Daily Alert – Example 1

From: alert@security-bulletins.com
Sent: Tuesday, January 12, 2020 3:30 AM
To: My Technicians
Subject: Network Detective Daily Alerts - Customer ABC

THREATS

1. [H] Unauthorized access to accounting computer **corp.myco.com\jane-hp**:
    - myco\jane

    Because of its sensitive nature, access to the accounting should be highly restricted. If the user should have access, tag them as an Accounting User.

2. [H] Unauthorized access to computer containing ePHI **corp.myco.com\frank-pc**:
    - myco\dgreen
    - myco\paul

    Because of its sensitive nature, access to any system with ePHI should be highly restricted. If the user should have access, tag them as a HIPAA Authorized User.

3. [M] Computer that should not have direct Internet access not properly restricted:
    - corp.myco.com\maury-pc (192.168.2.3)
    - corp.myco.com\intranet1 (192.168.1.16)
    - corp.myco.com\intranet1build (192.168.6.67)

    Ensure a misconfiguration has not inadvertently allowed this system to access the Internet directly.

4. [M] Critical security patches have not been installed on the following computers in a timely manner (last 30 days):
    - TOM-WIN8 (192.168.7.44) missing 24 critical updates

    Keeping up with critical security patches is one of the best defenses against malicious attackers and software.

ANOMALIES

There are no anomalies to report at this time.

CHANGES

1. [M] Unauthorized printer found on network:
    - \\greend\SEC30CDA792322C (192.168.6.35)
    - \\BRUCE-PC\Brother Color Leg Type1 Class Driver (192.168.6.9)

    Printing to an unauthorized printer may lead to inadvertent information disclosure. Any printer not authorized should be remove from the network.

2. [M] New local administrator added to **TOM-WIN8**:
    - administrator
    - jon
    - stark

    Local administrator accounts may be used to bypass domain level security. Verify if the new local administrator account is authorized.

3. [M] New local administrator added to **ACCOUNTING-HP**:
    - administrator

    Local administrator accounts may be used to bypass domain level security. Verify if the new local administrator account is authorized.

4. [M] New local administrator added to **MARY-PC**:
    - administrator

    Local administrator accounts may be used to bypass domain level security. Verify if the new local administrator account is authorized.

RapidFireTools

Daily Alert – Example 2

From: alert@security-bulletins.com
Sent: Saturday, January 16, 2020 3:30 AM
To: My Technicians
Subject: Network Detective Daily Alerts - Customer ABC

THREATS

1. [H] Unauthorized access to accounting computer **corp.myco.com\jane-hp**:
    - myco\jane

    Because of its sensitive nature, access to the accounting should be highly restricted. If the user should have access, tag them as an Accounting User.

2. [H] Unauthorized access to computer containing ePHI **corp.myco.com\jane-hp**:
    - myco\jane

    Because of its sensitive nature, access to any system with ePHI should be highly restricted. If the user should have access, tag them as a HIPAA Authorized User.

3. [M] Computer that should not have direct Internet access not properly restricted:
    - corp.myco.com\maury-pc (192.168.2.3)
    - corp.myco.com\intranet1 ()
    - corp.myco.com\intranet1build (192.168.6.67)

    Ensure a misconfiguration has not inadvertently allowed this system to access the Internet directly.

4. [M] Critical security patches have not been installed on the following computers in a timely manner (last 30 days):
    - TOM-WIN8 (192.168.7.44) missing 24 critical updates

    Keeping up with critical security patches is one of the best defenses against malicious attackers and software.

ANOMALIES

1. [L] Login attempt outside normal time frames by user **tywin**:
    - TOM-WIN8 - Friday, 2016-05-20 18:58:28

    Verify that the user's account to resources outside their normal usage pattern was authorized.

2. [L] Login attempt outside normal time frames by user **jane**:
    - ACCOUNTING-HP - Friday, 2016-05-20 12:43:26
    - ACCOUNTING-HP - Friday, 2016-05-20 19:33:42

    Verify that the user's account to resources outside their normal usage pattern was authorized.

CHANGES

1. [M] Unauthorized printer found on network:
    - \\greend\SEC30CDA792322C (192.168.6.35)
    - \\BRUCE-PC\Brother Color Leg Type1 Class Driver (192.168.6.9)

    Printing to an unauthorized printer may lead to inadvertent information disclosure. Any printer not authorized should be remove from the network.

2. [M] New local administrator added to **TOM-WIN8**:
    - administrator
    - jon
    - stark

    Local administrator accounts may be used to bypass domain level security. Verify if the new local administrator account is authorized.

3. [M] New local administrator added to **ACCOUNTING-HP**:
    - administrator

    Local administrator accounts may be used to bypass domain level security. Verify if the new local administrator account is authorized.

4. [L] A new user has been added to your network:
    - Lin Miranda (myco\lmiranda)

    New users do not always represent a threat, but you should always be aware when new users are added.

RapidFireTools

Daily Alert – Example 3

From: alert@security-bulletins.com
Sent: Wednesday, January 20, 2020 3:30 AM
To: My Technicians
Subject: Network Detective Daily Alerts - Customer ABC

THREATS

1. [M] Computer that should not have direct Internet access not properly restricted:
    - corp.myco.com\maury-pc (192.168.2.3)
    - corp.myco.com\intranet1 (192.168.1.16)
    - corp.myco.com\intranet1build (192.168.6.67)

    Ensure a misconfiguration has not inadvertently allowed this system to access the Internet directly.

ANOMALIES

There are no anomalies to report at this time.

CHANGES

1. [M] Unauthorized printer found on network:
    - \\greend\SEC30CDA792322C (192.168.6.35)

    Printing to an unauthorized printer may lead to inadvertent information disclosure. Any printer not authorized should be remove from the network.

2. [L] A new user profile added to computer **corp.myco.com\dc03**:
    - Carl Grande (corp.myco.com\cmgrande)

    A new user profile is typically added when a person who has never logged into a computer successfully logs in. New users will typically do this on their own workstation, but suspicious creation of profiles could indicate a user accessing a system they should not.

