Cyber Threat Response

CISCO SECURITY

Simple Open Automated

cisco Security

www.cisco.com/go/security

Cyber Threat Response

Brought to you by **CISCO SECURITY**

course architects

Moses Hernandez

Ron Taylor

Katherine McNamara

Jamey Heary

William Young

John Columbus

Jeff Fanelli

Joey Muniz

Bobby Acker

Christopher Heffner

writing

Joey Muniz

art

Tariq Hassan

colors

Brian Arthur McGee

letters

Santos Vega

creative direction

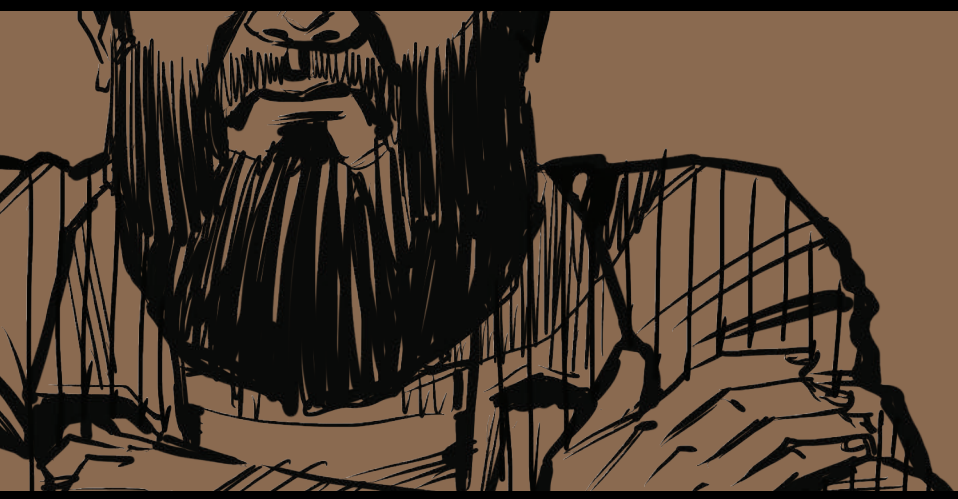
Brian McGee

art direction/design

Santos Vega

editing

Andrew Akers



Insider Threats

Chapter Three

Mr. Brown (alias)

Linked to sales of black market pharmaceutical drugs

Associated with a mafia organization

Street criminal for hire


"LET'S LOOK AT MY NOTES AGAIN.
PERIMETER SECURITY IS NOT 100%.
YOU SHOULD ASSUME YOU WILL EVENTUALLY HAVE YOUR NETWORK COMPROMISED.
Notes
Various users and devices
Perimeter security focused
Possibly a flat network
High dollar data
Skeleton IT staff
Blind to Insider threats
Lack internal monitoring
BREACH TECHNOLOGY IS DESIGNED FOR DETECTING INSIDER THREATS
I CAN GET YOU INTO AN INTERNAL MEDICAL UNIT
USING STOLEN, AUTHORIZED CREDS TO BYPASS PERIMETER DEFENSES.
Mr. Green (alias)
Financial advisor on paper but also involved with money laundering
Known for stolen credentials
Minor drug related arrests
10:37 Mr Black - Perfect. Now Mr Brown can bring me the goods.
10:37 Mr Brown - I'll find the data and send it to your cloud drive.
ONCE INSIDE THE HACKMDS NETWORK
MR. BROWN CAN IDENTIFY AND CONNECT TO OTHER SYSTEMS.
10:37 Mr Black - Use this login to access HackMDs network.

HEY KIDS

There are lots of things to remember about **EXCELLENT** Cyber Threat Response! We know it's a lot to learn, but Cisco has you covered!

SILVER BULLET MYTH

There isn't a silver bullet for providing 100% protection against cyber crime. Sorry... we can't promise that. **NOBODY CAN!**

REDUCE RISK

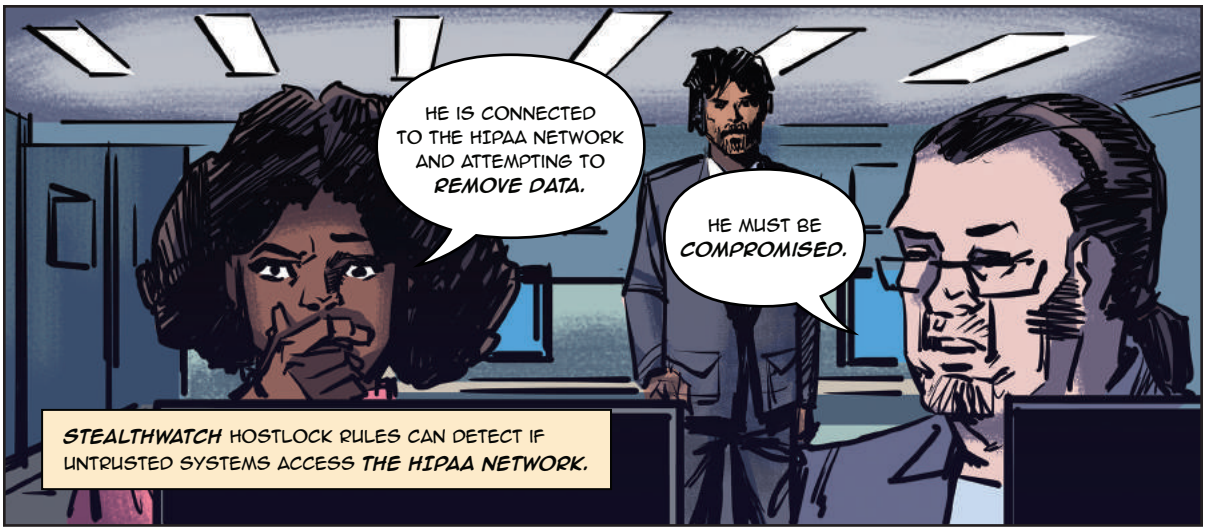
You can, however, learn to reduce the risk of being compromised to an acceptable level using industry best practices for security architecture.

EDUCATE YOURSELF

The Cisco Cyber Threat Response Clinics give you hands-on experience as both **ATTACKER** and **DEFENDER** so you can better understand both sides of the cyber **CAT AND MOUSE** game.

CTR HEROES ACTIVATE!


HACKMDS SECURITY OPS CENTER.
LET'S SEE WHAT ARE THE TOP CONCERNS TO INVESTIGATE TODAY
WHY IS DR. HOWSER LOGGING INTO HIPAA SERVERS LIKE THAT?
STEALTHWATCH SHOWS SECURITY AND NETWORK EVENTS BASED BEHAVIOR AND CONCERN TRIGGERS.
"WAIT, NOW HE'S SCANNING THE NETWORK FTP?
COME TO DADDY.
NETFLOW CAN GIVE ALL COMMON NETWORK DEVICES SECURITY DETECTION CAPABILITIES.
DR. HOWSER'S ACCOUNT HAS NOW SCANNED THE HIPPA NETWORK!


HE IS CONNECTED TO THE HIPAA NETWORK AND ATTEMPTING TO *REMOVE DATA.*
HE MUST BE *COMPROMISED.*
STEALTHWATCH HOSTLOCK RULES CAN DETECT IF UNTRUSTED SYSTEMS ACCESS ***THE HIPAA NETWORK.***


DR. HOWSER'S SYSTEM IS NO LONGER A *THREAT.*
CALL DR. HOWSER.
NOW!
DR. HOWSER, YOU HAVE A *CALL.*
I HAVE NOT TOUCHED A COMPUTER *ALL DAY.*
DON'T WORRY.
WE *QUARANTINED* ALL COMPROMISED SYSTEMS AND *RESET* YOUR LOGIN.
STEALTHWATCH CAN TRIGGER ***CISCO IDENTITY SERVICES ENGINE*** TO QUARANTINE ALL ***CRITICAL THREATS.***

www.xploitz.com

Infect Me Feeling Lucky

x

Don't Do It!

Exploits are everywhere!

An exploit kit is a web server designed to identify and exploit vulnerabilities in client machines. The goal is to deliver something malicious such as a backdoor or ransomware.

Exploit kits can be rented online making it easy for non-technical attackers to deliver technical attacks without understanding the details of how the attack works.

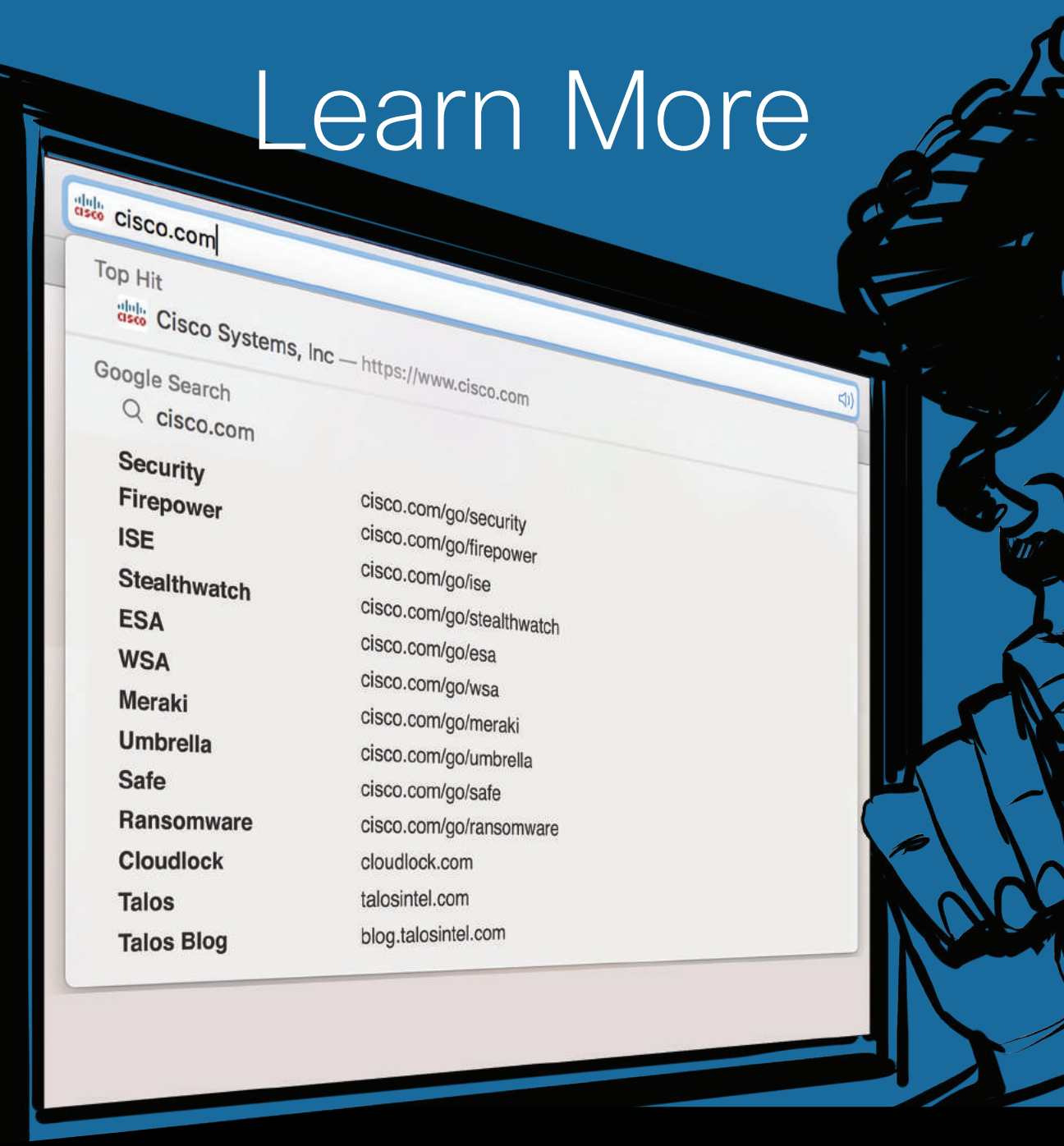
Coming Soon 2 ur CPU

Ransomware

Never stop the incident response at removing the infection, or you may experience it AGAIN!!

Identifying ransomware means an attacker was able to breach your network and deliver malicious software. **Best practice is to identify and remediate infected machines, harden the network against the attack method used, and blacklist any sources linked to the original attack!**

Learn More



We hope you enjoyed the Cisco Cyber Threat Response Clinic!

Make sure to come back and complete any modules you didn't have a chance to work on and check back for more future modules!

Cisco Security

Product Suite

Firepower
URL, IPS, and Breach security

Cisco Umbrella
DNS Security and forensics

ESA
Email security for cloud and on-prem

ISE
Access control and security policy management

Meraki
Cloud managed security, network and collaboration

AMP
Advanced breach detection for endpoint and network

VPN
Encrypted communication

Stealthwatch
Netflow anomaly monitoring and breach detection

Cisco Cloudlock
Cloud application security

Threatgrid
Threat analytics, detection and prevention

Talos
Security research and threat intelligence

WSA
Secure proxy, content control and security

Physical · Virtual · Cloud