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

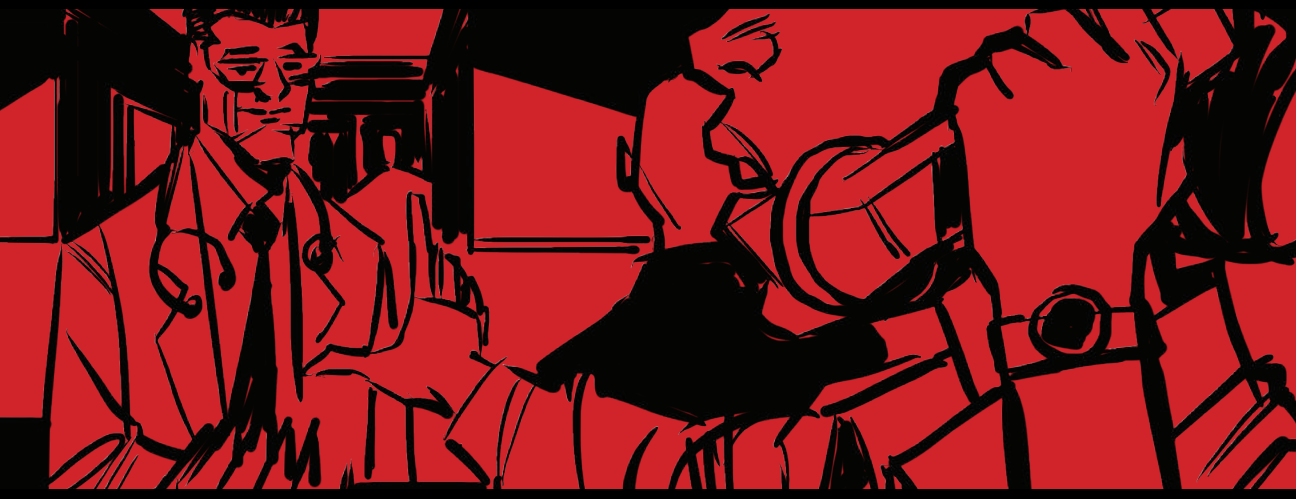
Brian McGee

art direction/design

Santos Vega

editing

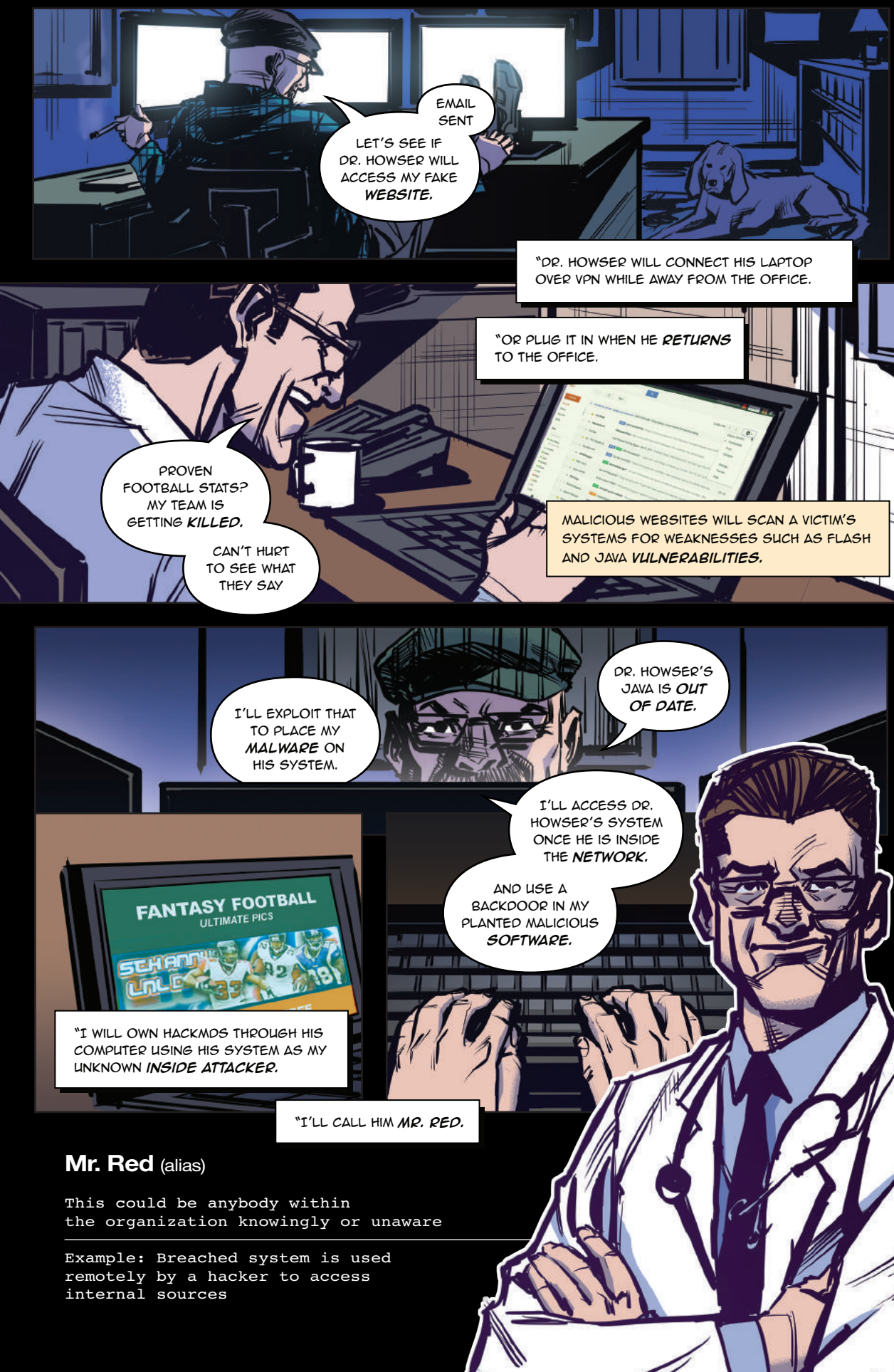
Andrew Akers



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



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

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!**

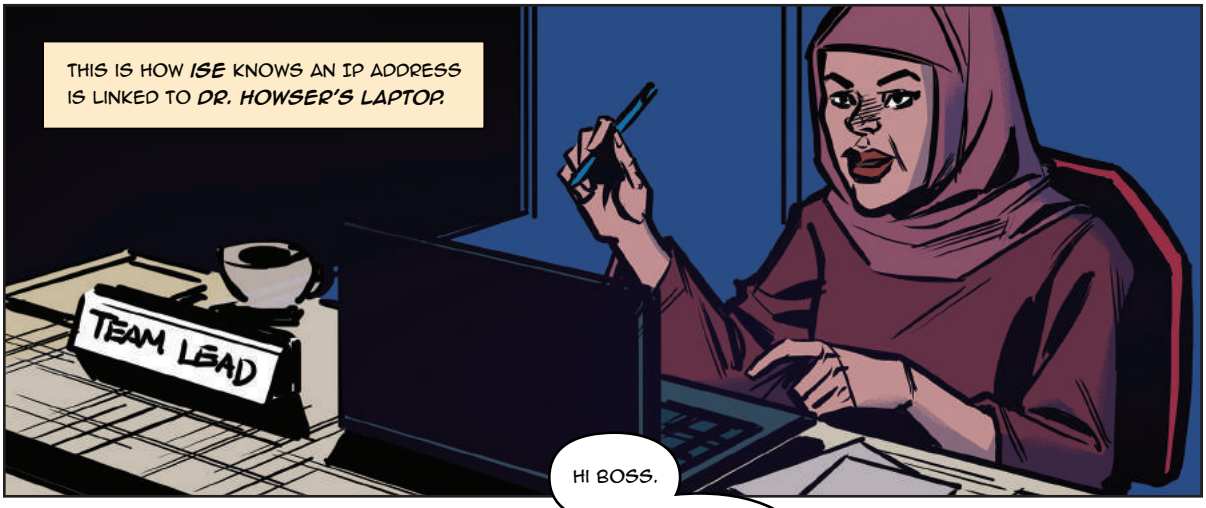
REDUCE RISK

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

EDUCATE YOURSELF

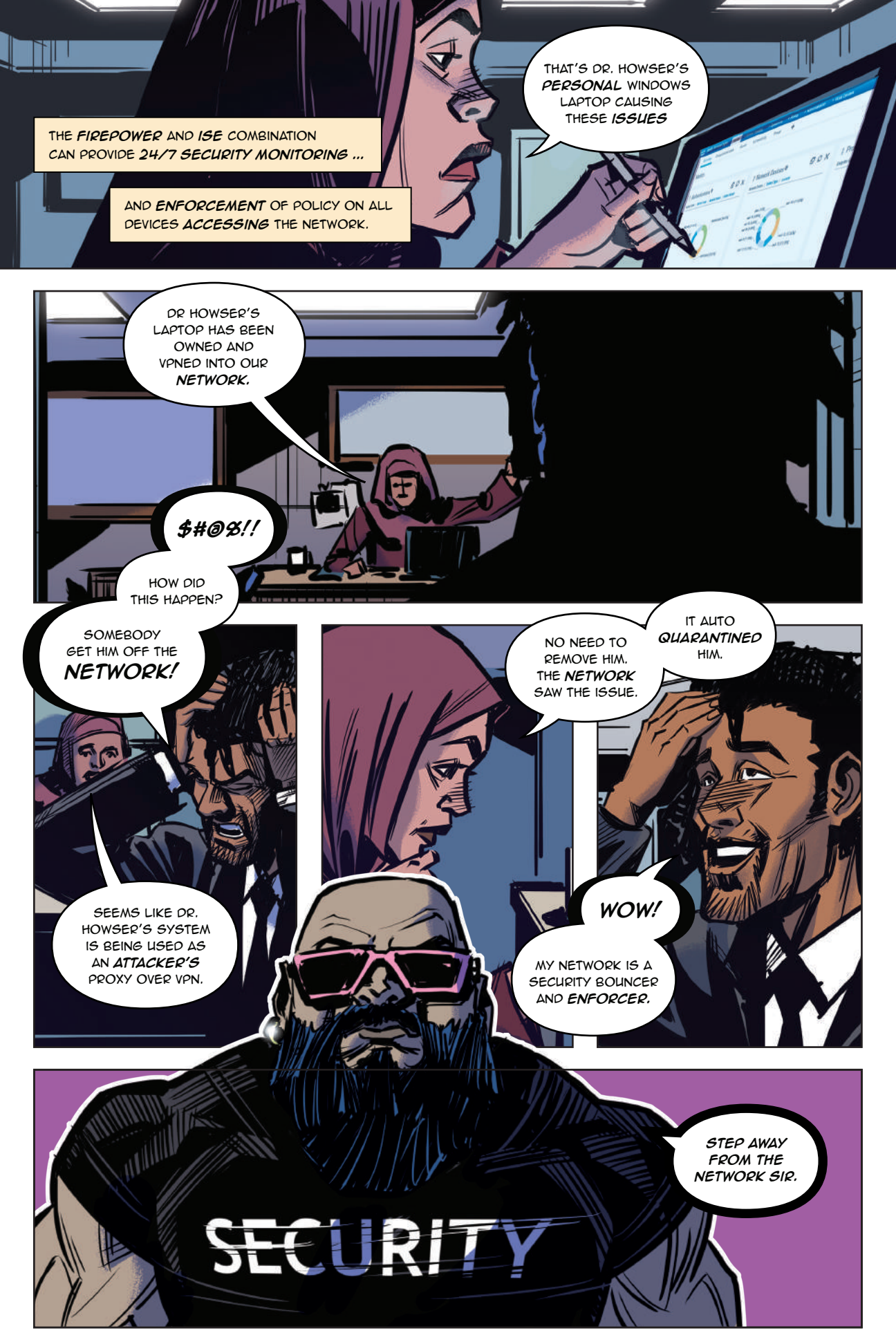
The Cisco Cyber Threat Response Clinics give you hands-on experience as both **ATTACKER** and **DEFENDER** so you can better understand both sides of the cyber **CAT AND MOUSE** game.

CTR HEROES ACTIVATE!



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.
SECURITY
STEP AWAY FROM THE NETWORK SIR.

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.

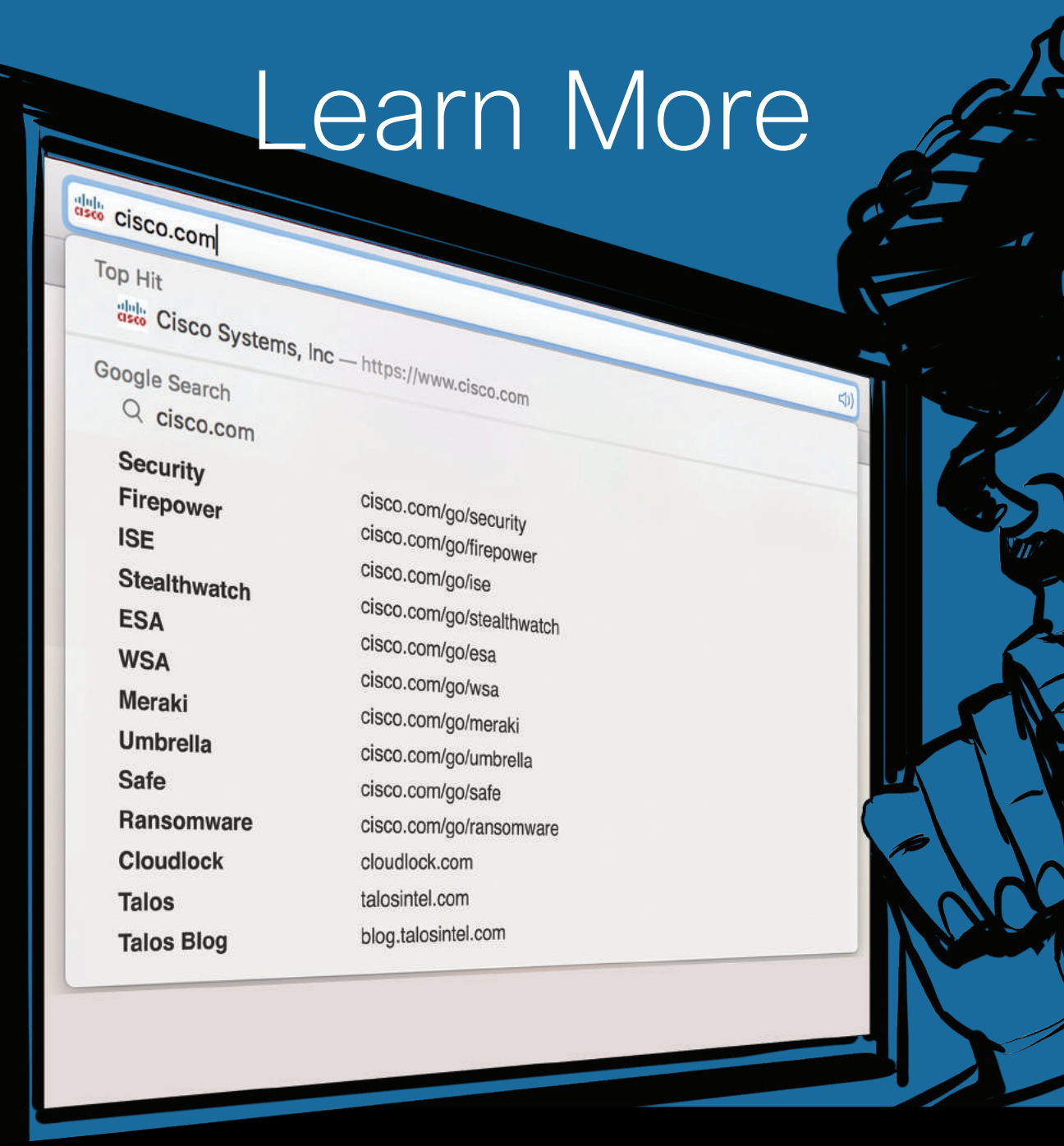
Coming Soon 2 ur CPU

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