Cyber Threat Response

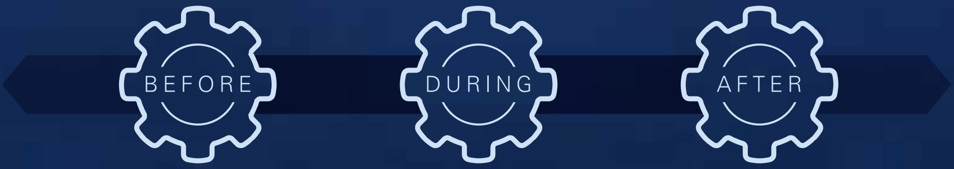
CISCO SECURITY

Cisco
BDA Strategy

Defending real world cyber threats requires a layered approach as no single defense tactic is 100% effective. Attacks typically involve multiple steps known as “The Kill Chain”. Your goal is to prevent the attack as early in the kill chain as possible.

At Cisco, we call our recommended layered approach for security the **Before**, **During** and **After** defense design.

Appliance – Virtual – Cloud



BEFORE

DURING

AFTER

NGFW/UTM

Firewall/VPN

Secure Access + Identity Services Engine

NGIPS/Anti-Virus

Web Security

Email Security

Breach Detection

Behavior Analysis

File Analytics

Visibility, Intelligence and Automation

Watch for how each security technology is covered within the Cisco BDA blueprint.

CTR

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

Smash and Grab

Chapter One

EVENING. UNKNOWN LOCATION
"I SEE YOUR HACKMDS.COM SERVERS ARE ACCESSIBLE FROM THE OUTSIDE.
"EVERYBODY HAS VULNERABILITIES.
"LET'S LOOK AT MY NOTES ON THIS TARGET."
HMM
THIS WILL BE TOO EASY.

Notes

Lacks DNS and reputation security

Standard DMZ

Skeleton IT staff

Poor patch management

Weak security defenses

Vulnerable to web attacks

Poor event monitoring

Mr. Black (alias)

Laid-off after 25 years of employment

Goal is to obtain 30 million dollars using any means available

No criminal records

No social media, false records, limited digital footprint

Proficient technologist

LATER OVER A SECURE IRC CHANNEL
THIS IS MY CHANCE AT THE BIG LEAGUE.
GOOD THING THEY ARE A HOSPITAL BECAUSE AFTER MY ATTACK ...
THERE WILL BE BODIES ...
DINNER!
MOM I'M HACKING!
SPACE INVADERS

```
07:57 Mr Black - Hit the servers without alarming the staff.
07:57 -:- The goal is scan any system online for known vulnerabilities
07:58 -:- And exploit any vulnerability for access to the HackMDs Network.
07:59 -:- Using the compromised system, we will setup a hidden tunnel to exfiltrate any data we find!
```

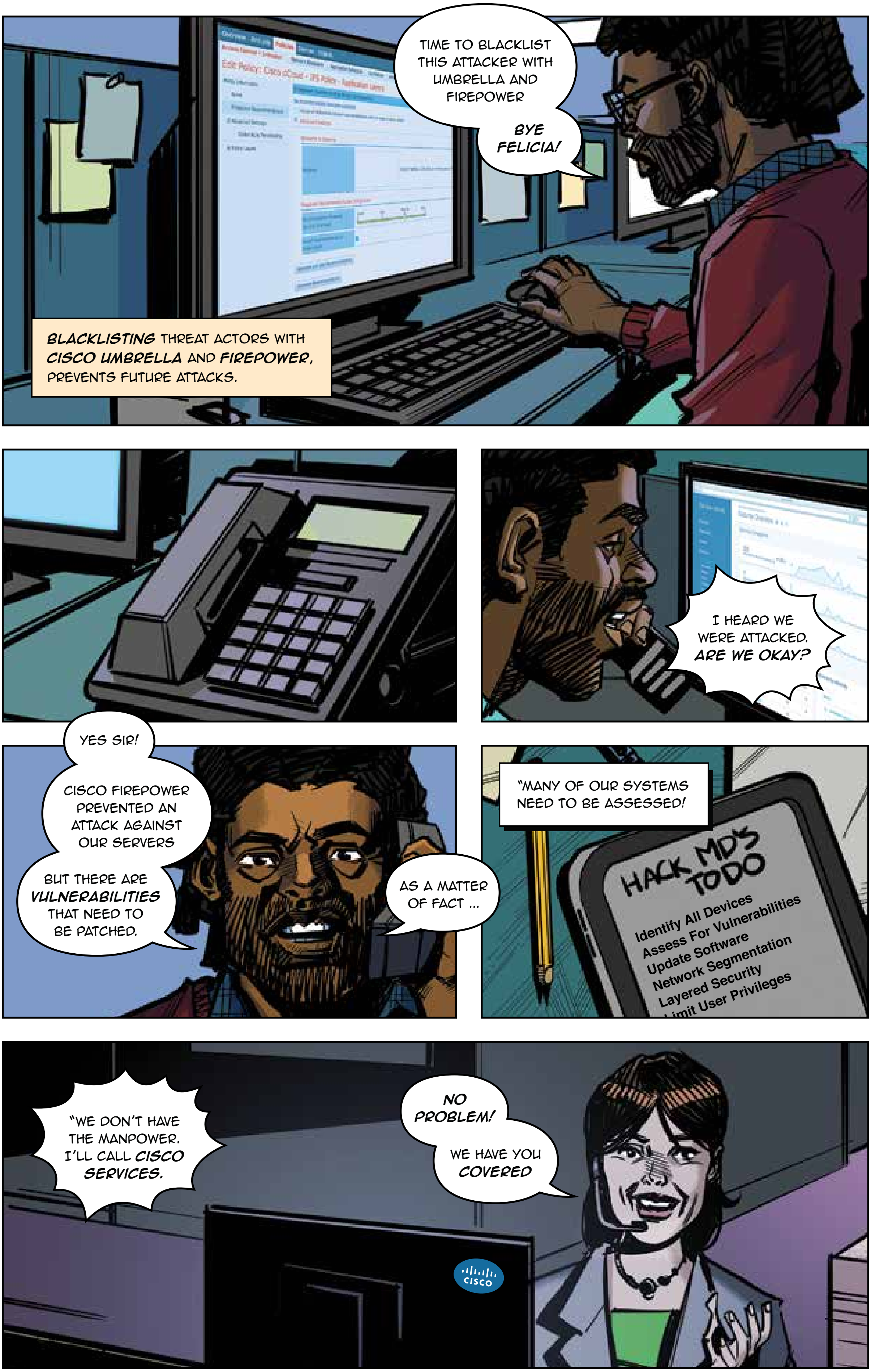
Mr. Orange (alias)

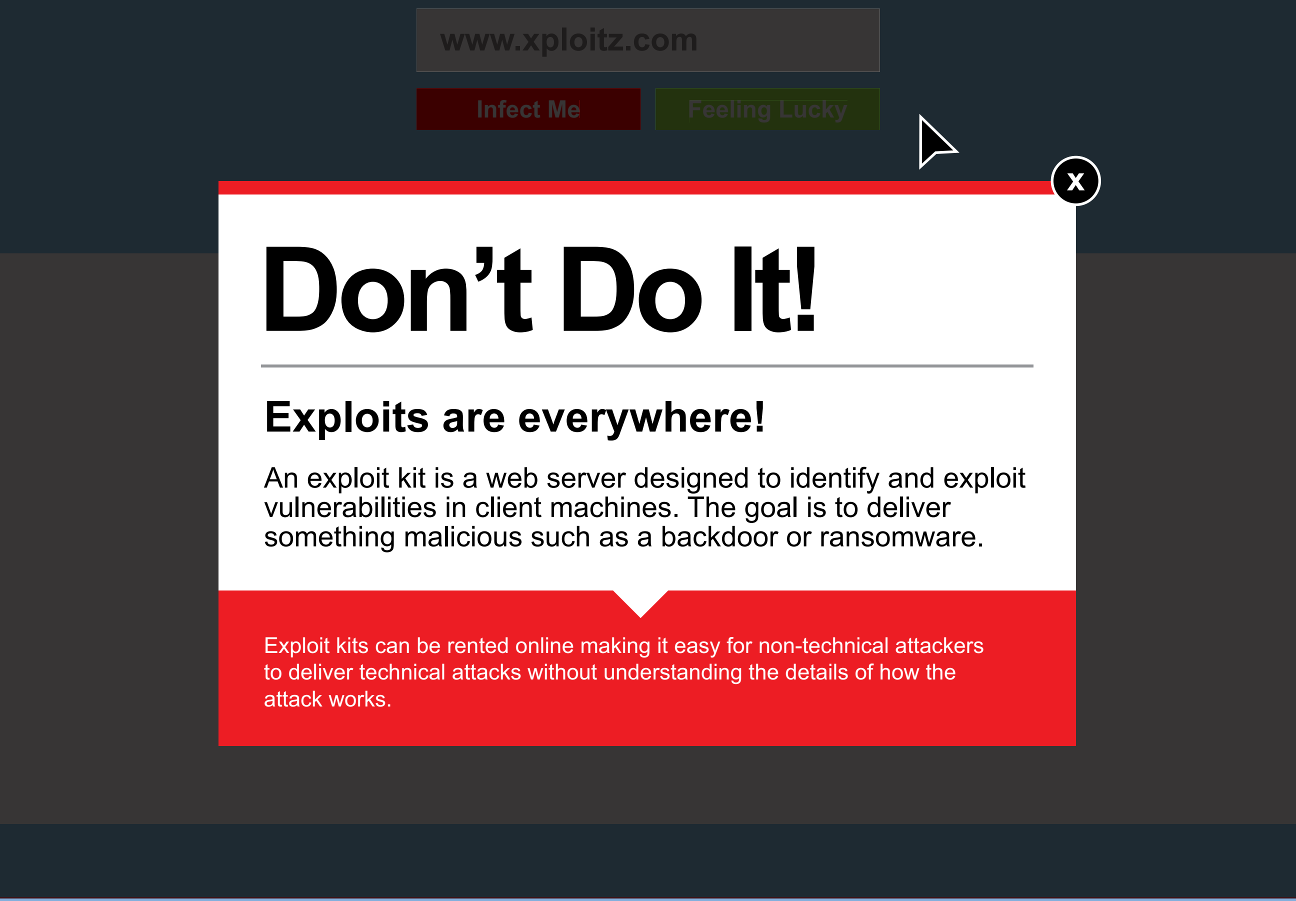
Known as the "Loud Jerk"

Day job unknown but has been dabbling in scripted cyber crime

Actively looking to prove himself as an elite hacker

HACKMDS SECURITY OPS CENTER
FIREPOWER GROUPS VARIOUS ALERTS AS A SECURITY INCIDENT.
OUR SERVERS ARE BEING HIT BY SOMETHING
WHAT ARE THESE ALARMS?
IT LOOKS LIKE SOMEBODY IS TRYING TO EXPLOIT OUR SERVERS.
GOOD THING OUR IPS IS TUNED FOR OUR ENVIRONMENT.
ANY HIGH RISK INCIDENT WILL INFORM HACKMDS.
FIREPOWER CAN AUTO-TUNE THE IPS TO ADAPT TO NEW VULNERABILITIES WITHIN THE NETWORK.


TIME TO BLACKLIST THIS ATTACKER WITH UMBRELLA AND FIREPOWER
BYE FELICIA!
BLACKLISTING THREAT ACTORS WITH CISCO UMBRELLA AND FIREPOWER, PREVENTS FUTURE ATTACKS.
I HEARD WE WERE ATTACKED. ARE WE OKAY?
YES SIR!
CISCO FIREPOWER PREVENTED AN ATTACK AGAINST OUR SERVERS
BUT THERE ARE VULNERABILITIES THAT NEED TO BE PATCHED.
AS A MATTER OF FACT ...
"MANY OF OUR SYSTEMS NEED TO BE ASSESSED!
HACK MD'S TODO
Identify All Devices
Assess For Vulnerabilities
Update Software
Network Segmentation
Layered Security
Limit User Privileges
"WE DON'T HAVE THE MANPOWER. I'LL CALL CISCO SERVICES.
NO PROBLEM!
WE HAVE YOU COVERED
CISCO



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

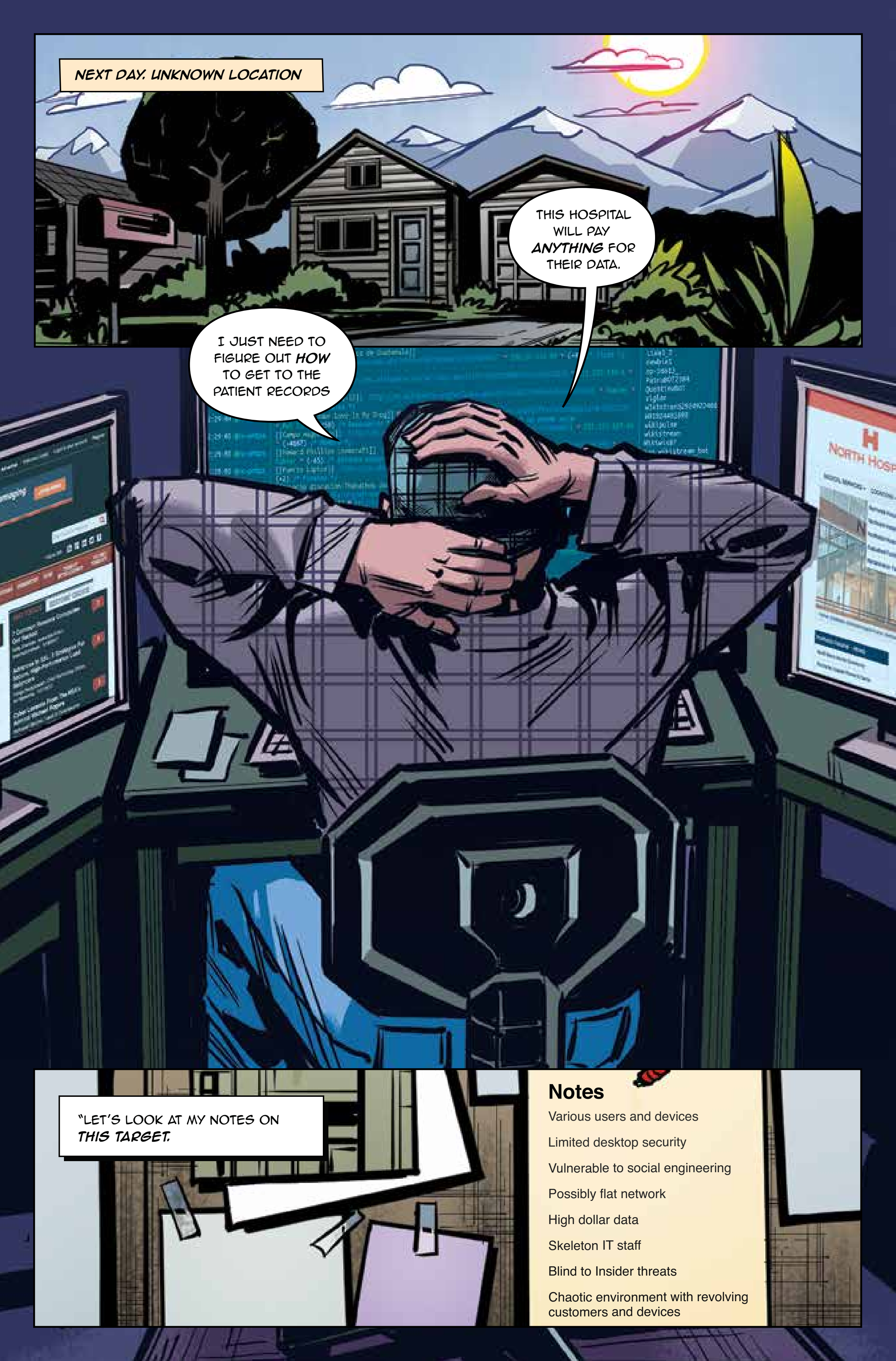
Ransomware

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!**

Ransomware

Chapter Two


NEXT DAY. UNKNOWN LOCATION
THIS HOSPITAL WILL PAY *ANYTHING* FOR THEIR DATA.
I JUST NEED TO FIGURE OUT *HOW* TO GET TO THE PATIENT RECORDS
NORTH HOSP
“LET’S LOOK AT MY NOTES ON *THIS TARGET.*

Notes

Various users and devices

Limited desktop security

Vulnerable to social engineering

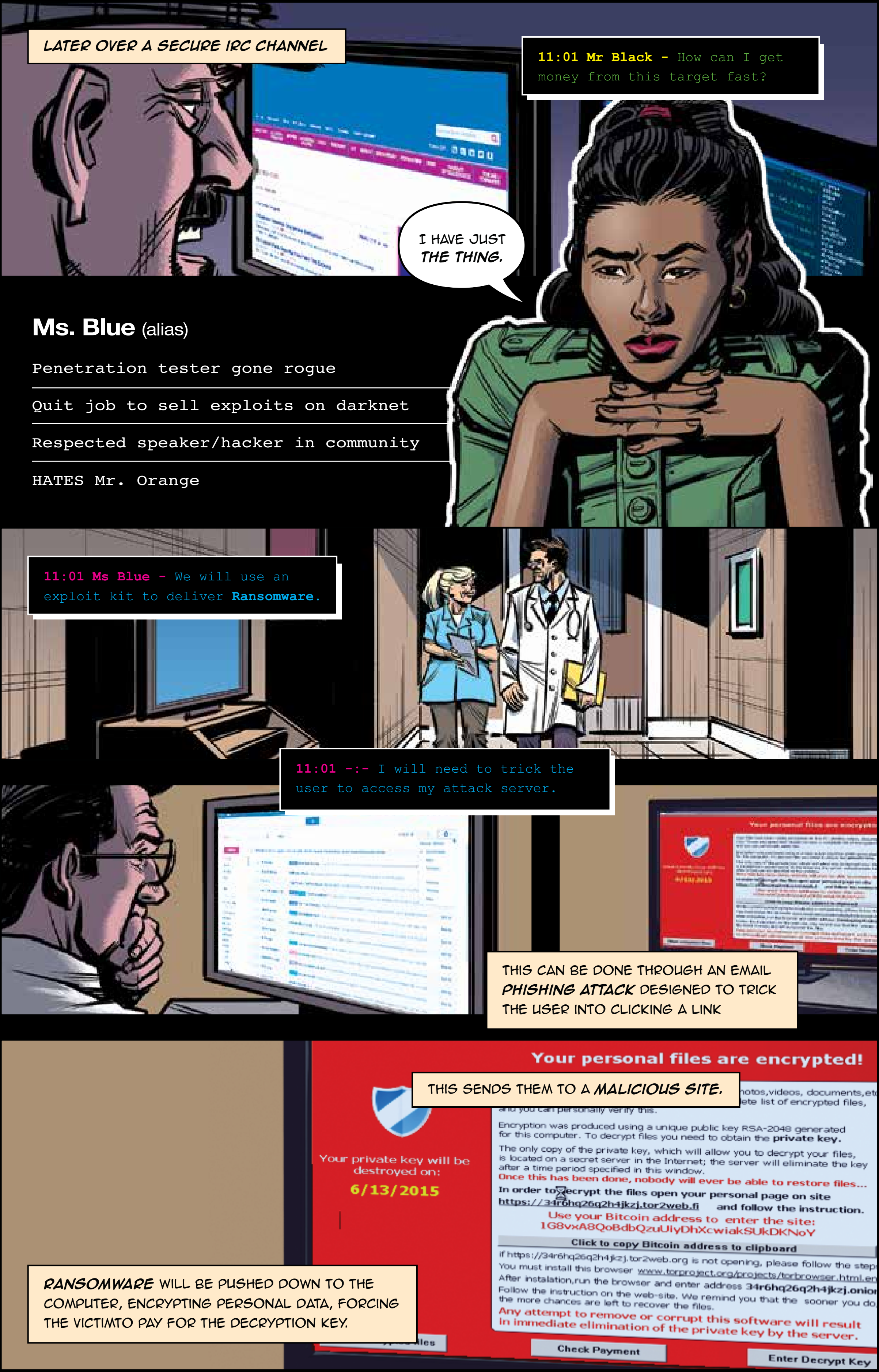
Possibly flat network

High dollar data

Skeleton IT staff

Blind to Insider threats

Chaotic environment with revolving customers and devices


LATER OVER A SECURE IRC CHANNEL
I HAVE JUST *THE THING.*

11:01 **Mr Black** - How can I get money from this target fast?

Ms. Blue (alias)

Penetration tester gone rogue

Quit job to sell exploits on darknet

Respected speaker/hacker in community

HATES Mr. Orange

11:01 **Ms Blue** - We will use an exploit kit to deliver **Ransomware**.

11:01 -:- I will need to trick the user to access my attack server.

THIS CAN BE DONE THROUGH AN EMAIL *PHISHING ATTACK* DESIGNED TO TRICK THE USER INTO CLICKING A LINK
THIS SENDS THEM TO A *MALICIOUS SITE.*

Your personal files are encrypted!

Your private key will be destroyed on:

6/13/2015

hotos,videos, documents,et
ete list of encrypted files,
and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.

Once this has been done, nobody will ever be able to restore files...

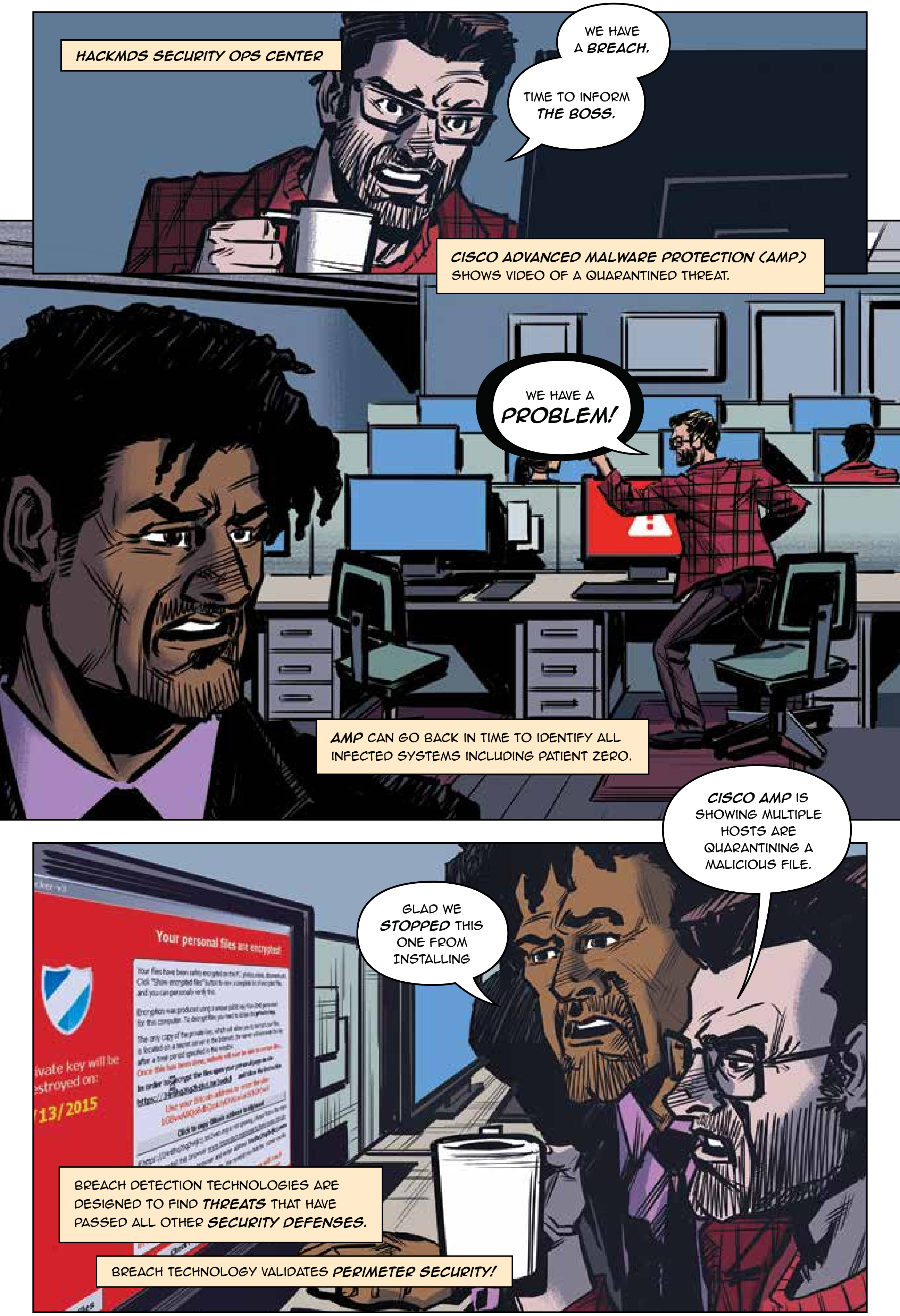
In order to decrypt the files open your personal page on site https://34r6hq26q2h4jkzj.tor2web.fi and follow the instruction.

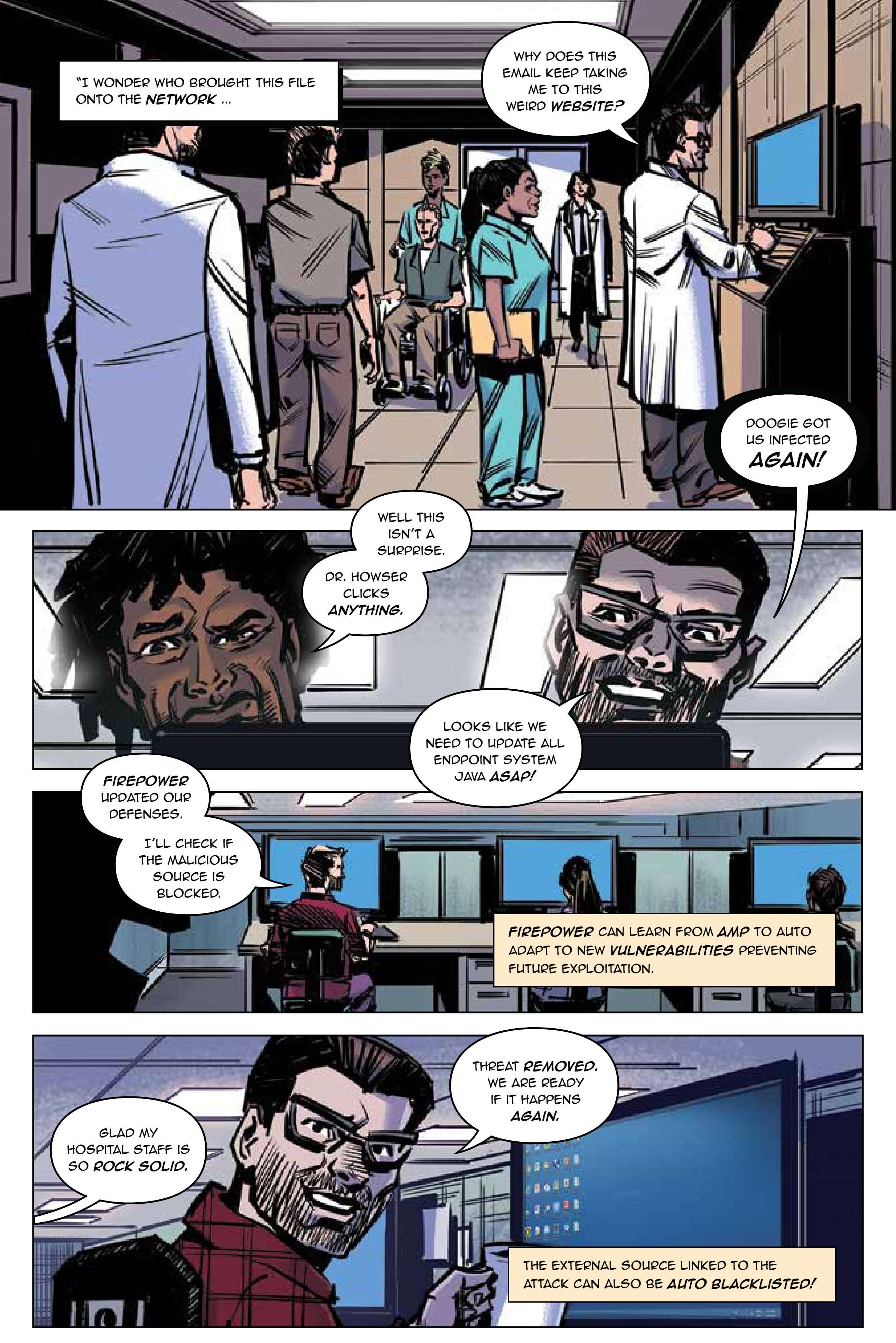
Use your Bitcoin address to enter the site:
1G8vxA8QoBdbQzuUlyDhXcwiakSUkDKNoY

If https://34r6hq26q2h4jkzj.tor2web.org is not opening, please follow the step
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address **34r6hq26q2h4jkzj.onion**
Follow the instruction on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.

Click to copy Bitcoin address to clipboard
Check Payment
Enter Decrypt Key
iles
RANSOMWARE WILL BE PUSHED DOWN TO THE COMPUTER, ENCRYPTING PERSONAL DATA, FORCING THE VICTIMTO PAY FOR THE DECRYPTION KEY.


HACKMDS SECURITY OPS CENTER
WE HAVE A BREACH.
TIME TO INFORM THE BOSS.
CISCO ADVANCED MALWARE PROTECTION (AMP) SHOWS VIDEO OF A QUARANTINED THREAT.
WE HAVE A PROBLEM!
AMP CAN GO BACK IN TIME TO IDENTIFY ALL INFECTED SYSTEMS INCLUDING PATIENT ZERO.
CISCO AMP IS SHOWING MULTIPLE HOSTS ARE QUARANTINING A MALICIOUS FILE.
GLAD WE STOPPED THIS ONE FROM INSTALLING
Your personal files are encrypted!
rivate key will be
estroyed on:
/13/2015
BREACH DETECTION TECHNOLOGIES ARE DESIGNED TO FIND THREATS THAT HAVE PASSED ALL OTHER SECURITY DEFENSES.
BREACH TECHNOLOGY VALIDATES PERIMETER SECURITY!


"I WONDER WHO BROUGHT THIS FILE ONTO THE NETWORK ...
WHY DOES THIS EMAIL KEEP TAKING ME TO THIS WEIRD WEBSITE?
DOOGIE GOT US INFECTED AGAIN!
WELL THIS ISN'T A SURPRISE.
DR. HOWSER CLICKS ANYTHING.
LOOKS LIKE WE NEED TO UPDATE ALL ENDPOINT SYSTEM JAVA ASAP!
FIREPOWER UPDATED OUR DEFENSES.
I'LL CHECK IF THE MALICIOUS SOURCE IS BLOCKED.
FIREPOWER CAN LEARN FROM AMP TO AUTO ADAPT TO NEW VULNERABILITIES PREVENTING FUTURE EXPLOITATION.
THREAT REMOVED. WE ARE READY IF IT HAPPENS AGAIN.
GLAD MY HOSPITAL STAFF IS SO ROCK SOLID.
THE EXTERNAL SOURCE LINKED TO THE ATTACK CAN ALSO BE AUTO BLACKLISTED!

TARGET RE:SEARCH

RECONNAISSANCE*

The first step in a cyber attack. This is where you learn as much as possible about the target. The more you know, the more likely you will find the quickest and most effective attack strategy.

VULNERABILITIES*

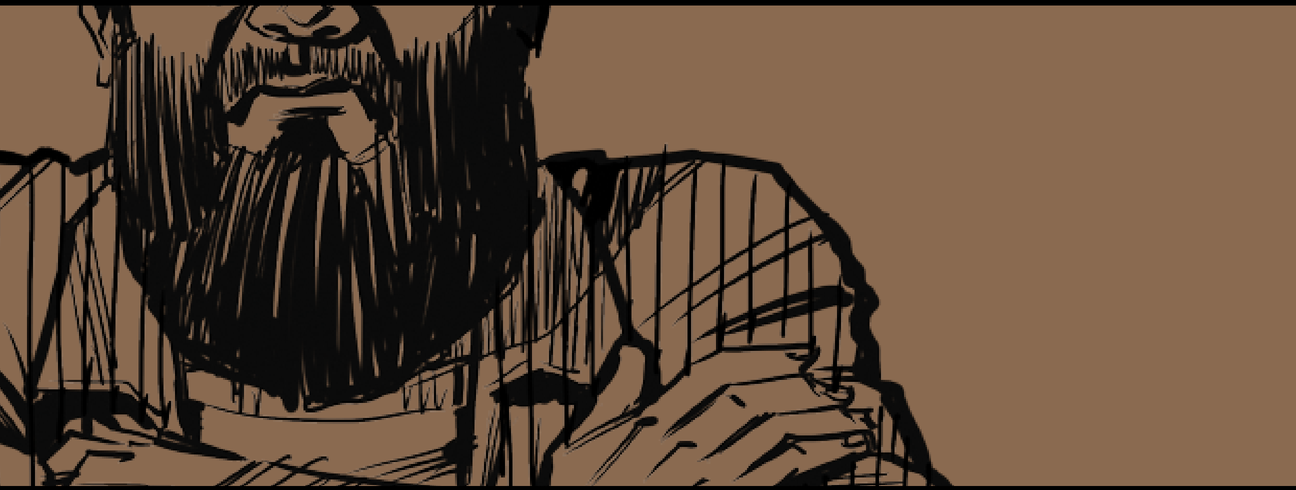
Weakness in a system that can be exploited. This could be a configuration error, missing patch, flaw in design or many other factors happening at any moment.

Security tools such as anti-virus and IPS look for attacks against vulnerabilities using signatures of known exploitation.

EXPLOITS*

Abusing a vulnerability to achieve an outcome. Result could be planting a Remote Access Tool (RAT), delivering Ransomware, Crashing the system, etc.

*Recon finds Vulnerabilities that can be Exploited



Insider Threats

Chapter Three

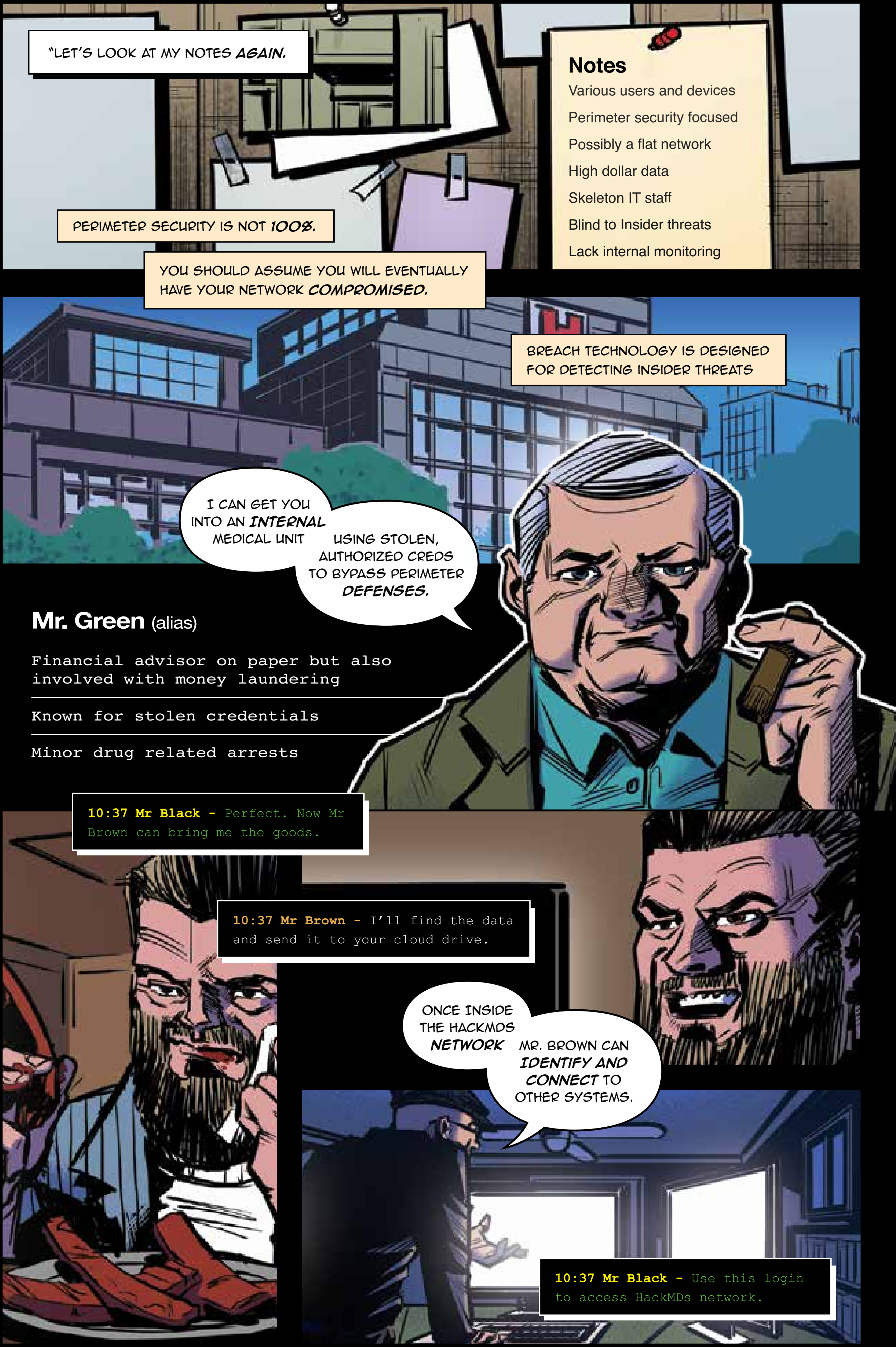
LATER
"MANY DARKNET SOURCES SELL **STOLEN CREDENTIALS.**
I CAN ***BUY*** MY WAY INTO THE ***NETWORK.***
LET'S SEE IF MR. GREEN IS ***AVAILABLE.***
"I KNOW SOMEBODY THAT CAN GET ME INSIDE THE ***HACKMDS NETWORK.***
MR. BROWN CAN THEN ***COLLECT*** MY DATA ONCE I GET HIM ***INSIDE.***

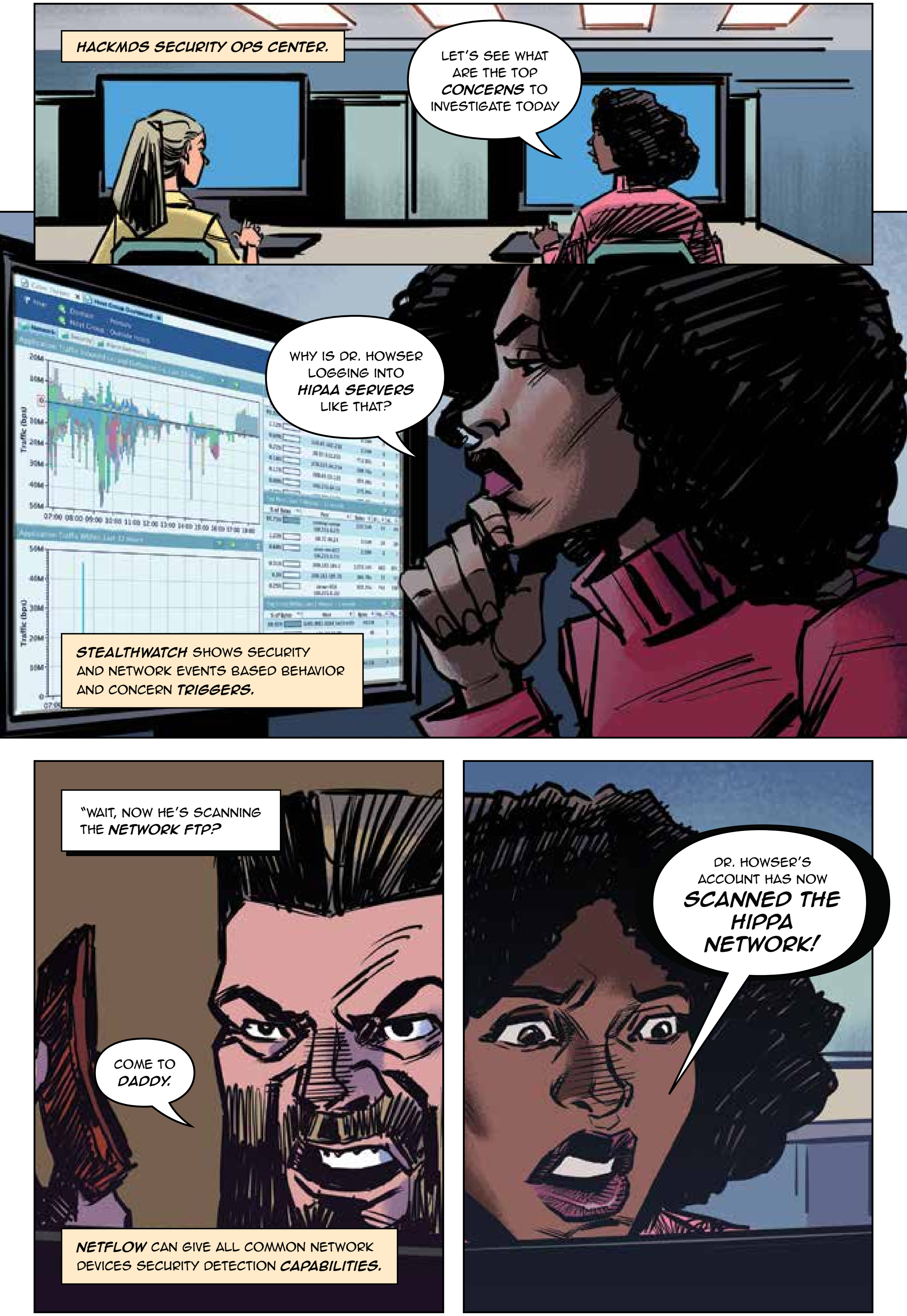
Mr. Brown (alias)

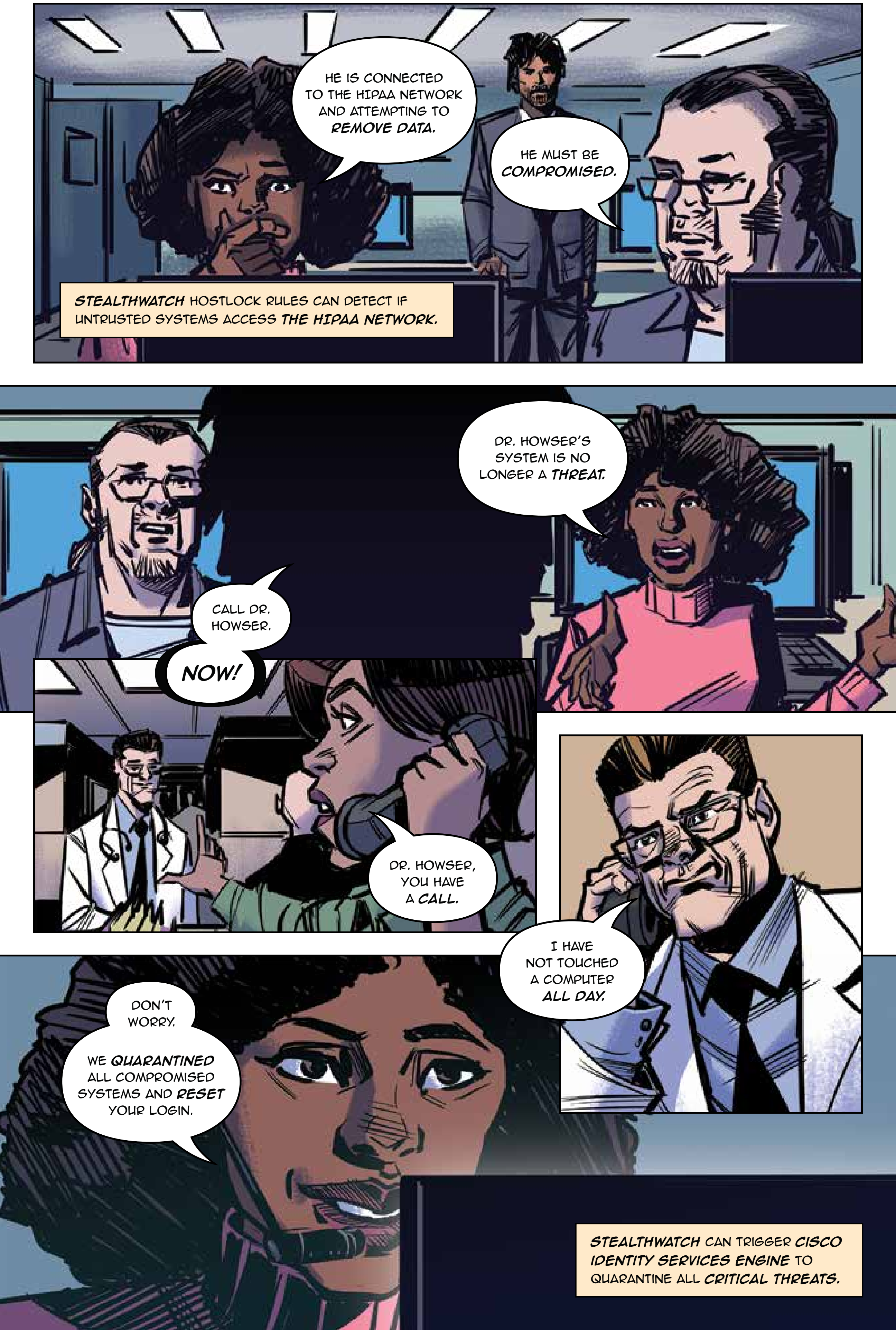
Linked to sales of black market pharmaceutical drugs

Associated with a mafia organization

Street criminal for hire


"LET'S LOOK AT MY NOTES *AGAIN.*
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
PERIMETER SECURITY IS NOT *100%.*
YOU SHOULD ASSUME YOU WILL EVENTUALLY HAVE YOUR NETWORK *COMPROMISED.*
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.


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.***

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

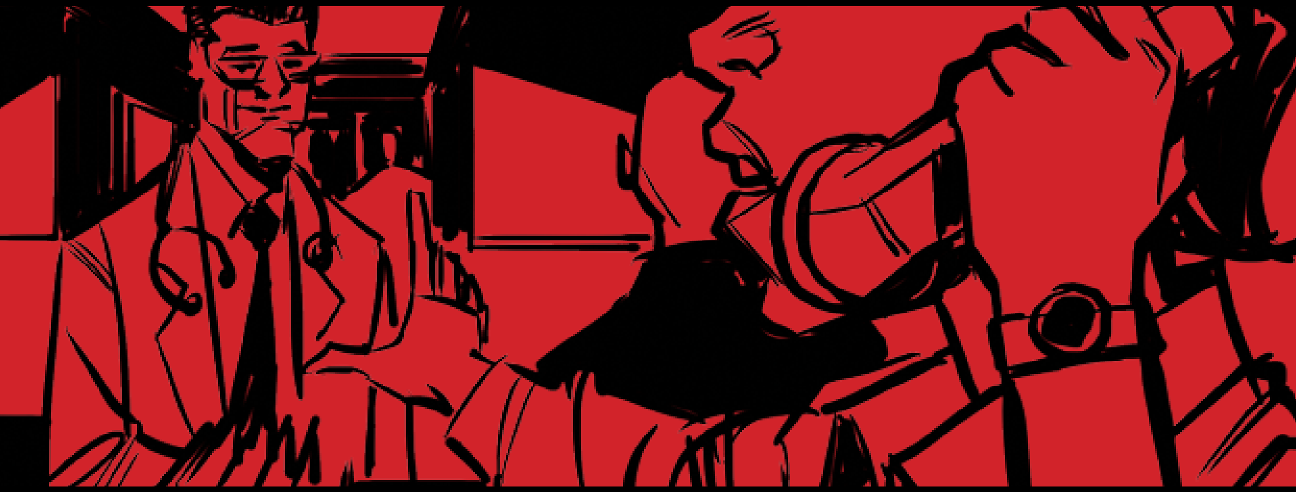
You can, however, learn to reduce the risk of being compromised to an acceptable level using industry best practices for security architecture.

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.

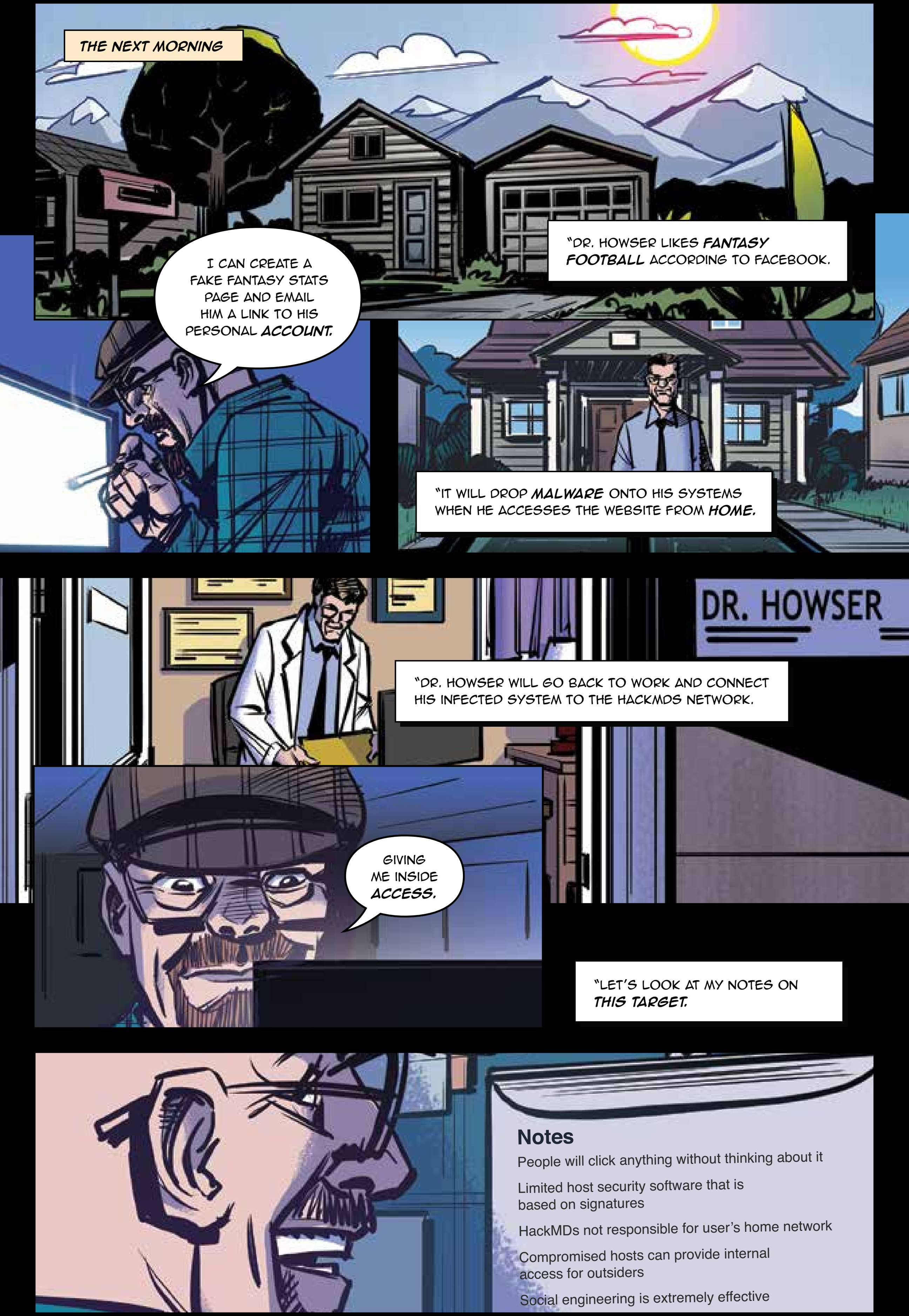
CTR HEROES ACTIVATE!

2017 Cisco Cyber Threat Response Clinic 2.0, International.



Compromised Laptop

Chapter Four


THE NEXT MORNING
"DR. HOWSER LIKES *FANTASY FOOTBALL* ACCORDING TO FACEBOOK.
I CAN CREATE A FAKE FANTASY STATS PAGE AND EMAIL HIM A LINK TO HIS PERSONAL *ACCOUNT.*
"IT WILL DROP *MALWARE* ONTO HIS SYSTEMS WHEN HE ACCESSES THE WEBSITE FROM *HOME.*
DR. HOWSER
"DR. HOWSER WILL GO BACK TO WORK AND CONNECT HIS INFECTED SYSTEM TO THE HACKMDS NETWORK.
GIVING ME INSIDE *ACCESS.*
"LET'S LOOK AT MY NOTES ON *THIS TARGET.*

Notes

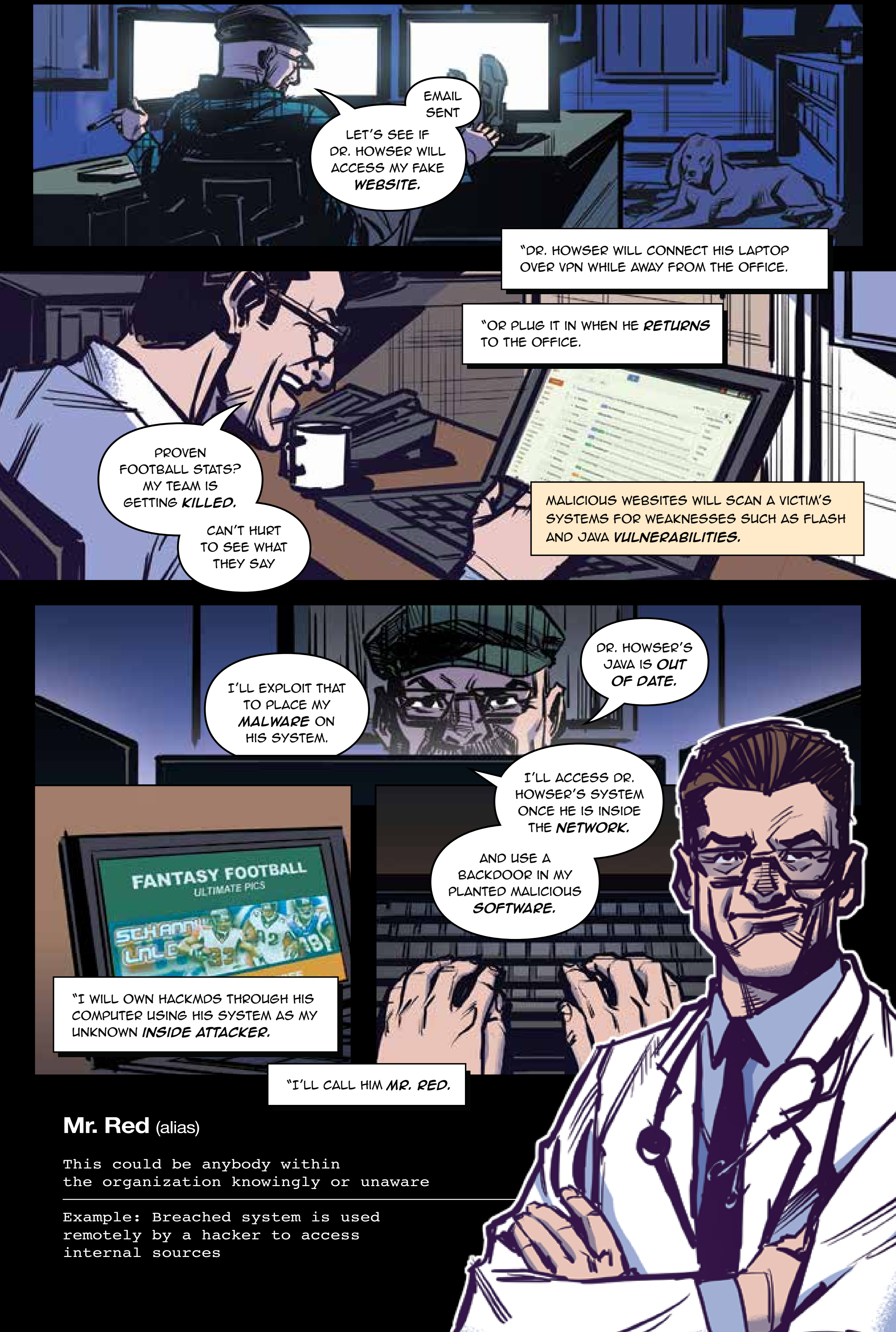
People will click anything without thinking about it

Limited host security software that is based on signatures

HackMDs not responsible for user's home network

Compromised hosts can provide internal access for outsiders

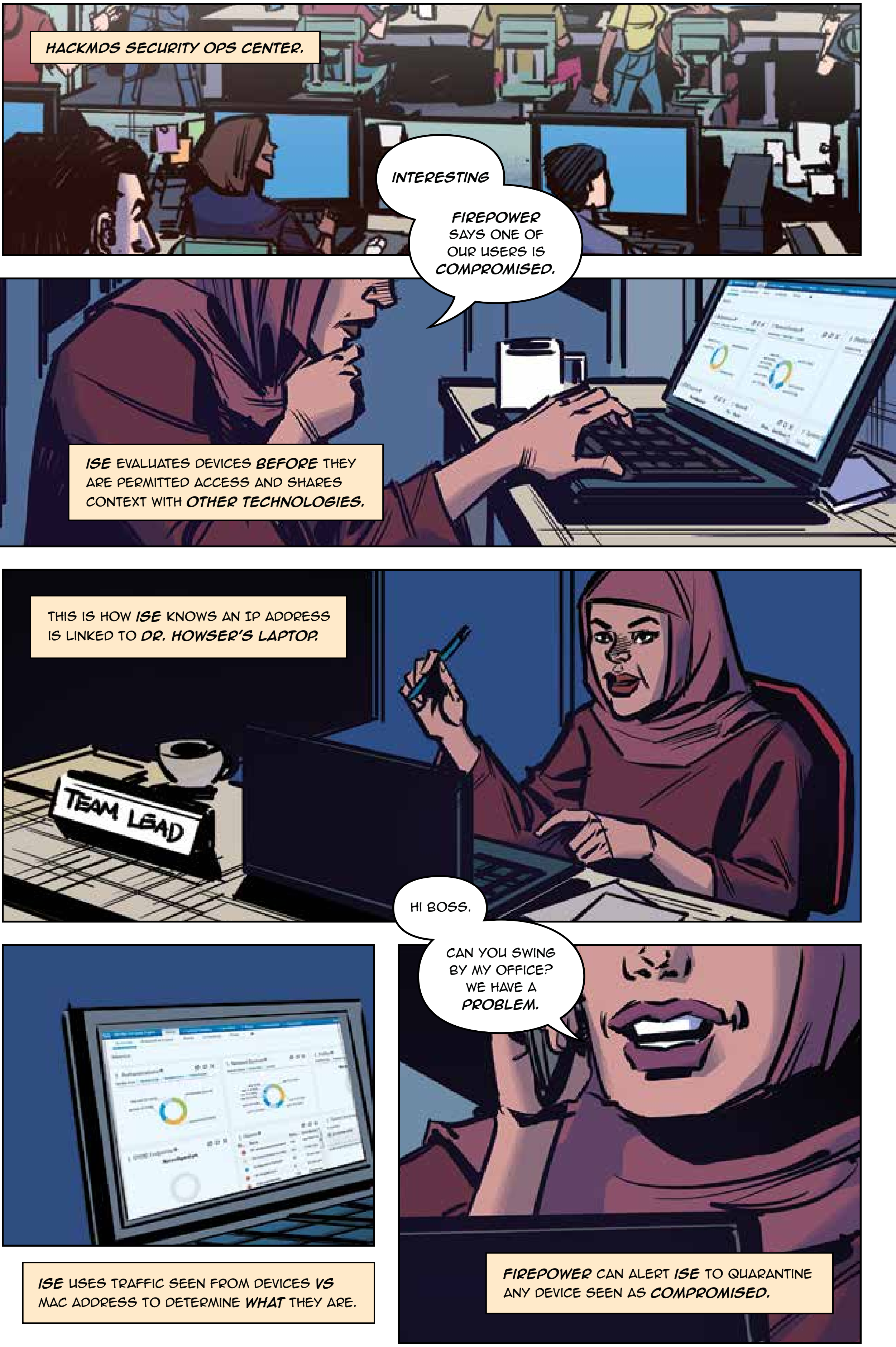
Social engineering is extremely effective

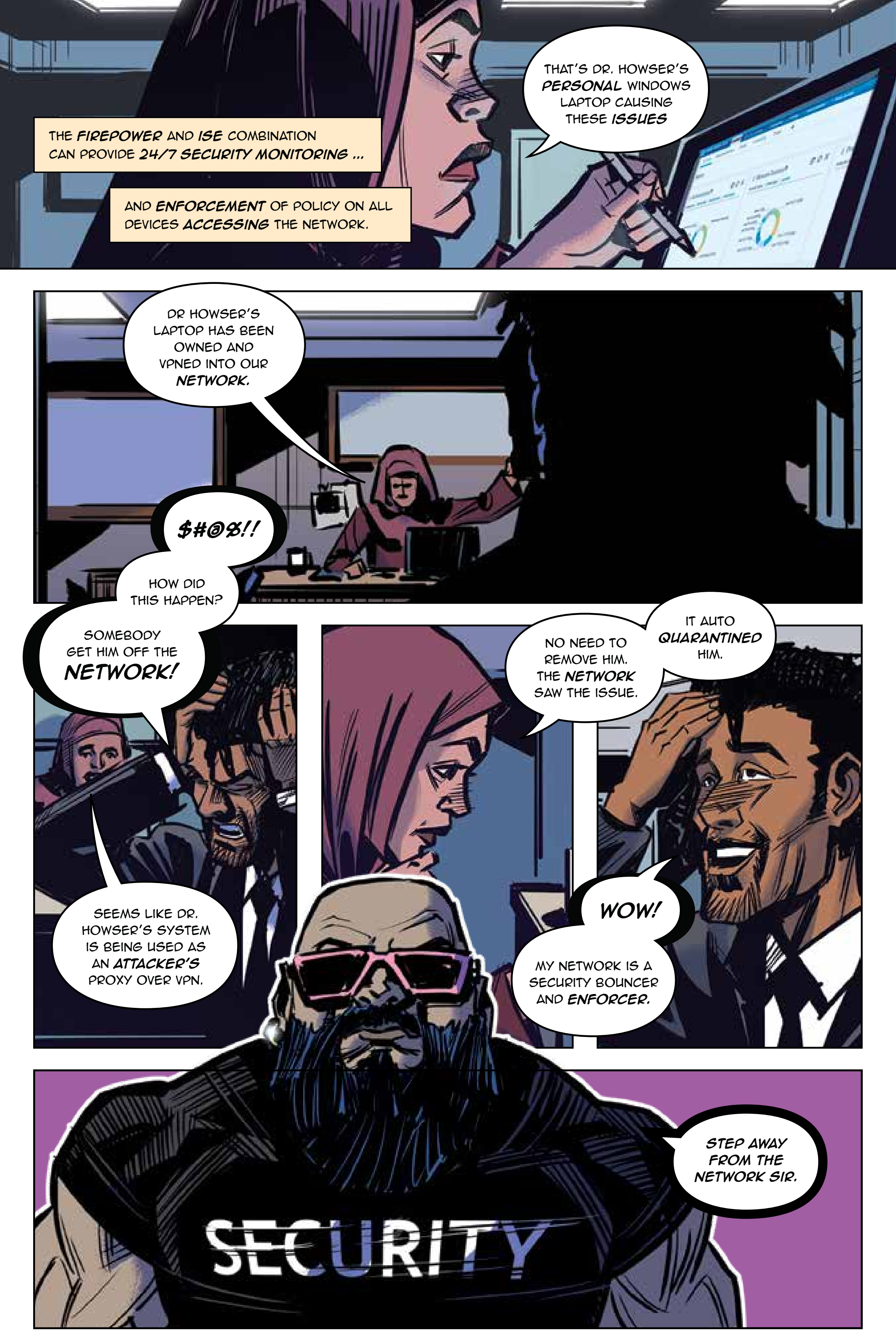

EMAIL SENT
LET'S SEE IF DR. HOWSER WILL ACCESS MY FAKE *WEBSITE.*
"DR. HOWSER WILL CONNECT HIS LAPTOP OVER VPN WHILE AWAY FROM THE OFFICE.
"OR PLUG IT IN WHEN HE *RETURNS* TO THE OFFICE.
PROVEN FOOTBALL STATS? MY TEAM IS GETTING *KILLED.*
CAN'T HURT TO SEE WHAT THEY SAY
MALICIOUS WEBSITES WILL SCAN A VICTIM'S SYSTEMS FOR WEAKNESSES SUCH AS FLASH AND JAVA *VULNERABILITIES.*
DR. HOWSER'S JAVA IS *OUT OF DATE.*
I'LL EXPLOIT THAT TO PLACE MY *MALWARE* ON HIS SYSTEM.
I'LL ACCESS DR. HOWSER'S SYSTEM ONCE HE IS INSIDE THE *NETWORK.*
AND USE A BACKDOOR IN MY PLANTED MALICIOUS *SOFTWARE.*
FANTASY FOOTBALL
ULTIMATE PICS
"I WILL OWN HACKMDS THROUGH HIS COMPUTER USING HIS SYSTEM AS MY UNKNOWN *INSIDE ATTACKER.*
"I'LL CALL HIM *MR. RED.*

Mr. Red (alias)

This could be anybody within the organization knowingly or unaware

Example: Breached system is used remotely by a hacker to access internal sources


HACKMDS SECURITY OPS CENTER.
INTERESTING
FIREPOWER SAYS ONE OF OUR USERS IS COMPROMISED.
ISE EVALUATES DEVICES BEFORE THEY ARE PERMITTED ACCESS AND SHARES CONTEXT WITH OTHER TECHNOLOGIES.
THIS IS HOW ISE KNOWS AN IP ADDRESS IS LINKED TO DR. HOWSER'S LAPTOP.
TEAM LEAD
HI BOSS.
CAN YOU SWING BY MY OFFICE? WE HAVE A PROBLEM.
ISE USES TRAFFIC SEEN FROM DEVICES VS MAC ADDRESS TO DETERMINE WHAT THEY ARE.
FIREPOWER CAN ALERT ISE TO QUARANTINE ANY DEVICE SEEN AS COMPROMISED.


THE FIREPOWER AND ISE COMBINATION CAN PROVIDE 24/7 SECURITY MONITORING ...
AND ENFORCEMENT OF POLICY ON ALL DEVICES ACCESSING THE NETWORK.
THAT'S DR. HOWSER'S PERSONAL WINDOWS LAPTOP CAUSING THESE ISSUES
DR HOWSER'S LAPTOP HAS BEEN OWNED AND VPNED INTO OUR NETWORK.
$#@%!!
HOW DID THIS HAPPEN?
SOMEBODY GET HIM OFF THE NETWORK!
SEEMS LIKE DR. HOWSER'S SYSTEM IS BEING USED AS AN ATTACKER'S PROXY OVER VPN.
NO NEED TO REMOVE HIM. THE NETWORK SAW THE ISSUE.
IT AUTO QUARANTINED HIM.
WOW!
MY NETWORK IS A SECURITY BOUNCER AND ENFORCER.
STEP AWAY FROM THE NETWORK SIR.
SECURITY

THREAT RESPONDERS WANTED

CTR* CLINIC 2.0

*The Cyber Threat Response

Your **EXCLUSIVE** training platform for learning a range of Cisco Security products and integrated solutions

VOUCHER CODE:
^^Un1z

LEARN

- How environments get compromised
- How breaches get discovered
- How to respond most effectively with Cisco security products and solutions

EXPERIENCE

- Cyber security attack situations in a virtual lab environment
- Play as both **ATTACHER** and **DEFENDER**

Hands On | 8 Modules | Core Certification | Real-World Attacks

Use the Voucher Code Above to receive **EXCLUSIVE** access!

Enjoy this unique lab oriented, hands-on learning and solution demonstration clinic **TODAY!**

APPLY TODAY!

CLIP and **MAIL*** to your Cisco Account Manager **TODAY** to reserve your spot and get your learn on!

Name: ____________________

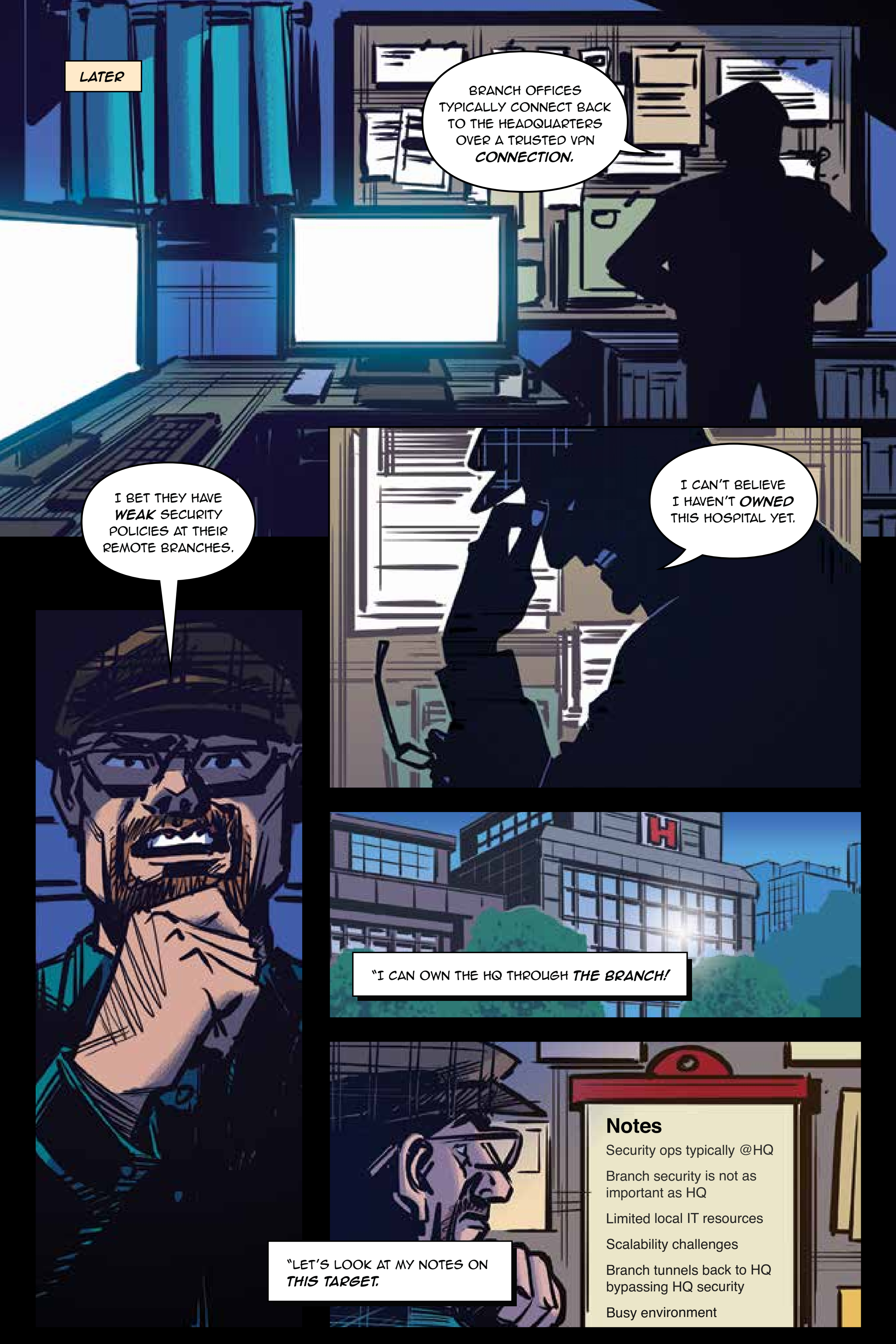
Address: ____________________

City: __________ State: __________

*or visit www.cisco.com/go/security

Attack The Branch

Chapter Five


LATER
BRANCH OFFICES TYPICALLY CONNECT BACK TO THE HEADQUARTERS OVER A TRUSTED VPN *CONNECTION.*
I BET THEY HAVE *WEAK* SECURITY POLICIES AT THEIR REMOTE BRANCHES.
I CAN'T BELIEVE I HAVEN'T *OWNED* THIS HOSPITAL YET.
H
"I CAN OWN THE HQ THROUGH *THE BRANCH!*
"LET'S LOOK AT MY NOTES ON *THIS TARGET.*
Notes
Security ops typically @HQ
Branch security is not as important as HQ
Limited local IT resources
Scalability challenges
Branch tunnels back to HQ bypassing HQ security
Busy environment

LATER OVER A SECURE IRC CHANNEL
THERE ARE *TONS* OF TOOLS THAT CAN DO THIS.

```
08:03 Mr Black - I need a physical
device planted at a branch office.
```

Mr. White (alias)

Government engineer and hardware hacking hobbyist

Develops bypass tools

Rarely involved with crime but against “The Man”

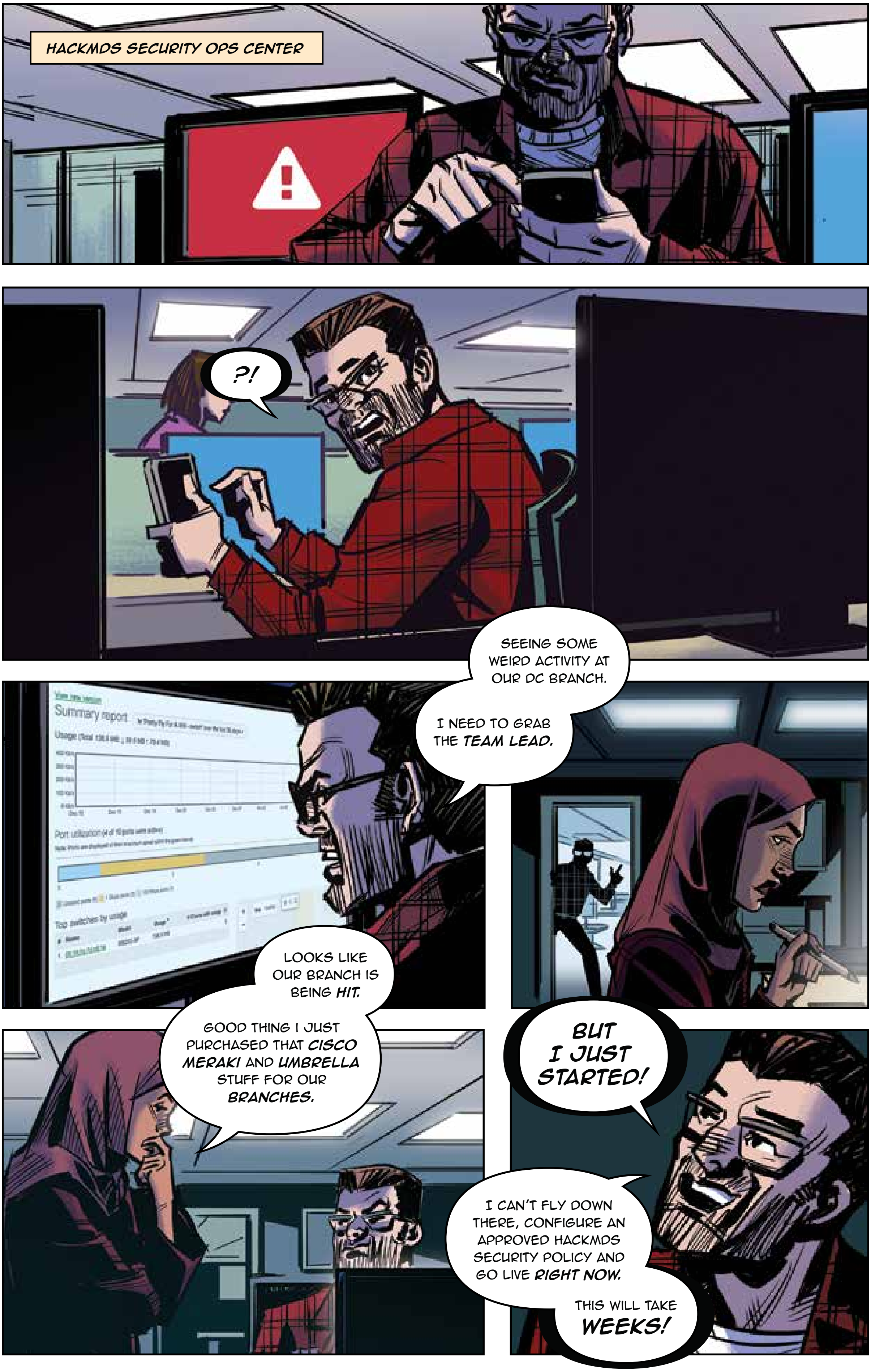
```
08:03 -:- They probably don’t enforce
security at remote locations.
```

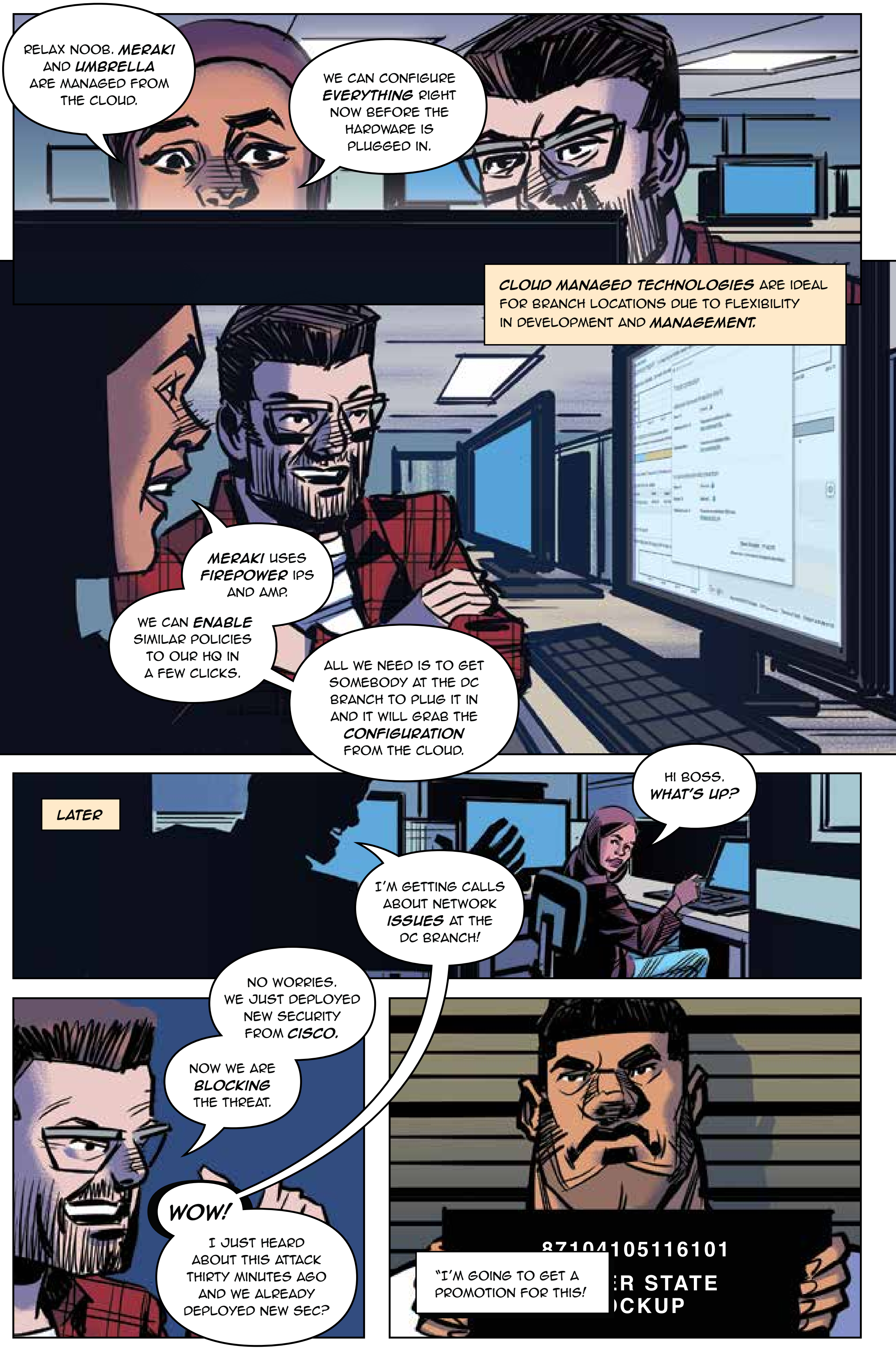
```
08:03 Mr White - I’ll plant a Pwnie
Express at one of their branch offices.
```

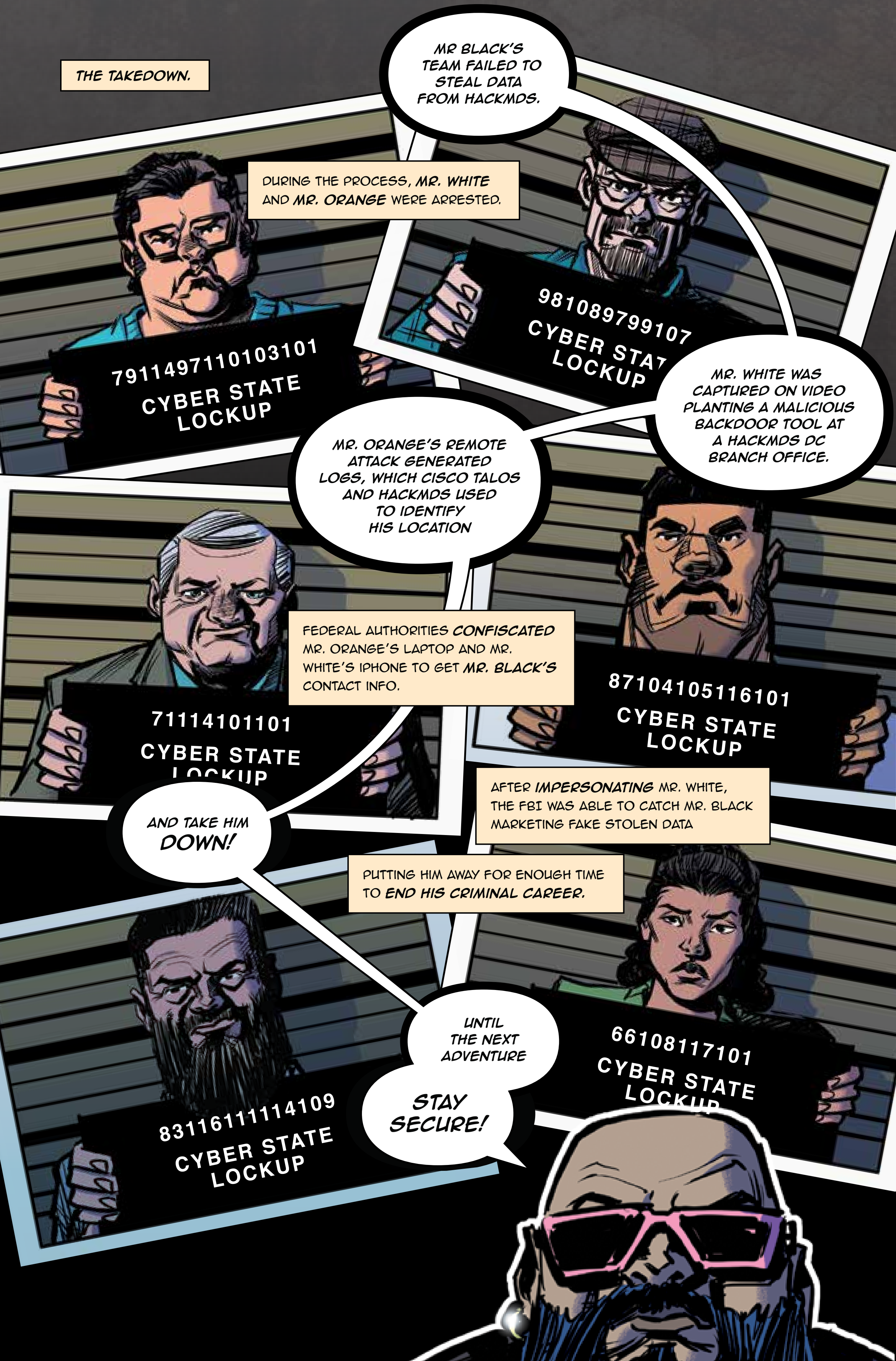
A *PWN PLUG* LOOKS LIKE A COMMON PLUG, *HOWEVER*, IS LOADED WITH ATTACKER TOOLS.

```
08:03 Mr Black - Once we have access to the branch
network, we can hit other internal targets
including the HQ through their site-to-site VPN.
```

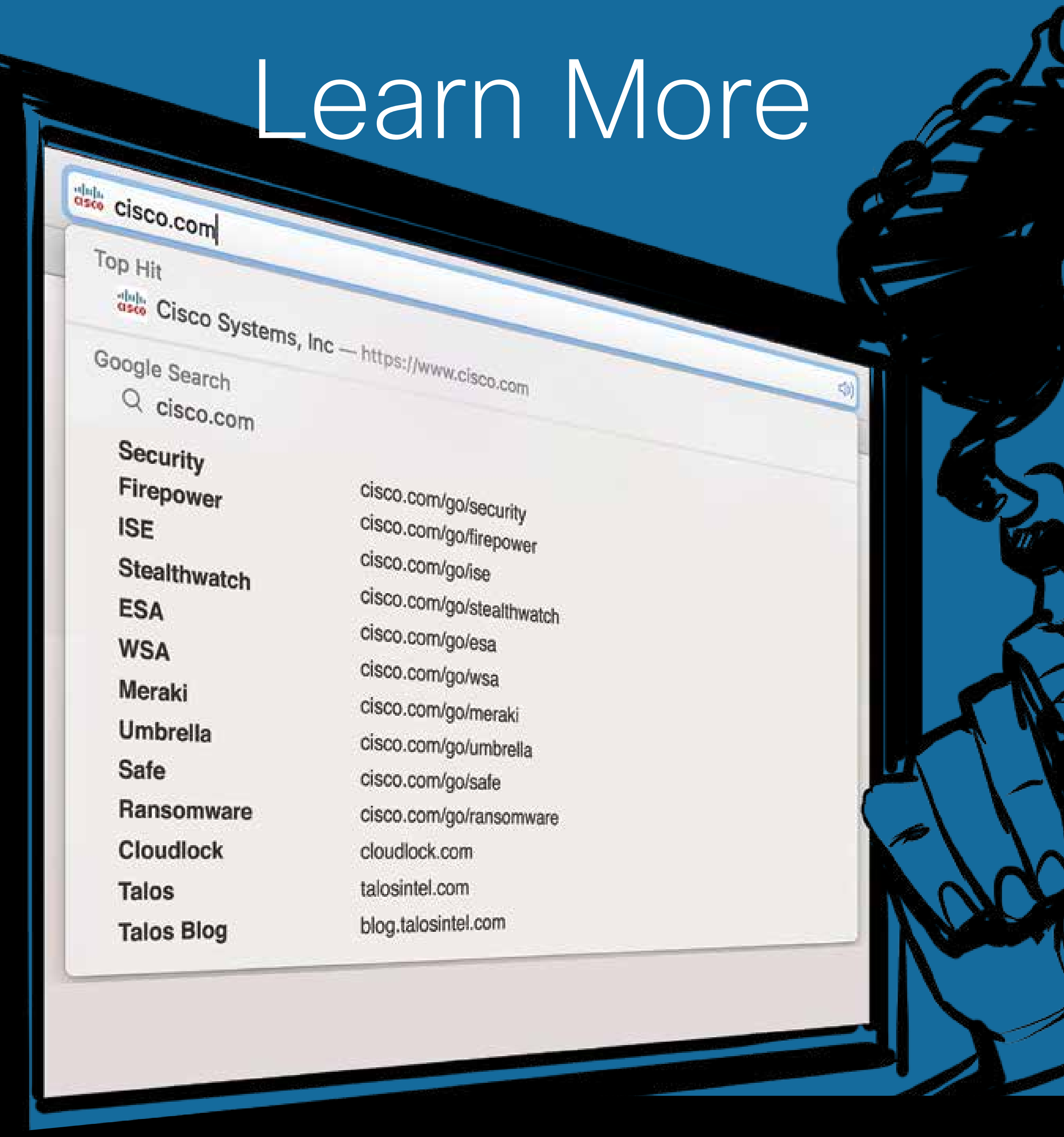
```
08:03 Mr White - I’ll pretend to hurt myself
skating and plant the tools on site.
```


HACKMDS SECURITY OPS CENTER
?!
SEEING SOME WEIRD ACTIVITY AT OUR DC BRANCH.
I NEED TO GRAB THE TEAM LEAD.
Summary report
Usage
Port utilization
Top switches by usage
LOOKS LIKE OUR BRANCH IS BEING HIT.
GOOD THING I JUST PURCHASED THAT CISCO MERAKI AND UMBRELLA STUFF FOR OUR BRANCHES.
BUT I JUST STARTED!
I CAN'T FLY DOWN THERE, CONFIGURE AN APPROVED HACKMDS SECURITY POLICY AND GO LIVE RIGHT NOW.
THIS WILL TAKE WEEKS!


RELAX NOOB. MERAKI AND UMBRELLA ARE MANAGED FROM THE CLOUD.
WE CAN CONFIGURE EVERYTHING RIGHT NOW BEFORE THE HARDWARE IS PLUGGED IN.
CLOUD MANAGED TECHNOLOGIES ARE IDEAL FOR BRANCH LOCATIONS DUE TO FLEXIBILITY IN DEVELOPMENT AND MANAGEMENT.
MERAKI USES FIREPOWER IPS AND AMP.
WE CAN ENABLE SIMILAR POLICIES TO OUR HQ IN A FEW CLICKS.
ALL WE NEED IS TO GET SOMEBODY AT THE DC BRANCH TO PLUG IT IN AND IT WILL GRAB THE CONFIGURATION FROM THE CLOUD.
LATER
HI BOSS. WHAT'S UP?
I'M GETTING CALLS ABOUT NETWORK ISSUES AT THE DC BRANCH!
NO WORRIES. WE JUST DEPLOYED NEW SECURITY FROM CISCO.
NOW WE ARE BLOCKING THE THREAT.
WOW!
I JUST HEARD ABOUT THIS ATTACK THIRTY MINUTES AGO AND WE ALREADY DEPLOYED NEW SEC?
87104105116101
ER STATE
CKUP
“I'M GOING TO GET A PROMOTION FOR THIS!


THE TAKEDOWN.
MR BLACK'S TEAM FAILED TO STEAL DATA FROM HACKMDS.
DURING THE PROCESS, MR. WHITE AND MR. ORANGE WERE ARRESTED.
7911497110103101
CYBER STATE LOCKUP
981089799107
CYBER STATE LOCKUP
MR. WHITE WAS CAPTURED ON VIDEO PLANTING A MALICIOUS BACKDOOR TOOL AT A HACKMDS DC BRANCH OFFICE.
MR. ORANGE'S REMOTE ATTACK GENERATED LOGS, WHICH CISCO TALOS AND HACKMDS USED TO IDENTIFY HIS LOCATION
FEDERAL AUTHORITIES CONFISCATED MR. ORANGE'S LAPTOP AND MR. WHITE'S IPHONE TO GET MR. BLACK'S CONTACT INFO.
71114101101
CYBER STATE LOCKUP
87104105116101
CYBER STATE LOCKUP
AFTER IMPERSONATING MR. WHITE, THE FBI WAS ABLE TO CATCH MR. BLACK MARKETING FAKE STOLEN DATA
AND TAKE HIM DOWN!
PUTTING HIM AWAY FOR ENOUGH TIME TO END HIS CRIMINAL CAREER.
83116111114109
CYBER STATE LOCKUP
66108117101
CYBER STATE LOCKUP
UNTIL THE NEXT ADVENTURE
STAY SECURE!

Learn More



cisco.com

Top Hit

Cisco Systems, Inc — https://www.cisco.com

Google Search

cisco.com

Security	cisco.com/go/security
Firepower	cisco.com/go/firepower
ISE	cisco.com/go/ise
Stealthwatch	cisco.com/go/stealthwatch
ESA	cisco.com/go/esa
WSA	cisco.com/go/wsa
Meraki	cisco.com/go/meraki
Umbrella	cisco.com/go/umbrella
Safe	cisco.com/go/safe
Ransomware	cisco.com/go/ransomware
Cloudlock	cloudlock.com
Talos	talosintel.com
Talos Blog	blog.talosintel.com

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

VPN
Encrypted communication

Cisco Umbrella
DNS Security and forensics

Stealthwatch
Netflow anomaly monitoring and breach detection

ESA
Email security for cloud and on-prem

CloudLock
Cloud application security

ISE
Access control and security policy management

Threatgrid
Threat analytics, detection and prevention

Meraki
Cloud managed security, network and collaboration

Talos
Security research and threat intelligence

AMP
Advanced breach detection for endpoint and network

WSA
Secure proxy, content control and security

Physical · Virtual · Cloud