Diyar United Company

Cyber Security Operations Center

Building your cyber defenses

APEX Cyber Insurance Conference

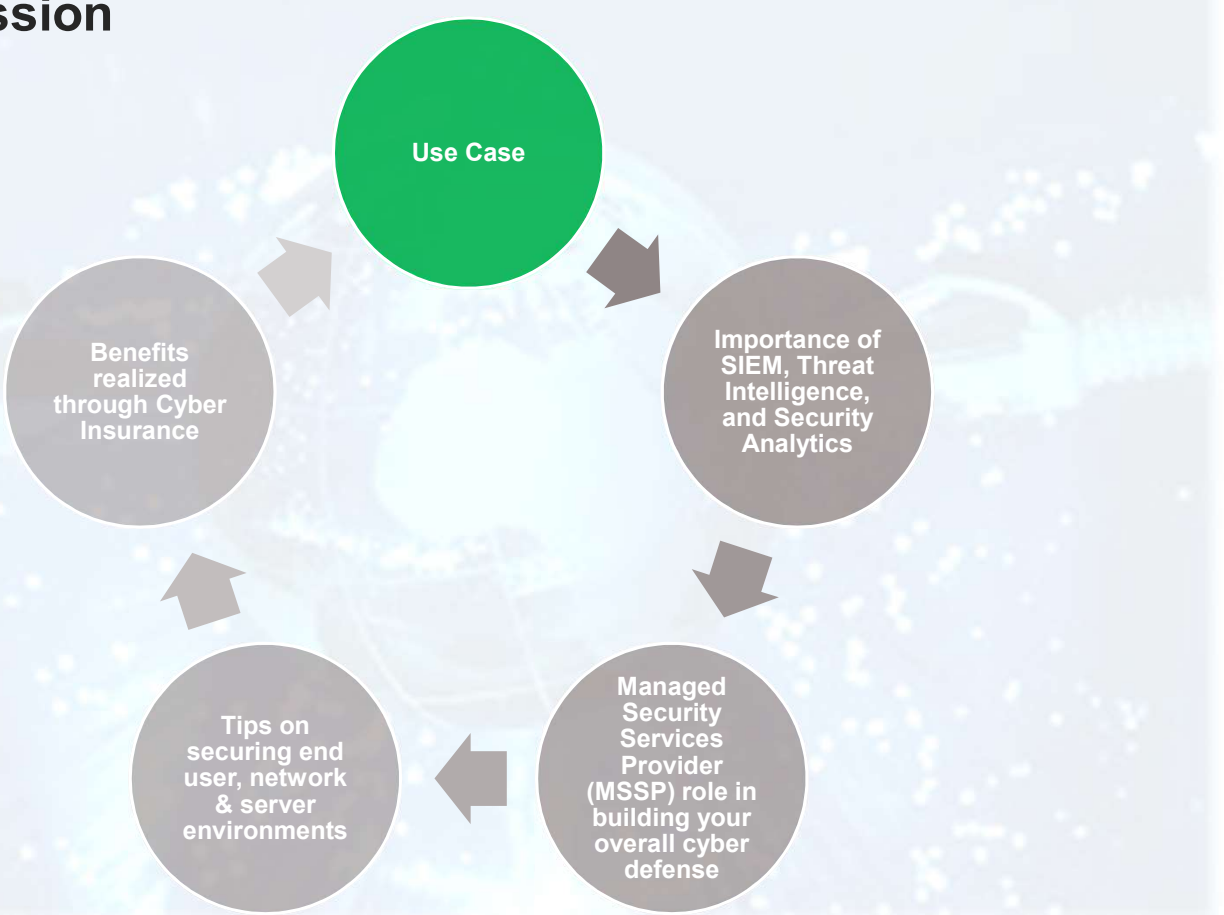
Tuesday, March 27, 2018

Ali Khan, Diyar United Company

Our discussion

CSOC
Diyar United Company
Cyber Security Operations Center

Our discussion



CSOC
Diyar United Company
Cyber Security Operations Center

Case: Vulnerabilities within pacemakers

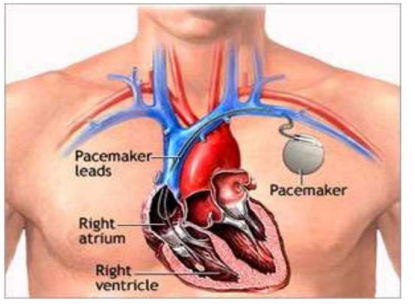
MedSec's CEO: St. Jude Has History of Sweeping Things Under Table, **length: 4:36 mins.**

Reference: https://www.youtube.com/watch?v=curdJoTysF8

St. Jude: Medical device maker (pacemaker)

MedSec: Vulnerability research and security solutions provider for healthcare manufacturers, vendors, and providers

Muddy Waters: Investment Research Biz



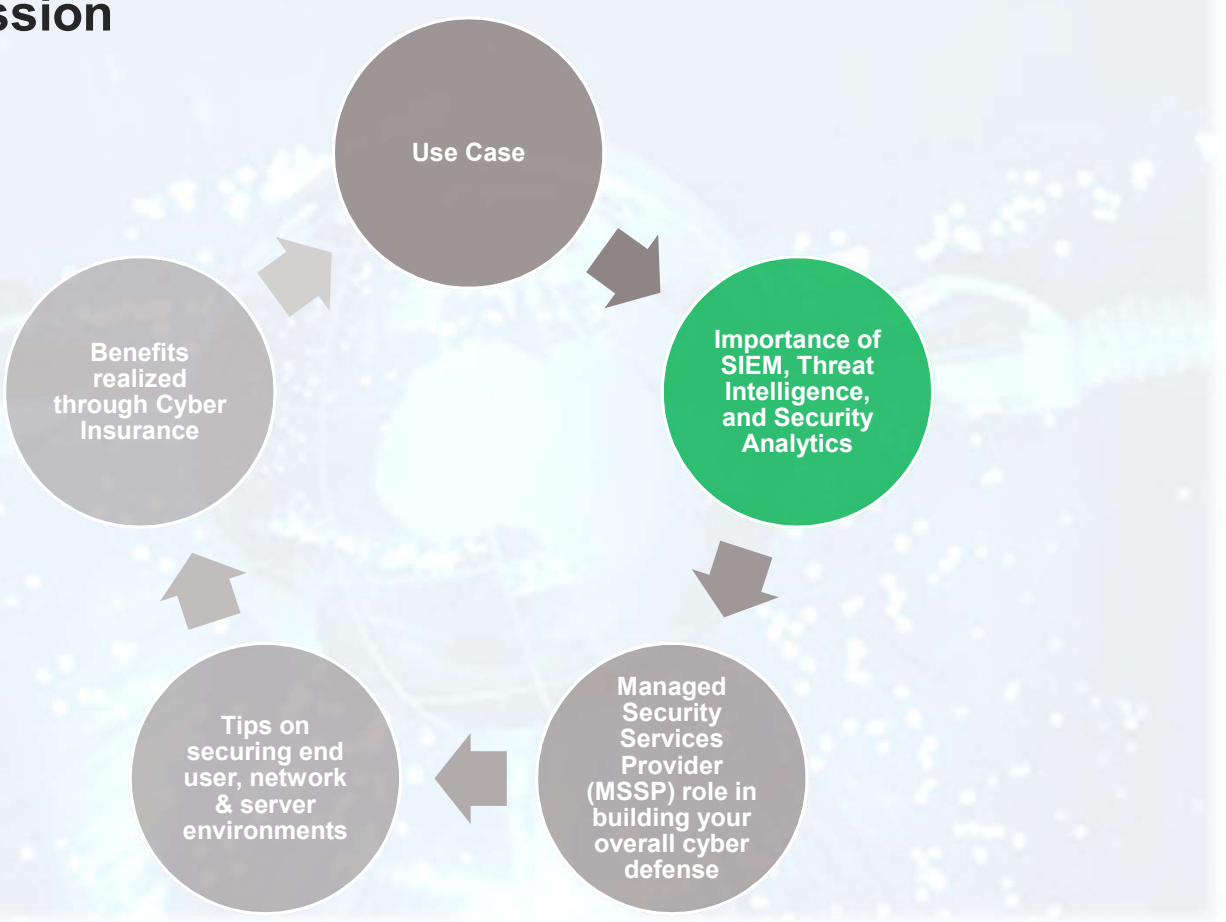
A **pacemaker** is a small device that's placed in the chest or abdomen to help **control abnormal heart rhythms.** This device uses electrical pulses to prompt the heart to beat at a normal rate.

Case:

Medical device maker St Jude has filed suit against a security startup that shorted its stock and publicized alleged flaws in its products for profit. The allegations include false advertising, false statements, conspiracy, and market manipulation.

Reference: http://www.theregister.co.uk/2016/09/07/st_jude_sues_over_hacking_claim/

Our discussion



CSOC
Diyar United Company
Cyber Security Operations Center

Why Security Information and Event Management (SIEM)?

- ✓ Visibility into network, server and application activity
- ✓ Monolithic and trend based threat detection
- ✓ Store raw information from various systems logs
- ✓ Aggregate the information in a single repository
- ✓ Normalize the information to make comparisons more meaningful
- ✓ Correlate, map and extract target information
- ✓ Alerting and reporting tool
- ✓ Maintaining the monitoring requirements of regulations, compliance, etc.

Audit log retention, visibility and compliance:

Challenge: Organizations need to maintain compliance to certain audit log retention requirements

Solution: SIEM technologies can provide audit log retention based on defined retention periods and provide threat monitoring use cases related to compliance

Forensics:

Challenge: Analyst must preserve the data in a way that makes it admissible in a court of law**.**

Solution: SIEM technologies allow for rapid, thorough and court-admissible forensics investigations.

Advanced persistent threats:

Challenge: Firewalls and IDS/IPS, two-factor authentication, internal firewalls, network segmentation, HIDS, AV all together generate a huge amount of data, which is difficult to monitor.

Solution: SIEM technologies bring all of these controls together into a single engine, capable of continuous real-time monitoring and correlation across the breadth and depth of the enterprise.

Alerting and reporting:

Challenge: Network security tools cannot correlate across an organizations network, server, and application spectrum to provide cyber threat alerting and reporting capabilities.

Solution: SIEM technologies have primarily functions related to log normalization and correlation.

Why Threat Intelligence?

Strategic cyber threat intelligence is the essential first step for protecting your business

By knowing what specific threats are coming your way and understanding their potential impact on your business, you can quickly align your security resources to address the risks that matter most.

- ✓ A proactive measure
- ✓ Continuously monitor external threats to key areas of your business
- ✓ Understand attack execution methods based on cyber trends related to your business profile
- ✓ Plan for attacks on your systems and sensitive information
- ✓ Know what information of yours may be available on the surface/deep/dark web
- ✓ Drive the most effective cyber defense tactics to mitigate business risk

Visibility into external threats:

To get effective visibility, an organization must have means of identifying and reviewing potential or active external threats that may be applicable or targeted to their environment.

Correlate external threats before they transpire into targeted threats to the organization:

Threat Intelligence functions as a proactive measure, enabling you to raise alerts before an actual incident may occur. It is a means to "stay ahead of the curve" in certain scenarios.

Monitor reputation, brand, and unauthorized data disclosure:

Ensure the organization maintains visibility across the deeper areas of the Web and can raise incidents if suspicious and unauthorized disclosures are discovered.

Why Security Analytics?

- ✓ Confidence based threat detection based on maching learning algorithms
- ✓ Non Indicator of Compromise (IoC) based threat detection
- ✓ Early warnings of potential threats
- ✓ Detecting low and slow events that traditional SIEMs will not detect
- ✓ Analyzing user behavior to detect potentially suspicious patterns
- ✓ Analyzing network traffic to pinpoint trends indicating potential attacks
- ✓ Identifying improper user account usage, such as shared accounts
- ✓ Detecting data exfiltration by attackers
- ✓ Detecting insider threats
- ✓ Identifying compromised accounts
- ✓ Investigating incidents
- ✓ Threat hunting
- ✓ Demonstrating compliance during audits

Zero-day threat detection:

Challenge: Many of the Firewalls, IDS/IPS and AV solutions are not equipped to detect zero-day attacks.

Solution: Security analytics can detect activity associated with an attack rather than the attack itself. Machine learning algorithms can function and provide behavioural based threat detection or Indicators of Compromise (IoC).

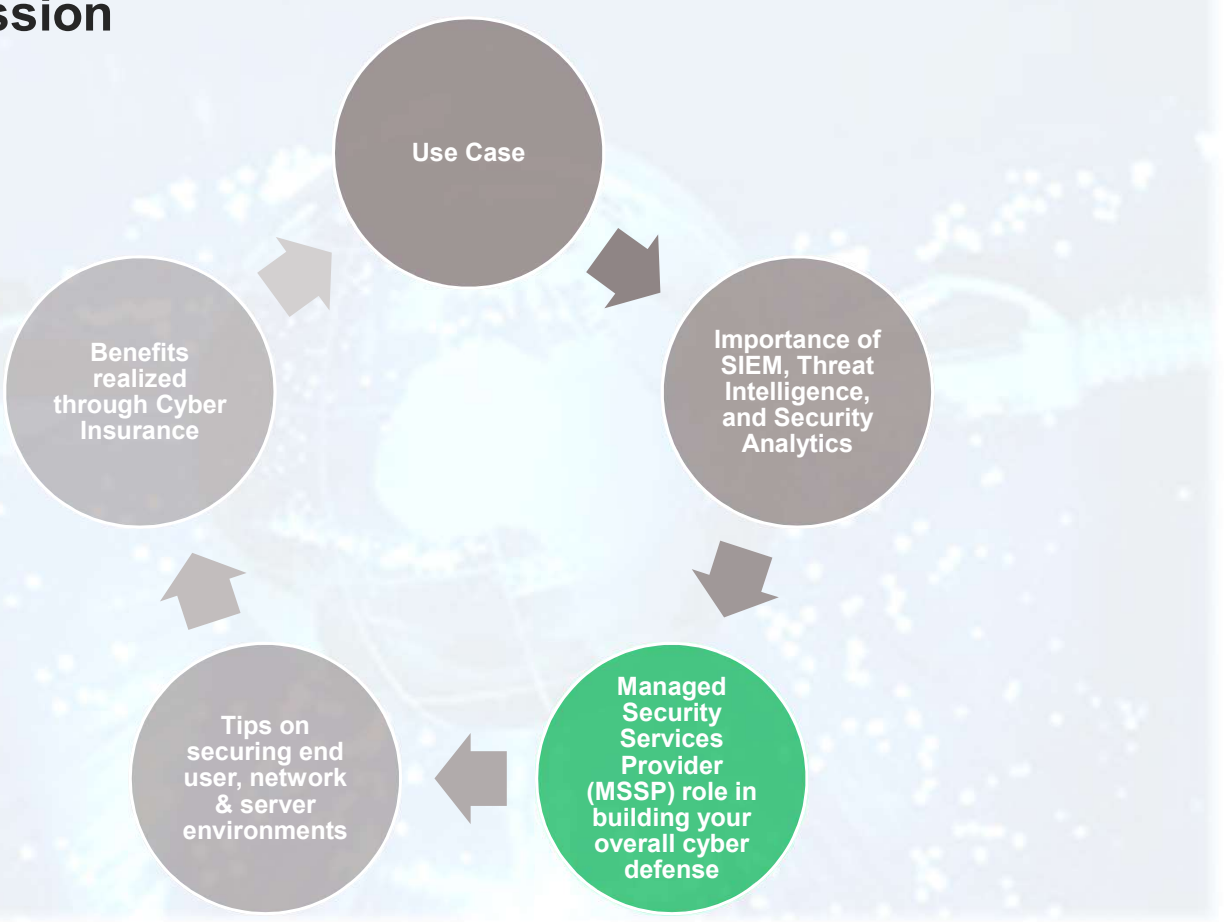
Data enrichment

Data ingested into analytics toolsets is enriched providing further metadata and field tags that can assist in building patterns and trends

Data lake

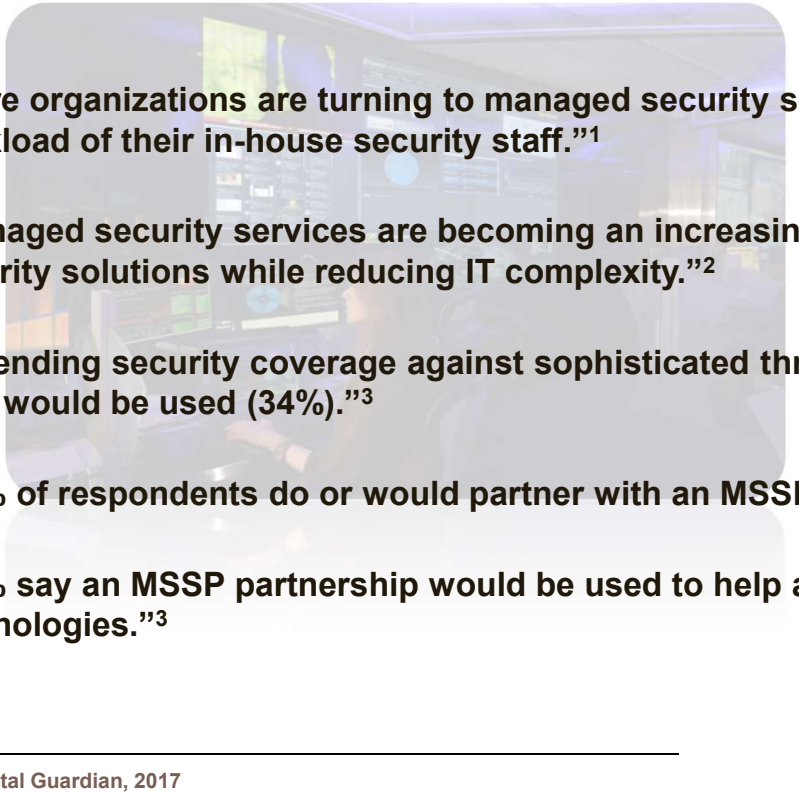
Analytics works off large sets of data; by building your security analytics capability, you are building your enterprise data lake.

Our discussion



CSOC
Diyar United Company
Cyber Security Operations Center

Why Managed Security Services (MSS)?



- **"More organizations are turning to managed security services to gain security expertise and lessen the workload of their in-house security staff."[1]**
- **"Managed security services are becoming an increasingly popular option for increasing the value brought by security solutions while reducing IT complexity."[2]**
- **"Extending security coverage against sophisticated threats is the most popular reason an MSSP partnership is or would be used (34%)."[3]**
- **"31% of respondents do or would partner with an MSSP to help compensate for skills shortages."[3]**
- **"33% say an MSSP partnership would be used to help adopt, deploy and operate hard-to-use security technologies."[3]**

1. Digital Guardian, 2017
2. Digital Guardian, 2015
3. Trustwave, 2017 Security Pressures Report

Why Managed Security Services (MSS)?

In-house continuous 24x7 security monitoring and analysis is very expensive

Customers security teams spend too much time on other day-to-day tasks

The lack of speed and agility when responding to a suspected data breach is the most significant issue facing security teams today

Customers security teams are understaffed

Finding skilled security staff is a challenge

Cyber security may not be your core business, it is for MSSPs. Focus on your business and let MSSPs focus on theirs

CSOC
Diyar United Company
Cyber Security Operations Center

A Managed Security Services Provider (MSSP) role in building your overall cyber defenses

24/7 security analysis, monitoring, alerting and response by a team of **certified experts**

Provide **improved** security posture

Minimize the time to identify any threat or attack by having **dedicated SOC analysts**

Provide access to the **latest security technologies**

Provide access to **security expertise** without staff turnover

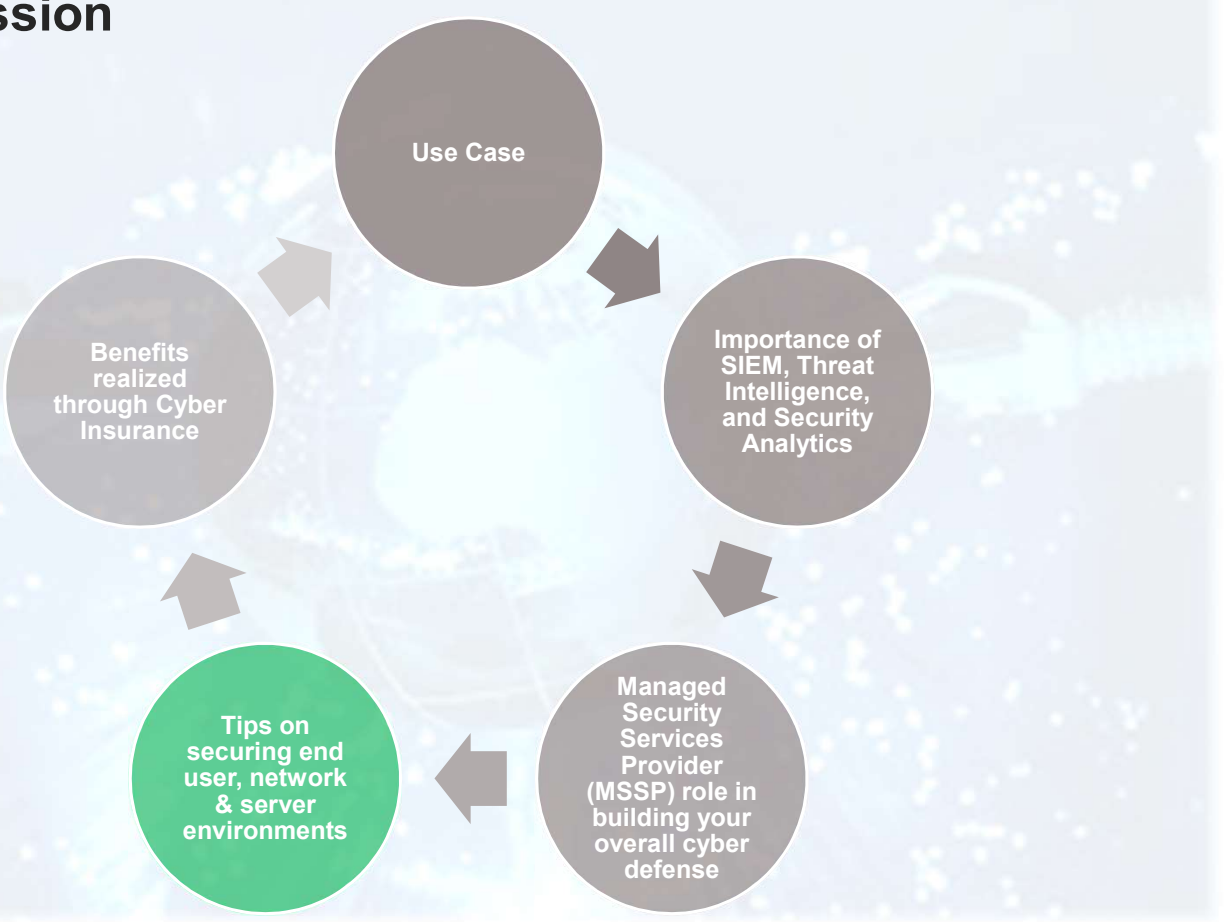
Risk **Mitigation** Strategy

Provide **correlation** with security threats **worldwide** and not only local security devices

Customized threat detection content

CSOC
Diyar United Company
Cyber Security Operations Center

Our discussion



CSOC
Diyar United Company
Cyber Security Operations Center

Tips on securing end user environments

Users need to know about Information security issues that affect their work. They need to understand the threats and risks as well as the methods they can personally use to defend against those threats.

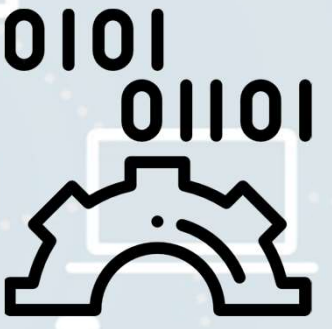
- **Malware**: defending against softwares that are designed to perform malicious activities (viruses, spyware, trojan, worms, ransomware, logic bombs, etc.)
- **Scams**: recognizing scam messages and social engineering attacks
- **Account security**: strong password practices and using appropriate account privilege levels
- **Information/Identity theft**: shredding disposable confidential documents, protecting personal and private information from theft
- **Safe Internet and email usage**: protecting the workplace from unsafe content
- **Physical security**: protecting the physical perimeter is also important

Tips on securing the end point:

I. Lock the BIOS
II. Use hard drive encryption (e.g. BitLocker)
III. Control and monitor configurations through centralized management techniques (e.g. GPO policies)
IV. Keep your endpoints up to date with the latest patches from SW/HW vendors
V. Install protective software (AV, EDR, etc.)
VI. Choose strong passwords (and a password change policy)
VII. Configure auto lock-out (if unattended)
VIII. If privilege access is provided, evaluate the use of softwares not provided by default
IX. Back up on a regular basis
X. Use secure connections where possible (e.g. in-office static IP assignments, signed certificates from a RA for https, etc.)
XI. Protect sensitive data (hide, mask, encrypt)
XII. Raise awareness to use email and the internet safely (if something sounds too good to be true, it usually is not true)

Tips on securing network environments

Networks are the backbone of any computing environment. All data travels through a network as it moves from one point to another. Here are some tips to keep our network environments secure:



I. Segregate the network (as much as possible) and build firewall rules in between the subnets
II. Do not use any default passwords on your devices; update them to customized, complex passwords
III. Ensure access is on a need-to-know / least privilege basis
IV. Centralize access management and perform regular access reviews
V. Ensure all public facing services are located within a DMZ or dedicated subnet with firewall rules that specifically control the ingress and egress traffic flow
VI. Use intrusion detection systems on key gates of your network (perimeter, internal, DMZ, etc.)
VII. Run regular discovery and vulnerability scans on your network
VIII. Monitor and log the environment, monitor your privilege users (network, system and database admins)
IX. Use static IP assignments throughout and build alerts for devices that appear with dynamic IP
X. Ensure segregation of duties, encourage job rotation, especially for your privileged users

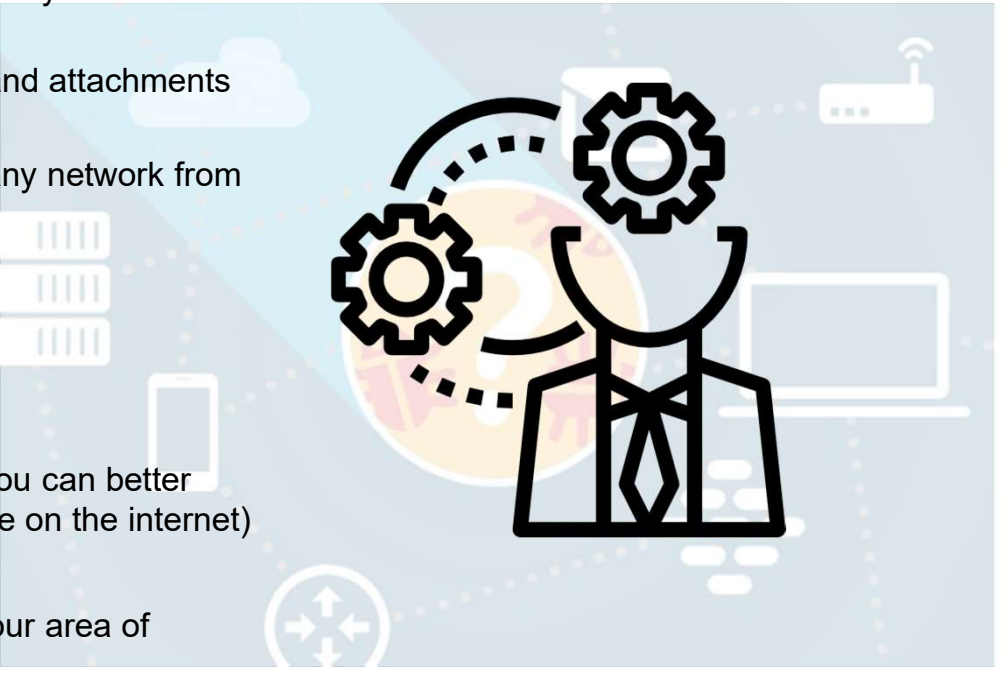
Tips on securing server environments

Here are some tips to keep our server environments secure:

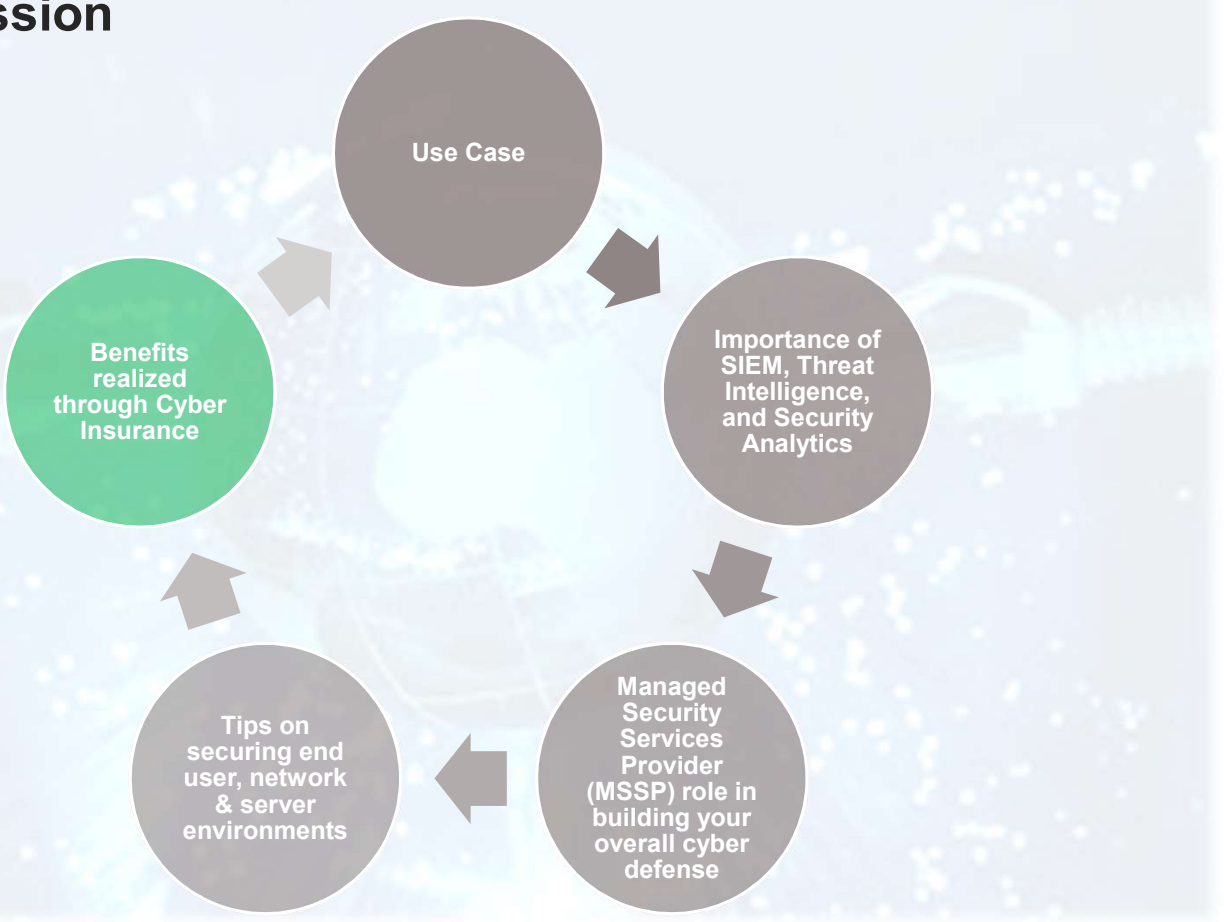
Control	Why
Access Management	I. Lock the BIOS II. Choose strong passwords (and a password change policy) III. Where possible, enable two factor authentication IV. Perform access reviews V. Ensure remote access to management pane (e.g. iDRAC, HPE iLO) is clearly defined and configured
Vulnerability and Patch Management	I. Keep your system up to date and patch vulnerabilities II. Centrally manage configurations (e.g. GPO)
Backup	Ensure an alternate/backup server is available
Features and roles configuration	I. Add what you need, remove what you do not II. Install protective software (AV, EDR, etc.) III. Configure auto lock-out (if unattended)
NTP Configuration	Prevent clock drift
Local Firewall Configuration (if being used)	For critical applications, review the use of local firewall configurations
Remote Access Configuration	Harden remote administration sessions
Harden the server	Protect the OS and other applications, remove unwanted services
Security and system logging	I. Have visibility and know what is happening on your system II. Use centralized log collection mechanisms (e.g. Windows Event Collector), where possible

General Security Awareness

I. Make password management a top priority
II. Automate application and OS locking capabilities on systems that are unattended
III. Trust but “verify” - think twice before clicking links and attachments that you are not expecting
IV. Use VPN connections when accessing your company network from outside
V. Always keep your applications up-to-date
VI. Install protective software (AV, EDR, etc.)
VII. Maintain backups
VIII. Control what you post on social media
IX. Understand what is “social engineering” and how you can better prepare yourself (lots of awareness videos available on the internet)
X. Where possible, enable two factor authentication
XI. Attend to and enforce a culture of security within your area of management/operations



Our discussion



CSOC
Diyar United Company
Cyber Security Operations Center

Cyber Insurance - Benefits

Closing the Gap Between Traditional Coverage and Current Needs

Traditional insurance only covers liability arising out of “tangible” property, for instance the server on which a data is stored, rather than the data itself

Traditional policies also do not explicitly cover first-party breach notification costs.

Cyber insurance is designed to cover these gaps and it provides coverage for

(1) Liability for data breach or loss of data

(2) Remediation costs to respond to breach

(3) Regulatory and legal fines and penalties

Offsetting the Expenses of a Data Breach

Due to their unpredictable nature, data breaches are difficult to budget for.

The size, scope, and complexity of each data breach vary widely.

Typical breach coverage includes forensics investigations, legal fees, data analysis, communication, identity monitoring, identity restoration services, public relations, regulatory fines, legal settlements

Providing Resources for Data Breach Response

Many Insurance providers offer resources to companies facing a data breach. Often, this includes a breach coach, and an attorney who guides the insured through the breach response process and seeks to limit the organization’s legal exposure.

In addition, insurers may be able to provide referrals for forensics, data breach notification, legal and PR, often at a pre-negotiated, discounted rate. The other benefit to using a carrier’s resources is that of experience. A company’s legal counsel, for example, may not have experience in the data breach/privacy sector.

Cyber Insurance - Considerations

Limits on Coverage

Not all policies are the same. What one may cover, another will not. For instance, **some data breaches may be caused by a third-party service provider** as opposed to a data owners (e.g. a cloud service provider).

Limits on Choice

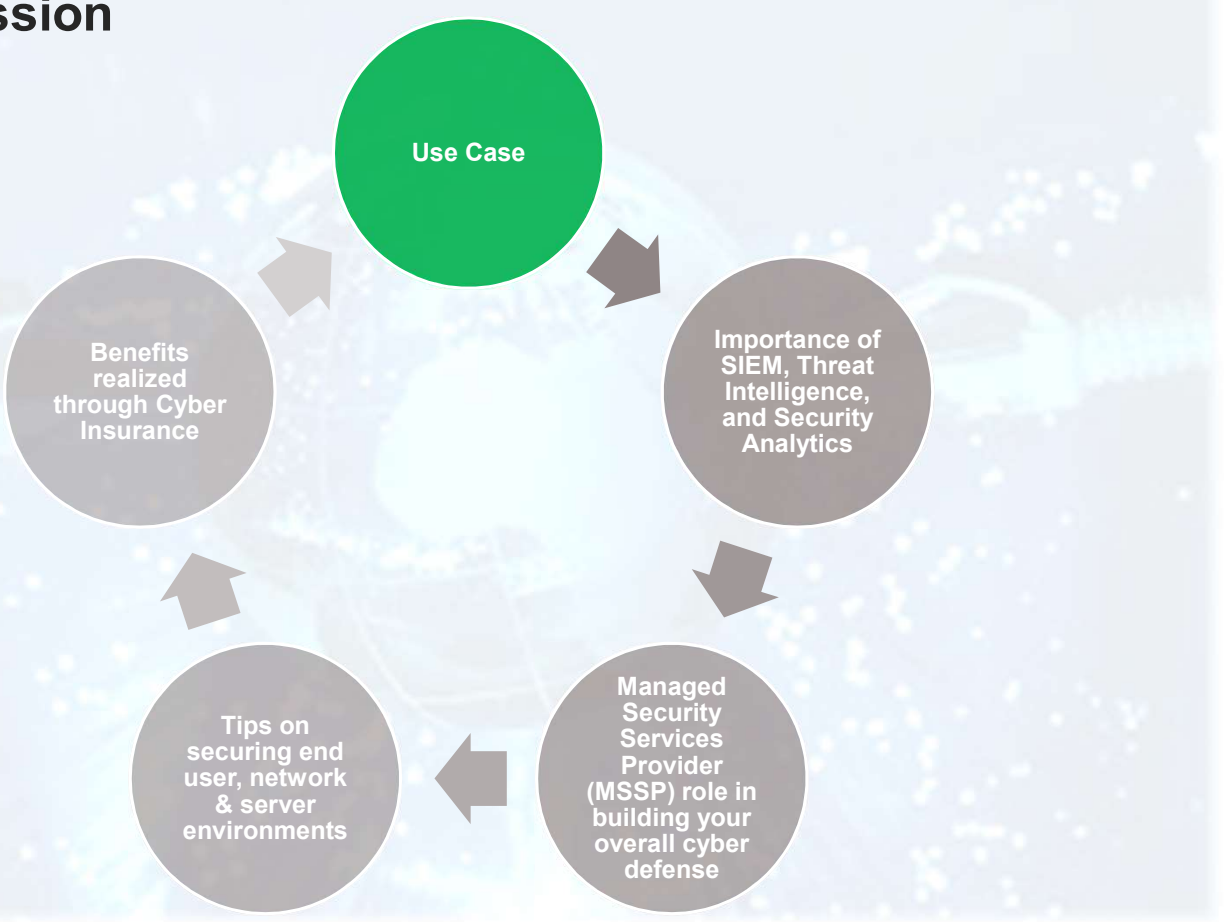
The **terms of a cyber insurance policy** may restrict the way an organization responds to a data breach. For instance, it may cover credit monitoring services for the breach of protected health information, which requires the monitoring of a patient's medical identity, not their credit.

It Cannot Replace the Need for Data Protection

Even with the most comprehensive cyber coverage, companies still have the **responsibility to improve their internal privacy and security measures.**

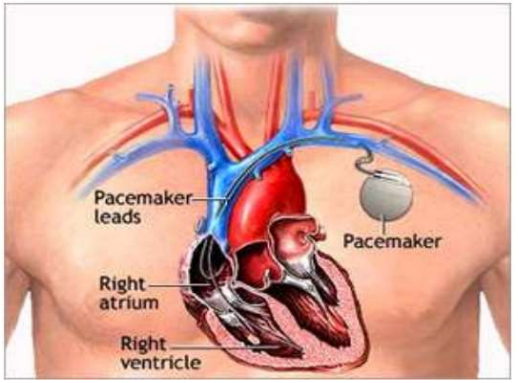
Ultimately, **prevention** is still the best form of insurance against a data breach.

Our discussion



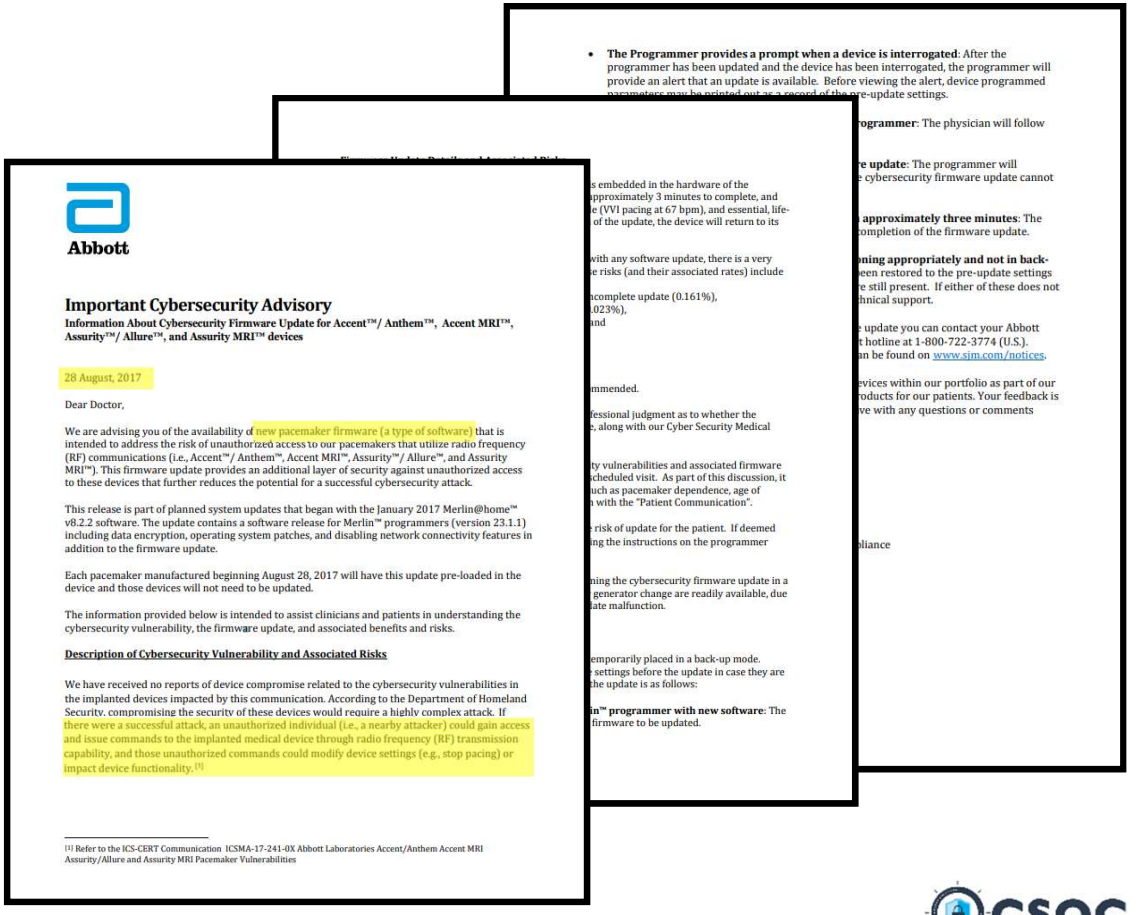
CSOC
Diyar United Company
Cyber Security Operations Center

Case: Vulnerabilities within pacemakers (securing the pacemakers)



A **pacemaker** is a small device that's placed in the chest or abdomen to help **control abnormal heart rhythms.** This device uses electrical pulses to prompt the heart to beat at a normal rate.

- ✓ Keep your endpoints up to date with the latest patches from SW/HW vendors
- ✓ Harden remote administration sessions
- ✓ Use secure connections where possible
- ✓ Protect sensitive data (hide, mask, encrypt)
- ✓ Any others?



Abbott

Important Cybersecurity Advisory

Information About Cybersecurity Firmware Update for Accent™/ Anthem™, Accent MRI™, Assurity™/ Allure™, and Assurity MRI™ devices

28 August, 2017

Dear Doctor,

We are advising you of the availability of new pacemaker firmware (a type of software) that is intended to address the risk of unauthorized access to our pacemakers that utilize radio frequency (RF) communications (i.e., Accent™/ Anthem™, Accent MRI™, Assurity™/ Allure™, and Assurity MRI™). This firmware update provides an additional layer of security against unauthorized access to these devices that further reduces the potential for a successful cybersecurity attack.

This release is part of planned system updates that began with the January 2017 Merlin@home™ v8.2.2 software. The update contains a software release for Merlin™ programmers (version 23.1.1) including data encryption, operating system patches, and disabling network connectivity features in addition to the firmware update.

Each pacemaker manufactured beginning August 28, 2017 will have this update pre-loaded in the device and those devices will not need to be updated.

The information provided below is intended to assist clinicians and patients in understanding the cybersecurity vulnerability, the firmware update, and associated benefits and risks.

Description of Cybersecurity Vulnerability and Associated Risks

We have received no reports of device compromise related to the cybersecurity vulnerabilities in the implanted devices impacted by this communication. According to the Department of Homeland Security, compromising the security of these devices would require a highly complex attack. If there were a successful attack, an unauthorized individual (i.e., a nearby attacker) could gain access and issue commands to the implanted medical device through radio frequency (RF) transmission capability, and those unauthorized commands could modify device settings (e.g., stop pacing) or impact device functionality. [1]

[1] Refer to the ICS-CERT Communication ICSMA-17-241-0X Abbott Laboratories Accent/Anthem Accent MRI Assurity/Allure and Assurity MRI Pacemaker Vulnerabilities

THANK YOU

WWW.DIYARME.COM

KUWAIT

Phone +965 2206 8000
Fax +965 2206 8222
Email sales@diyarme.com

Kuwait City, Khaled Ibn Al-Waleed Street,
Block 3, Business Tower (BT)
PACI Number: 18817027