g., the Internet. Therefore, the wireless communication connecting <x and y> consists of two wireless channels in the access networks: node/station x to the wireless Access Point (AP) and the wireless AP to node/station y. Assuming these two channels are functionally the same, this common sub tree considers the wireless channel between the wireless AP and a node/station, x or y. The terms ‘sender’ and ‘receiver’ refer to the entity that sends or receives the wireless signal, respectively, which may be an AP or a node/station.

Common Tree: Threat Agent Blocks Wireless Communication Channel Connecting <x and y>



(1/2)

Common Tree: Threat Agent Blocks Wireless Communication Channel Connecting <x and y>



Common Tree: Threat Agent Blocks Wireless Communication Channel Connecting <x and y>

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Potential Mitigations

1 - *Create audit logs* for network connectivity; *Restrict remote access*; *Require multi-factor authentication*

2 - Restrict physical access to APs and nodes/stations

3 - Detect unusual patterns on wireless channel; *Generate alarm* on detection 4 - *Create audit logs* for network connectivity

5 - See mitigations for common sub tree *Threat Agent Gains Access to <network>*

6 - Detect unusual patterns on authentication and association for wireless communication

7 - Generate alarm on detection of abnormal association delay

8 - Generate alerts on changes to configurations; *Detect unauthorized configuration changes; Maintain patches* on all systems; *Maintain anti-virus* on all systems

9 - Generate alarm on network disconnection

Common Tree: Authorized Employee Brings Malware into <system or network>

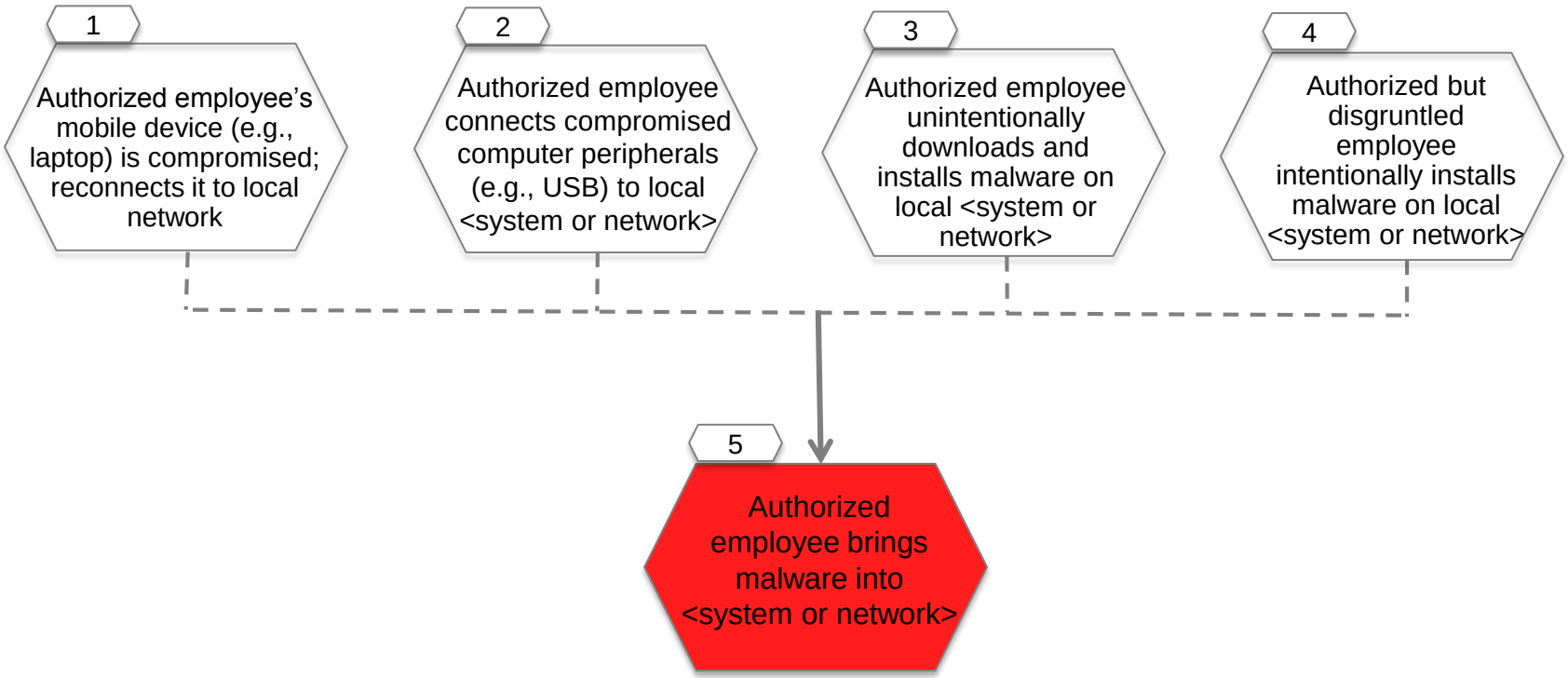
Description

An authorized employee uses the IT infrastructure to perform any action that results in the introduction of a particular piece of malware onto a specific network or a system.

Assumptions

- The network under discussion is protected by perimeter security tools (e.g., enterprise firewall), and communications within the local network is less restricted (e.g., no port number filtering and internet protocol (IP) address filtering).
- Once a compromised device is connected to the local network, the malware may infect other systems in the network.
- A compromised device may be remotely controlled by a threat agent.

Common Tree: Authorized Employee Brings Malware into <system or network>



Common Tree: Authorized Employee Brings Malware into <system or network>

Potential Mitigations

1, 2, 3 - Train personnel regarding possible paths for infection to internal network

1, 2, 3, 4 - Maintain patches on all systems; *Maintain anti-virus* on all systems; *Require intrusion detection and prevention*

1, 2 - Create policy regarding connection of mobile devices and peripherals to the network; *Test for malware* before connecting mobile device or peripheral to local network

4 - Verify personnel to find any previous actions against employers

Common Tree: Threat Agent Obtains Credentials for <system or function>

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

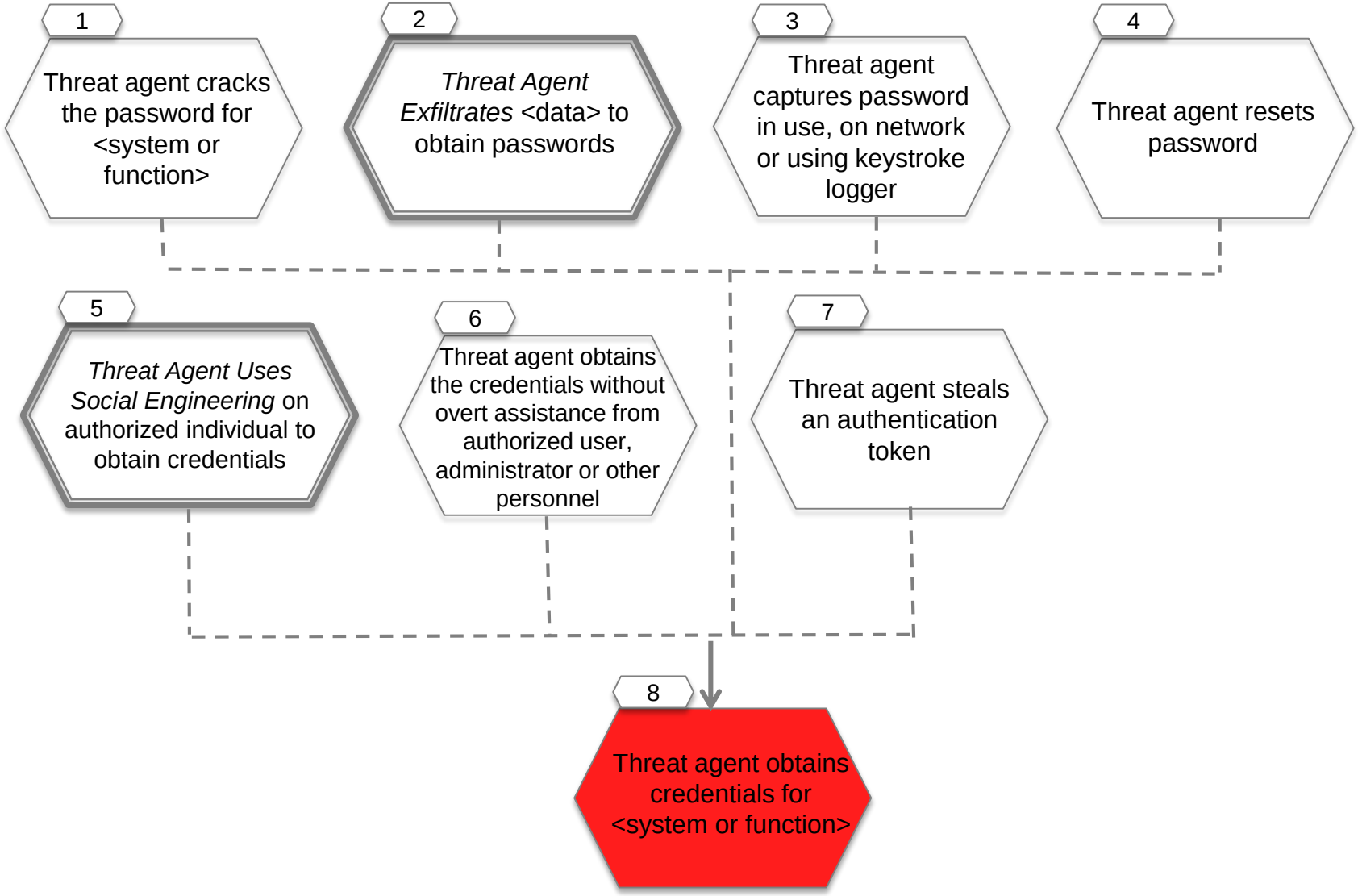
Description

A threat agent may gain credentials for a system, or credentials that provide privileges to perform specific functions, in a number of ways. This includes finding them, stealing them, guessing them, or changing them. The threat agent may use social engineering techniques to carry out these methods. Each technology and implementation used for credentials is resistant to some methods and susceptible to others.

Assumptions

- Credentials used are either any static piece of data (referred to as a password), biometrics, or a physical object (such as a key card/token).
- If multi-factor authentication is used, such as a token with a PIN, the adversary must take additional steps to obtain all “factors” of the credentials.

Common Tree: Threat Agent Obtains Credentials for <system or function>



Common Tree: Threat Agent Obtains Credentials for <system or function>

Potential Mitigations

1 - Design for security by using strong passwords

2 - See mitigations for common sub tree *Threat Agent Exfiltrates* <data>

2 - Design for security by not recording clear text passwords in log files

3 - Test for malware on user devices

3 - Design for security by not sending passwords in the clear over the network

3 - *Encrypt communication paths* on the network

3 - Protect against replay on the network

4 - Design for security by using strong security questions and protect answers

5 - See mitigations for common sub tree *Threat Agent Uses Social Engineering to* <desired outcome>

6 - Design for security by using strong security questions and protect answers; *Require multi-factor authentication*

7 - Require multi-factor authentication such as using a token with a PIN

7 - *Define policy* regarding reporting and revocation of missing tokens

Common Tree: Threat Agent Uses Social Engineering to <desired outcome>

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

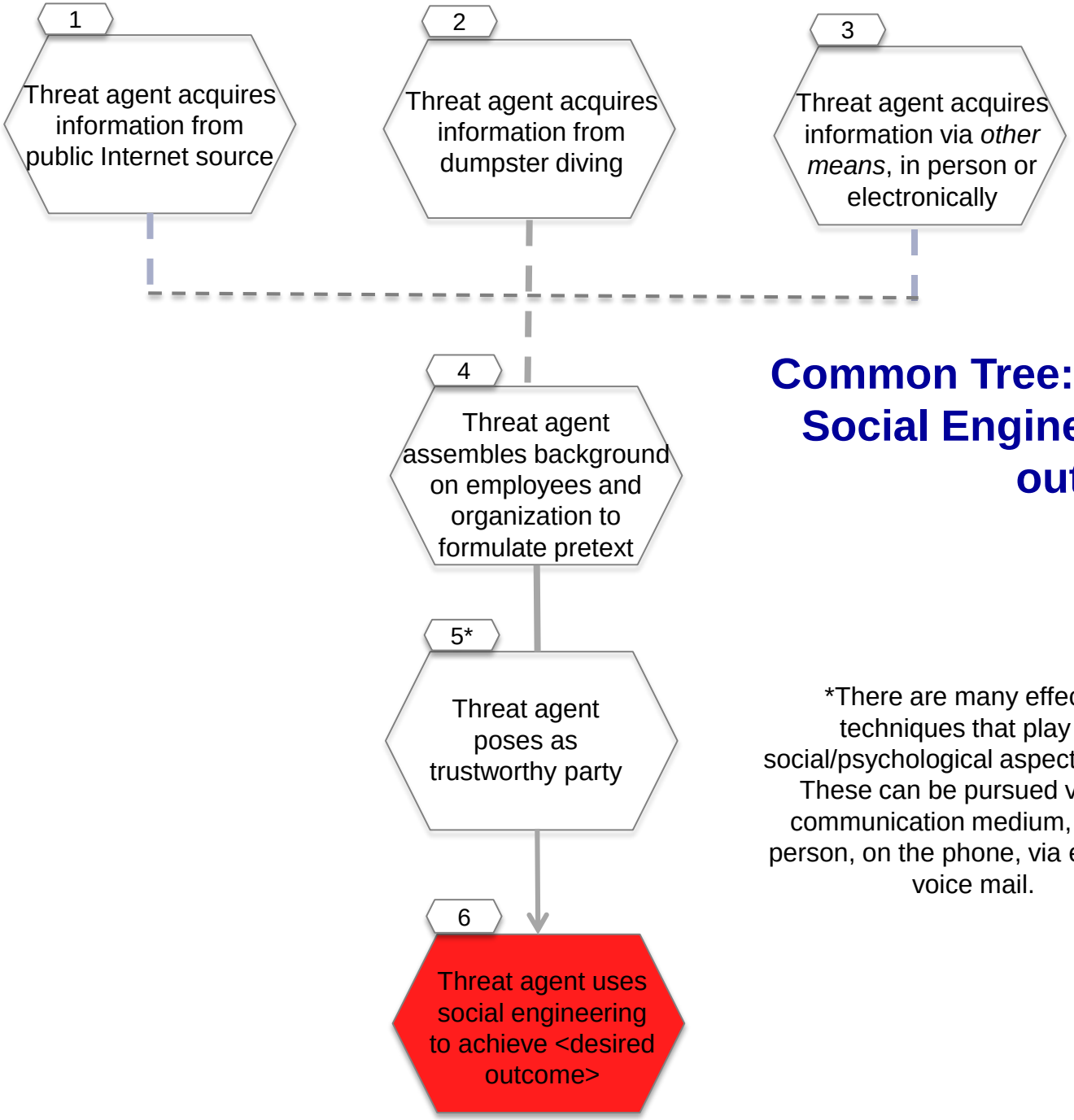
Description

A threat agent uses techniques of social engineering to persuade a victim to perform a desired action that results in an outcome that benefits the threat agent. Common examples of actions are to disclose particular information or to install/execute software that collects information or harms the victim's IT environment.

- **Notes**
  - The attack tree provides an overview of the use of social engineering, there are many varieties
  - More details and common examples may be found at: http://www.social-engineer.org/framework/Social_Engineering_Framework

Assumptions

- None currently identified



Common Tree: Threat Agent Uses Social Engineering to <desired outcome>

*There are many effective techniques that play on social/psychological aspects of trust. These can be pursued via any communication medium, e.g., in person, on the phone, via email, via voice mail.

Common Tree: Threat Agent Uses Social Engineering to <desired outcome>

Research conducted by EPRI for:
NESCOR – a DOE funded public-private partnership

Potential Mitigations

1 - Define policy to minimize Internet disclosure, e.g., “do not make calendars public”

1, 2, 3, 5 - Conduct penetration testing periodically, posing as a threat agent (Conditions 1, 2, 3, 5)

2 - Define policy to minimize leakage of physical artifacts (e.g., shredding, locked receptacle)

5 -Train personnel that they are potentially targeted for these types of attacks and the consequences for the organization

5 - Train personnel to report social engineering attacks

5 -Track social engineering attacks and warn personnel

5 -Train personnel including users and administrators in procedures to foil threat agents, e.g., always call back to the number in the directory

Common Tree: Threat Agent Exploits Firewall Gap in <specific firewall>

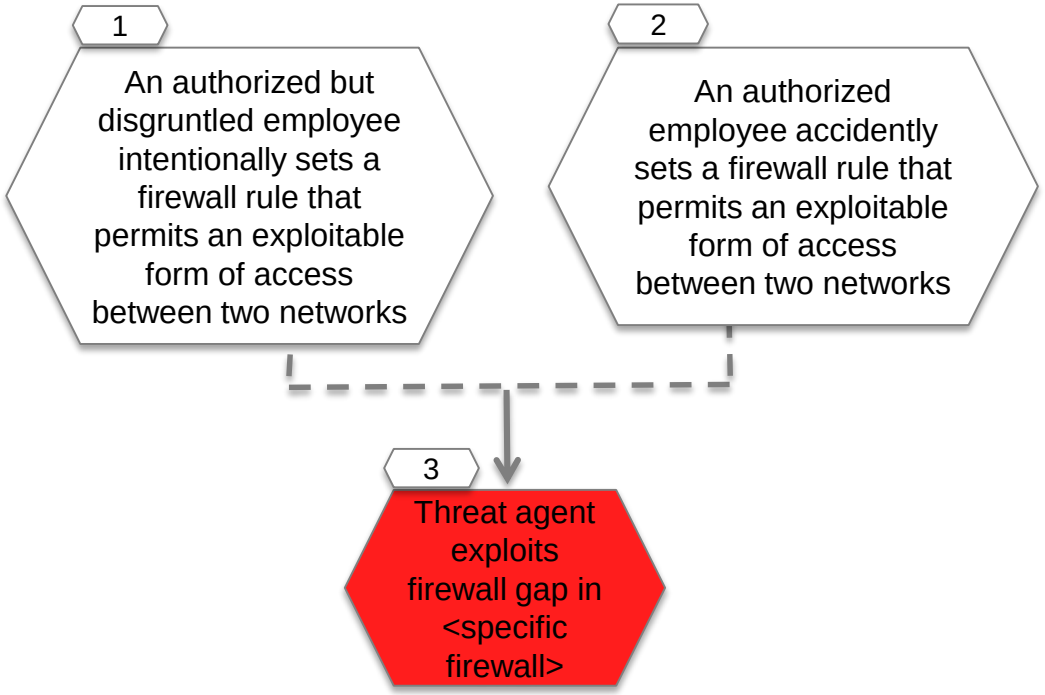
Description

An authorized employee either accidently or intentionally sets a firewall rule that allows an unnecessary and exploitable form of access to a network from another network.

Assumptions

- None currently identified

Common Tree: Threat Agent Exploits Firewall Gap in <specific firewall>



Common Tree: Threat Agent Exploits Firewall Gap in <specific firewall>

Potential Mitigations

1, 2 - Conduct penetration testing to uncover firewall gaps, *implement configuration management* to protect entire system

1, 2 - *Verify all firewall changes*

1, 2 - Require intrusion detection and prevention

1, 2 - Require authentication to network

1, 2 - Restrict database access to the firewall to authorized applications and/or locally authenticated users

Common Tree: Threat Agent Exfiltrates <Data>

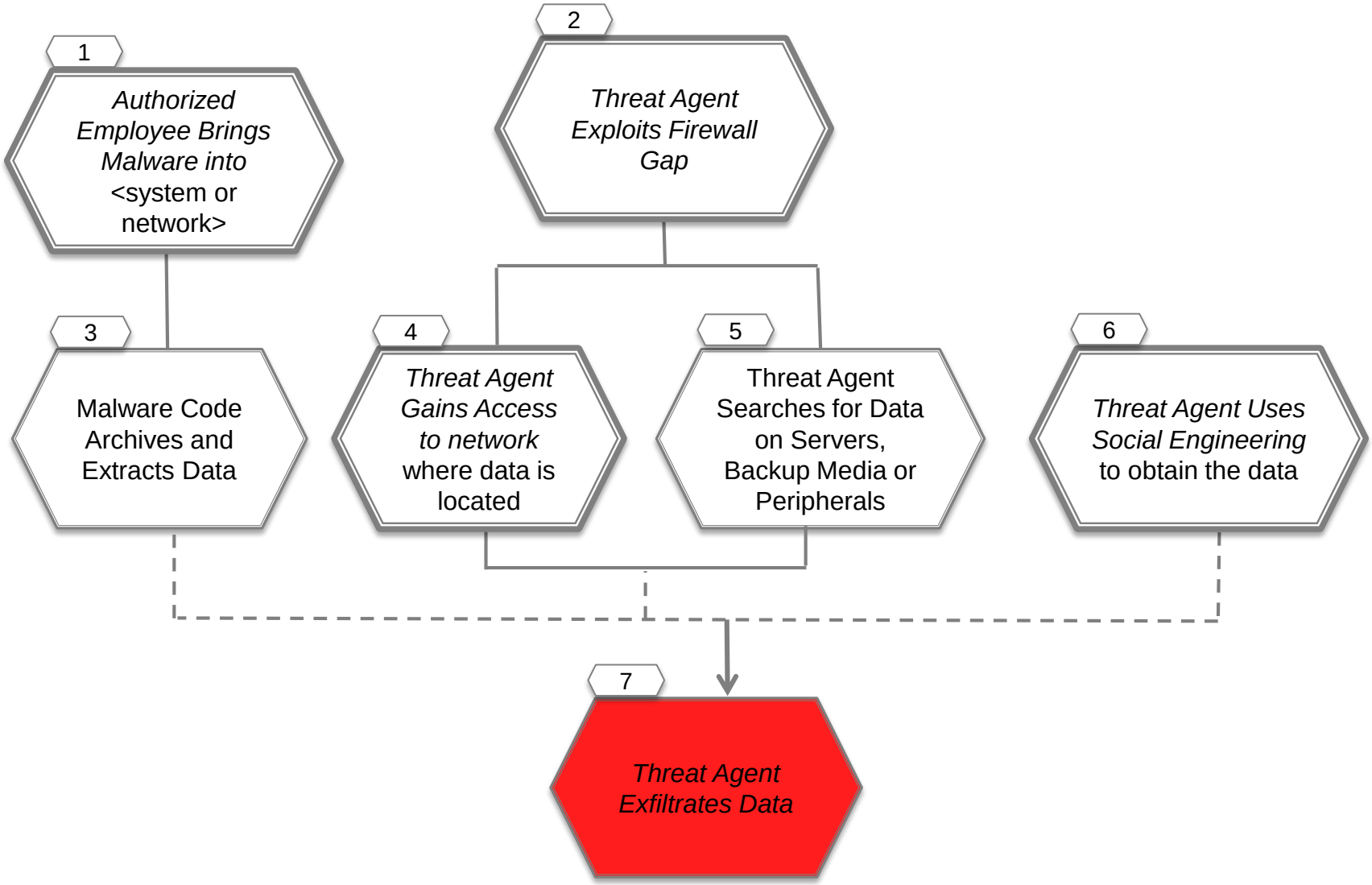
Description

A threat agent may use direct or indirect methods to obtain a copy of a file or data, including a direct break-in to the host holding the file, finding the data on back up media, scanning peripherals such as printers, and use of social engineering to influence a victim to give them the data.

Assumptions

- None currently identified

Common Tree: Threat Agent Exfiltrates <Data>



Common Tree: Threat Agent Exfiltrates <Data>

Potential Mitigations

1 - Train personnel to protect against malware

1, 3 -Test for malware on system or network

1 - Require on-going validation of software/firmware

2 - See mitigations for common sub tree *Threat Agent Exploits Firewall Gap in <specific firewall>*

3 - Detect abnormal output (unexpected data or destinations)

4 - See mitigations for common sub tree *Threat Agent Gains Access to* <network>

4 - Authenticate users to servers, backup media, and peripherals

4 - Enforce least privilege for individuals with access to hosts on the network

5 - Detect unusual patterns of usage on hosts and network

6 - See mitigations for common sub tree *Threat Agent Uses Social Engineering to* <desired outcome>

Common Tree: Threat Agent Gains Access to <network>

Description

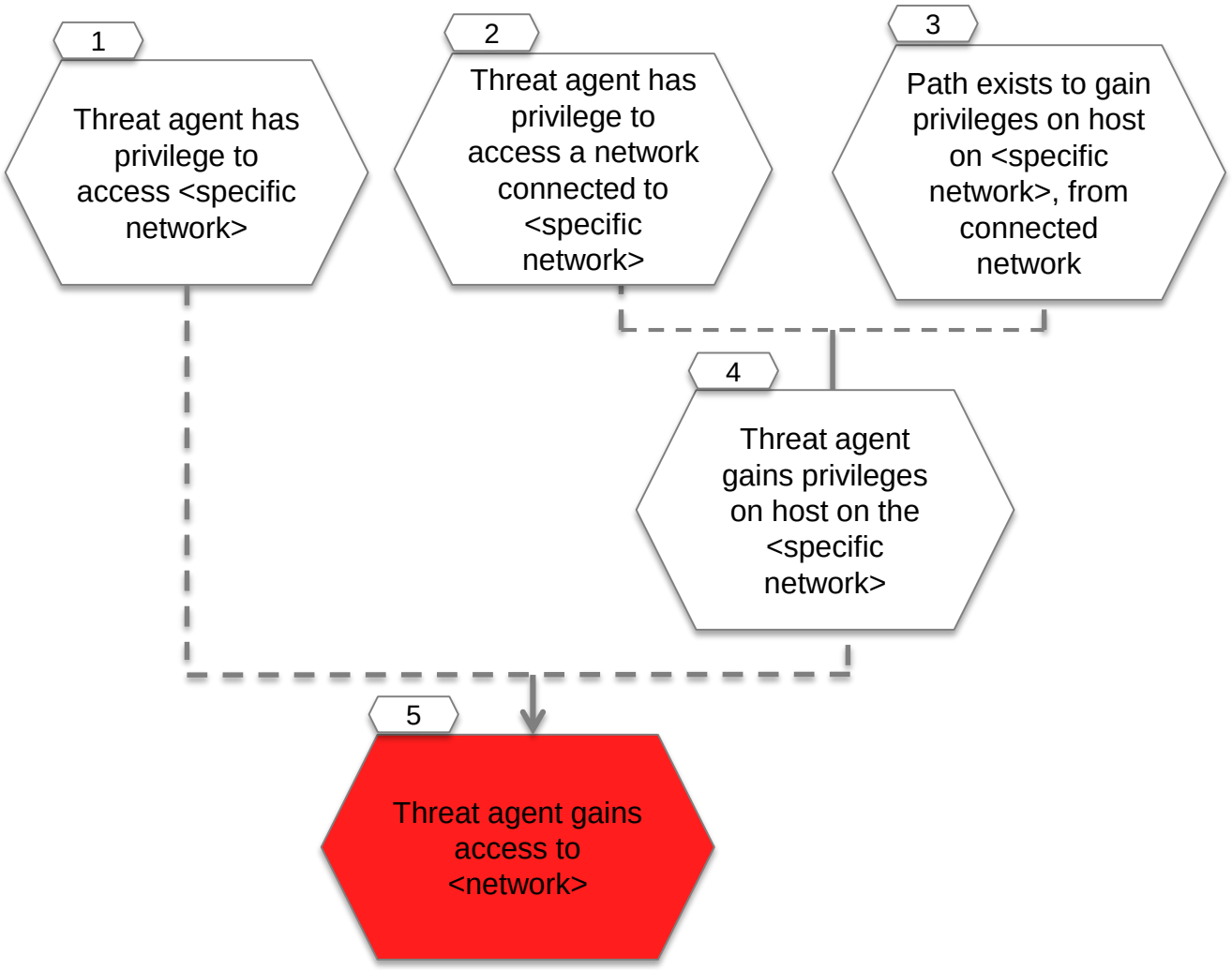
A threat agent becomes capable of sending traffic within a network and attempting to communicate with its resident hosts.

- **Note:** This draft tree currently expresses the high level concept of "bridging" sequentially between adjacent networks. Information should be added in future drafts related to:
  - Mitigations for detecting and preventing network reconnaissance
  - Specific differences in gaining access to networks that use various protocols and technologies

Assumptions

- None currently identified

Common Tree: Threat Agent Gains Access to <network>



Common Tree: Threat Agent Gains Access to <network>

Potential Mitigations

1, 2 - Enforce least privilege to limit individuals with privilege to the network and connected networks

2 - Isolate network

3 - Enforce restrictive firewall rules for access to network

3 - Design for security by limiting connection points to networks that are widely accessible and by limiting number of hosts on same network

3 - Require authentication to the network

4 - Enforce least privilege for individuals with access to hosts on the network

4 - Detect unusual patterns of usage on hosts and network

Acronyms Used in Trees

AMI	Advanced Metering Infrastructure
AP	Access Point
DCS	Distributed Control System
DDOS	Distributed Denial of Service
DMS	Distribution Management System
DMZ	Demilitarized Zone
DOS	Denial of Service
DR	Demand Response
DRAS	Demand Response Administration System
GUI	Graphical User Interface
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network

Acronyms Used in Trees (2)

MAC	Media Access Control
MITM	Man in the Middle
NESCOR	National Electric Sector Cybersecurity Organization Resource
RBAC	Role Based Access Control
SCADA	Supervisory Control and Data Acquisition
S/W	Software
USB	Universal Serial Bus
3G	LTE Third Generation Long Term Evolution

Together…Shaping the Future of Electricity