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

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.
"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
08:03 Mr Black - I need a physical device planted at a branch office.
THERE ARE TONS OF TOOLS THAT CAN DO THIS.
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.

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.

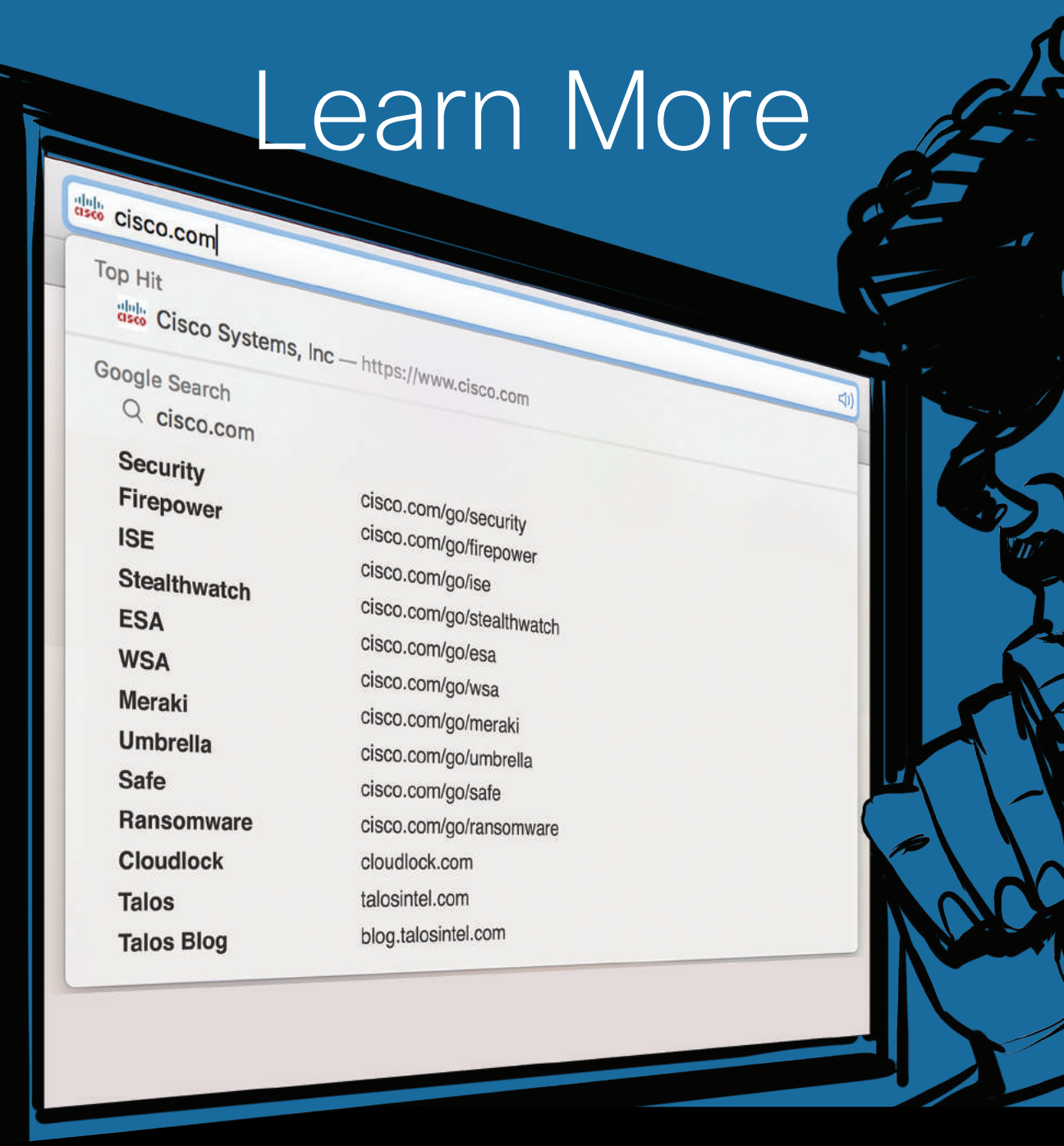
CTR HEROES ACTIVATE!


HACKMDS SECURITY OPS CENTER
?!
SEEING SOME WEIRD ACTIVITY AT OUR DC BRANCH.
I NEED TO GRAB THE TEAM LEAD.
View new version
Summary report
Usage (Total 138.9 MB ↓ 59.5 MB ↑ 79.4 MB)
Port utilization (4 of 10 ports were active)
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?
"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 STAT
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
AND TAKE HIM DOWN!
AFTER IMPERSONATING MR. WHITE, THE FBI WAS ABLE TO CATCH MR. BLACK MARKETING FAKE STOLEN DATA
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



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