Re-Thinking Security Operations

Do your security solutions deliver effective coverage against the challenging new threat environment?

Presenters: Mike Lecky and Dave Millier

Date: 21 October 2014

Contents

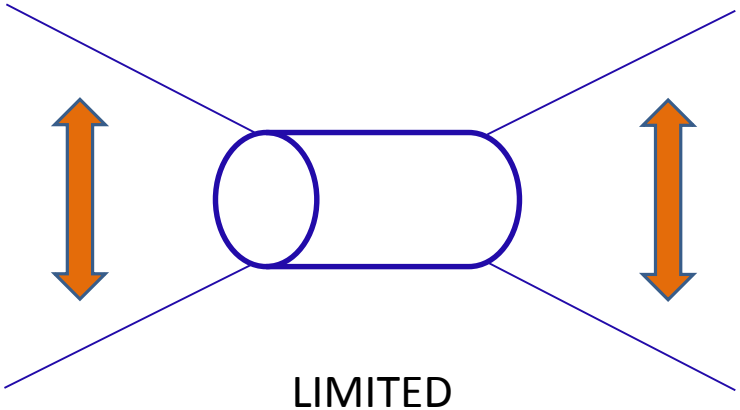
- Compelling Reasons to Re-Think Security Operations
- Grass Roots Approach
- Building Capability, Progressively
- Expanding on Incident Type Use Cases
- Leveraging Use Cases Under Attack
- Benefits and Summary

Compelling Reasons to Re-Think Security Operations

Threat Environment has grown to be *too large a problem* and
Protection Infrastructure *too narrow a solution*
to cover every possible attack circumstance

EXPANDING
Threat Environment

- Increasingly Hostile
- Malware Complexity
- Attack Sophistication



EXPANDING
IT-Enabled Business Solutions

Examples:

- Mobile Apps
- Mobile Devices
- More Sensitive Data

LIMITED
Operational Security Capability

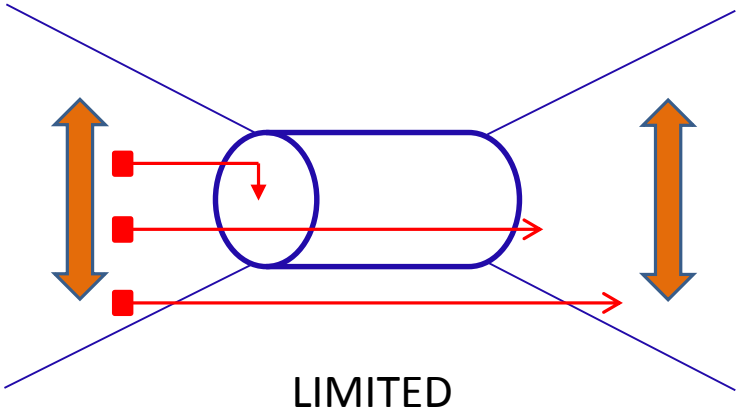
- Complex, Highly Integrative Security Platform
- Long Technology Deployment Timeframes
- Limited Skilled Resources
- Financial Pressures
- Expectation of Simplicity

Compelling Reasons to Re-Think Security Operations

Threat Environment has grown to be *too large a problem* and
Protection Infrastructure *too narrow a solution*
to cover every possible attack circumstance

EXPANDING
Threat Environment

- Increasingly Hostile
- Malware Complexity
- Attack Sophistication



EXPANDING
IT-Enabled Business Solutions

Examples:

- Mobile Apps
- Mobile Devices
- More Sensitive Data

LIMITED
Operational Security Capability

- Complex, Highly Integrative Security Platform
- Long Technology Deployment Timeframes
- Limited Skilled Resources
- Financial Pressures
- Expectation of Simplicity

Grass Roots Approach

Objective:

- To minimize the likelihood of a security incident and when there is one, to effectively and efficiently contain and resolve

Foundational Propositions

1. The amount of impact will depend on the strengths and vulnerabilities of the organization.
2. Systematic methods can be used to lesson likelihood of an incident and reach resolution sooner.
   - **Incident Type Use Cases**
3. The key goal is to build momentum by creating positive cycles that progressively build capability and move the 'readiness bar' forward.
4. Previous incidents are a crucible for improving security readiness, maturing operational practices and building organizational knowledge.
5. A common framework accelerates 'readiness' and aligns the organization through common language and standard practices.
   - **Three Key Questions**

Grass Roots Approach

Three Key Questions

1. What is it?
   - What are the facts about the incident?

2. Why do we care?
   - What impact or potential impact does this have?

3. What should be do?
   - What action should be taken by who to move this through investigation, containment and to resolution?

Building Capability, Progressively

- Use the 3 Keys to build momentum cross-function – before incidents occur
  - Progressively expand to increase security awareness and participation
  - Frame pre-planning discussions and establish Use Case requirements
  - Increase 'organizational readiness' to respond to security events
  - Build detective, preventative and corrective controls

Worksheet Example

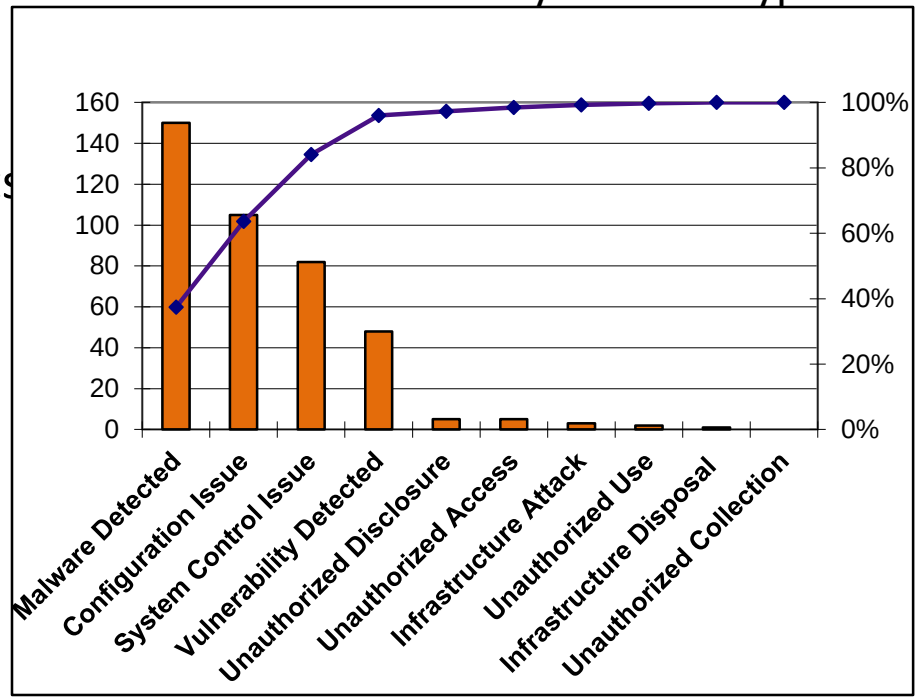
Discussion Topics	3 Key Questions: What is it? (The Facts?)	Why do we care? (The Impact?)	What should we do? (The Action?)
Events -Something that has happened	What information do we need to have logged?	What is the business impact?	What are the timelines we should consider for this event?
Awareness -Something someone needs to know	Are we equipped to identify if this happened and determine false positives?	What expectations need to be set?	Who should be involved? Who are the decision makers?
Response -Something that needs to be done	Should we build a preventative control?	When are key stakeholders (Privacy Officer, Crisis Management) informed?	Should we have trial runs and practice drills?

Building Capability, Progressively

- Systematic Approach – Incident Type Use Cases

- Comprehensive set (NIST)
- Clearly defined
- Streamline recurring incidents (ie botnets)
- Maintainable inventory
- Tools configured to support
- Reportable

Pareto Chart – Incidents by Incident Type



Incident Type Use Case Baseline Categories

Sample Baseline Categories

- Privileged Access Violation
- Unauthorized Access
- Infrastructure Attack
- Unauthorized Disclosure
- Malware Detected
- Configuration Issue
- System Control Issue
- Vulnerability Detected

What is a Use Case?

"A list of steps typically defining interactions between an role (actor) and a system, to achieve a goal" - Wikipedia

- A use case provides clarity for an operator/analyst on the steps required to respond to an event
- A use case can provide detailed information on specific types of events that may be seen by the Operations Team
- A use case streamlines incident response and change management by helping to minimize or eliminate the guesswork about next steps
- A use case, when created properly, ensures there is always a way forward when responding to an event

Sample Use Case #1

New Admin Account Created in Active Directory

- What is it: An account with administrative privileges has been created in Active Directory, the database of users and permissions
- Why do we care: Administrative accounts typically have almost complete unrestricted access to all aspects of a company's system and files
- What should we do about it: Determine if the account creation was approved, if there is a ticket associated with it, proper account creation process has been followed. If the account doesn't have an approval, flag it for disabling, escalate the incident internally and determine if a breach has occurred resulting in the account being created

Sample Use Case #2

Outbound Traffic to known blacklisted destinations

- What is it: Traffic is leaving our network headed to external destinations that are known to participate in malicious activity
- Why do we care: Traffic going to a known bad place on the Internet usually indicates that an internal host has been infected with malware, need to determine the criticality of the internal asset
- What should we do about it: Verify the type of traffic going to the external host is not expected traffic, confirm the criticality of the internal host where the traffic is originating, request that the internal host be taken offline immediately, arrange a forensic analysis of the infected host, inform Operations team to be extra vigilant for any similar traffic existing the corporate network which may indicate an infection or outbreak

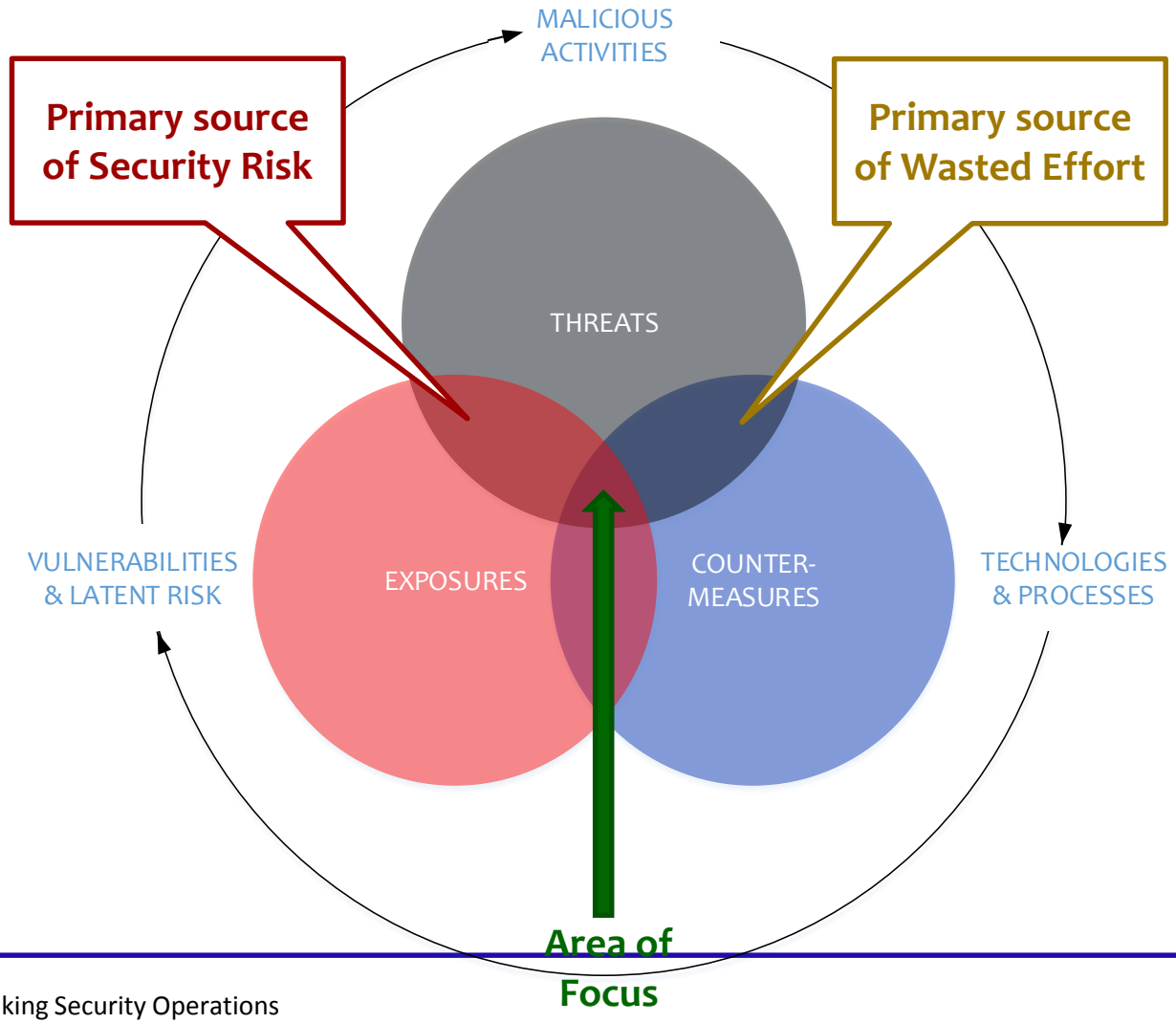
How do Use Cases Help Incident Response?

- Rules can be created with the Use Case # in their title
  - UC17: Multiple failed logins followed by successful login
  - UC23: New Administrator Account Created in Active Directory
- Operations Team can be taught all of the key use cases, what they are, what impact they may have, and what the recommended response should be
- Significantly reduce the amount of time responding to an incident: if two of our three questions are already answered, the responder only has to focus on determining the impact
  - What is it: Use Case already has the details
  - Why do we care: Operator/Analyst focuses on this
  - What should we do: Use Case provides of the details

Other Ways Use Cases Help in Operations

- Significant reduction in training
  - new employees can contribute to incident response almost immediately
  - Properly documented use cases allow the new employee to respond without requiring them to have a complete understanding
  - New employees with good technical skills but no knowledge of operation processes can still contribute right away
- Handle more incidents with the same or potentially less resources
  - Cut the time spent on each incident by 50-70%.
  - Operator spends his/her time on the impact analysis, not on researching details on what the incident is, and once validated has immediate access to the recommended responses and reasons behind same
  - Incident tickets can be pre-populated with Use Case information from a WIKI or internal knowledgebase, instead of having to write all of the information out each time

Context is Key to Effective Use Case Triggers



Building Relevant and Useful Use Cases

- A Use Case ISN'T a rule: rather it's typically two or more rules or business logic combined together to infer or confirm a suspected activity has occurred
- Turn off or significantly tune most out-of-the-box correlation rules/use cases provided by vendors, align them with the Use Case approach
- Use Cases should be meaningful and relevant to the systems you have, the applications you have, and the users and applications that are running on your corporate network
- Many times one Use Case can be used to handle a number of correlated rules from a SIEM
  - UC29: Internal host communicating to a known C&C server: correlation rules could relate to source and destination traffic, an alert from anti-virus, an alert from Malware monitoring, etc.

Case Study: Target Breach

- 110 records exposed
- Confirmed 40 million credit/debit card details
- Encrypted PINs (but not the encryption key)
- 70 million customer records
- Compromised by a phishing email containing malware
- Target wasn't breached directly, breached through one of their 3rd party HVAC contractor

What do we know about the breach?

Timeline through November

- FireEye Threat Prevention Platform purchased and installed in August, 2013
- Certified PCI Compliant in September, 2013
- November 12: First breach of the network through 3rd party compromise
- November 15-28: Attackers successfully install malware on POS systems
- Symantec Anti-Virus identifies and alerts on malware installed on various POS machines
- FireEye malware detection sends out various alerts

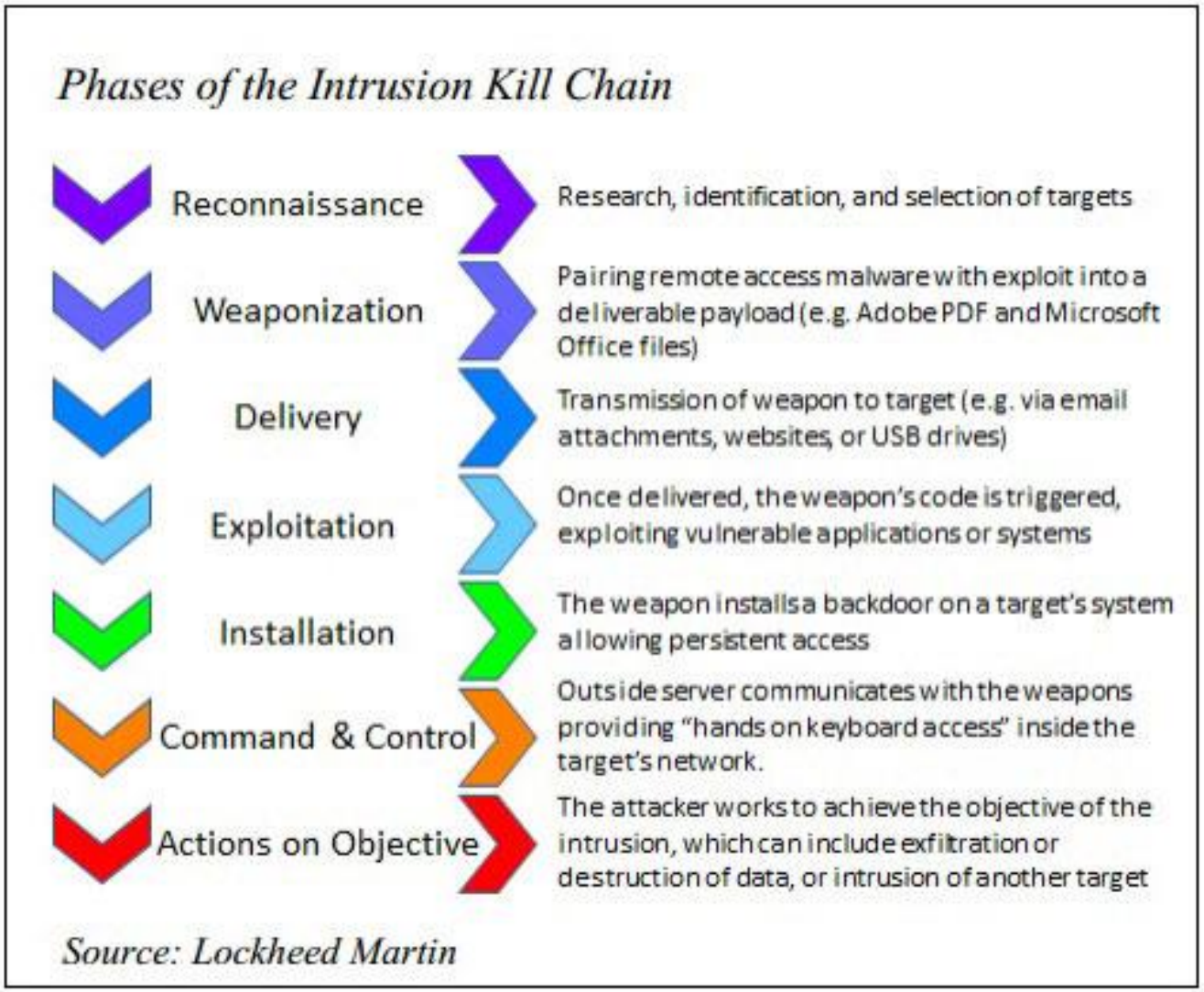
Into December

- December 2: attackers update their malware to export stolen data
- December 2: FireEye once again sends out automated alerts
- December 12: Target is alerted by US Justice Dept. of suspicious activity
- December 15: Target confirms breach and removes most malware from POS systems
- December 18: Target finds malware and removes it from 25 additional hosts
- December 19: Target confirms data breach of credit card information for more than 40 million customers

And January, February, March

- January 10: Target announces information on 70 million customers has also been compromised
- January 13: CEO apologies to customers
- February 4th and 5th: Testifying before various committees
- February 26th: Target reports earnings, including a $61million spend in 4th quarter directly related to the breach
- March 5th: CIO resigns
- March 13th: Bloomberg reveals alerts that Target and Trustwave missed
- Throughout January, February, March: Dozens of lawsuits announced against Target and Trustwave

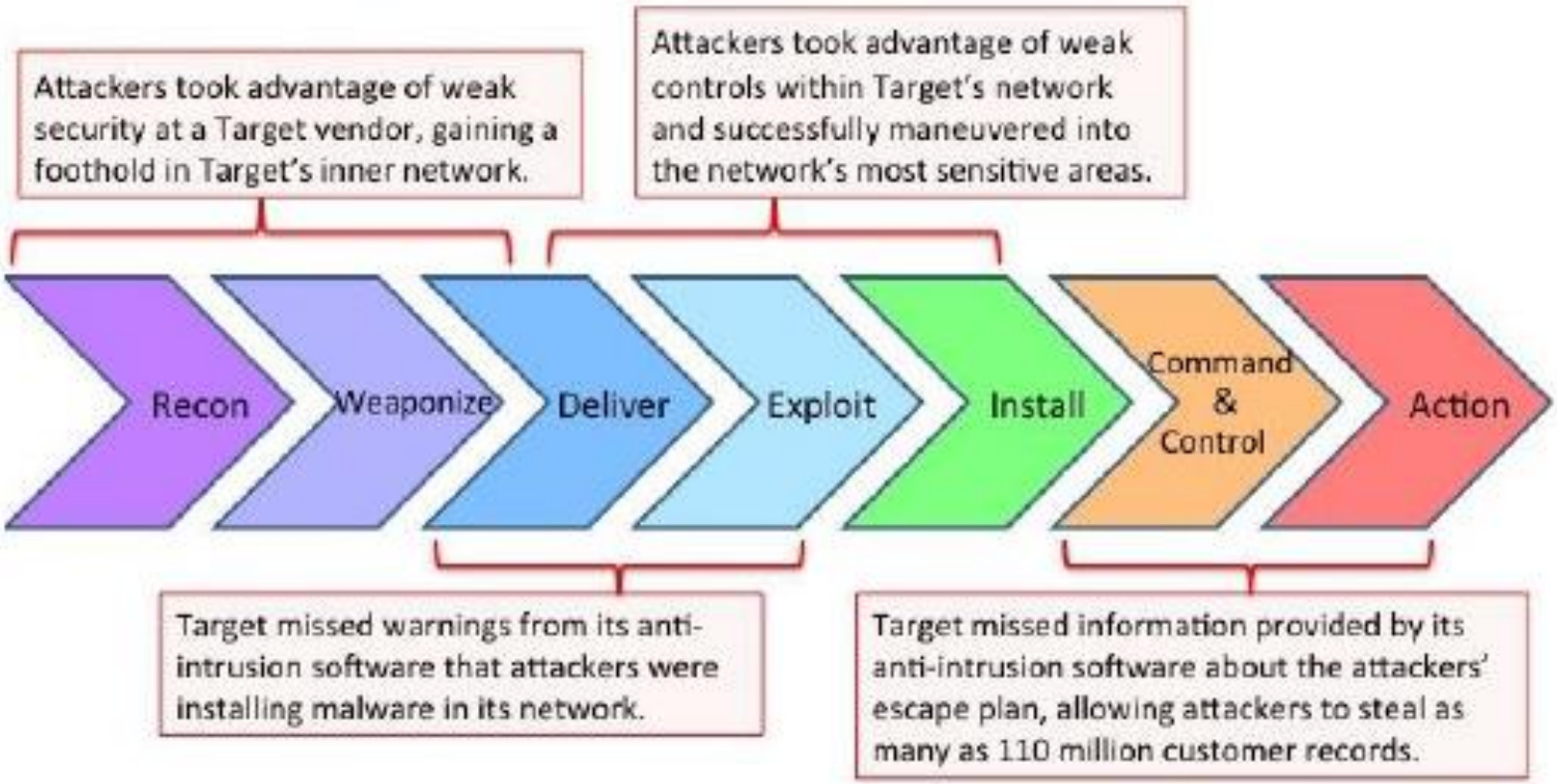
What is the Lockheed Martin Kill Chain?



Kill Chain Analysis of Target Breach

- Reconnaissance – Target keeps a list of main of its vendors and suppliers on its web site
- Weaponization – Phishing email created to target HVAC vendor
- Delivery – emailed to HVAC vendor, successfully executed
- Exploitation – Gained access to network using stolen credentials, elevated privileges, gained access to network where POS systems reside
- Installation – Installed malware on POS machines, installed malware to facilitate exporting data
- Command & Control - Ongoing link established from cardholder network and Internet
- Actions – Attacker exports credit card information, PINs, customer information

Leveraging Use Cases Under Attack



Where could Use Cases have Helped?

- Use Case: Identify Vendor Accounts being accessed from non-standard locations
- Use Case: Identify Vendor Accounts being used after a period of inactivity
- Use Case: Identify Internal Network Probing Attempts
- Use Case: Identify Internal System Access from System Logged in with Vendor Credentials
- Use Case: Identify Recurring Alerts and Escalate Priority
- Use Case: Identify Outgoing Attempts to Transfer Data (large volumes, same source various destinations, etc.)

Use Cases and the Kill Chain

- Leveraging the Kill Chain methodology allows us to identify a tremendous number of potential use cases
- Using the knowledge of our own networks allows us to really customize our incident type use cases to be very meaningful
- Creating Use Cases and identifying where they exist within the Kill Chain allows us to identify how far along a potential attack is and how long it may have existed in our environment
- Aligning Kill Chain Steps with Use Cases and Incident Response allows us to really tailor our responses both from an investigation activities perspective as well as from a real time response perspective

Benefits to Operations

- "Do more with Less"
- Reduce time responding to and resolving incidents, handling changes, etc.
- New employees can be productive much quicker
- Knowledge Transfer amongst the team becomes much easier
- Consistent way to document and explain incidents in your incident management system
- A good Use Case template allows new Use Cases to be quickly created and added to your Use Case Library
- The Use Case document can be provided to other people within your organization to provide them with details when an incident occurs
- Use Cases help to manage risk more effectively, resulting in fewer breaches and faster responses and resolution should one occur

Call to Action

- Review your existing polices and processes, determine where Use Cases could be leveraged to streamline
- Create new processes that allow your team to take advantages of everything Use Cases have to offer
- Hold a brainstorming session with your team with a goal of documenting as many Use Cases as your team can identify. Use existing rules and correlation rules from SIEMs and other security tools to act as a starting point
- Document each Use Case thoroughly, at a minimum make sure each one answers the three important questions
- Train your team and the organization on the Use Cases
- Hold incident response simulations to test and validate the Use Cases

Summary

Incident Type Use Cases

- Use Cases are a systematic method to lesson likelihood of an incident and reach resolution sooner
  - Strengthen the right controls
  - Reduce the right vulnerabilities
- Reduce impact of attacks

Three Key Questions

- Align stakeholders
  - **What is it?**
  - **Why do we care?**
  - **What should we do?**
- Accelerate 'security readiness' prevent and respond