

The logo for 'ixia' is displayed in a bold, black, lowercase sans-serif font. The letter 'i' has a small red dot above it, and the letter 'a' has a small green dot above it. The background of the slide is a vibrant blue sky with a cityscape at sunset, featuring a river, various high-rise buildings, and a prominent skyscraper on the right side.

ixia

TRAIN LIKE YOU FIGHT

MODELLING CYBER REAL-WORLD SCENARIOS

Alexandru Enache, System Engineer

UKRAINE ELECTRIC GRID HACK



- Phishing Email
- 'KillDisk' and BlackEnergy 3
- Coordinated DDoS attack

- 23rd of December, when half of the staff is off duty

<http://thehackernews.com/2016/01/Ukraine-power-system-hacked.html>

Current Defense Mechanisms and Challenges

Cyber Defense Technologies

- ✓ **Network Based Mitigation**
Applications awareness and control
User Identity and Control
Content Security (IPS, GAV, DLP, AntiSpam)
SSL encryption/decryption
DDoS mitigation
IP reputation, URL filtering
- ✓ **Network Behavior Analysis Detection**
collects and analyzes traffic from the entire network — host and applications
- ✓ **Host Based Mitigation (AV, DLP, IPS)**
- ✓ **Vulnerability Management**

Cyber Defense Challenges

- ✓ **Cyber Security Threats** have become more complex, targeted and persistent
- ✓ **The Information Security landscape** is constantly evolving
- ✓ **Borderless Networks**
driven by new technologies and trends (Mobility/BYOD, Cloud, Social Media)
- ✓ **Staff Education**
How to test and train with network and Internet technologies and systems



Modern cyber-defenses require proactive security operations

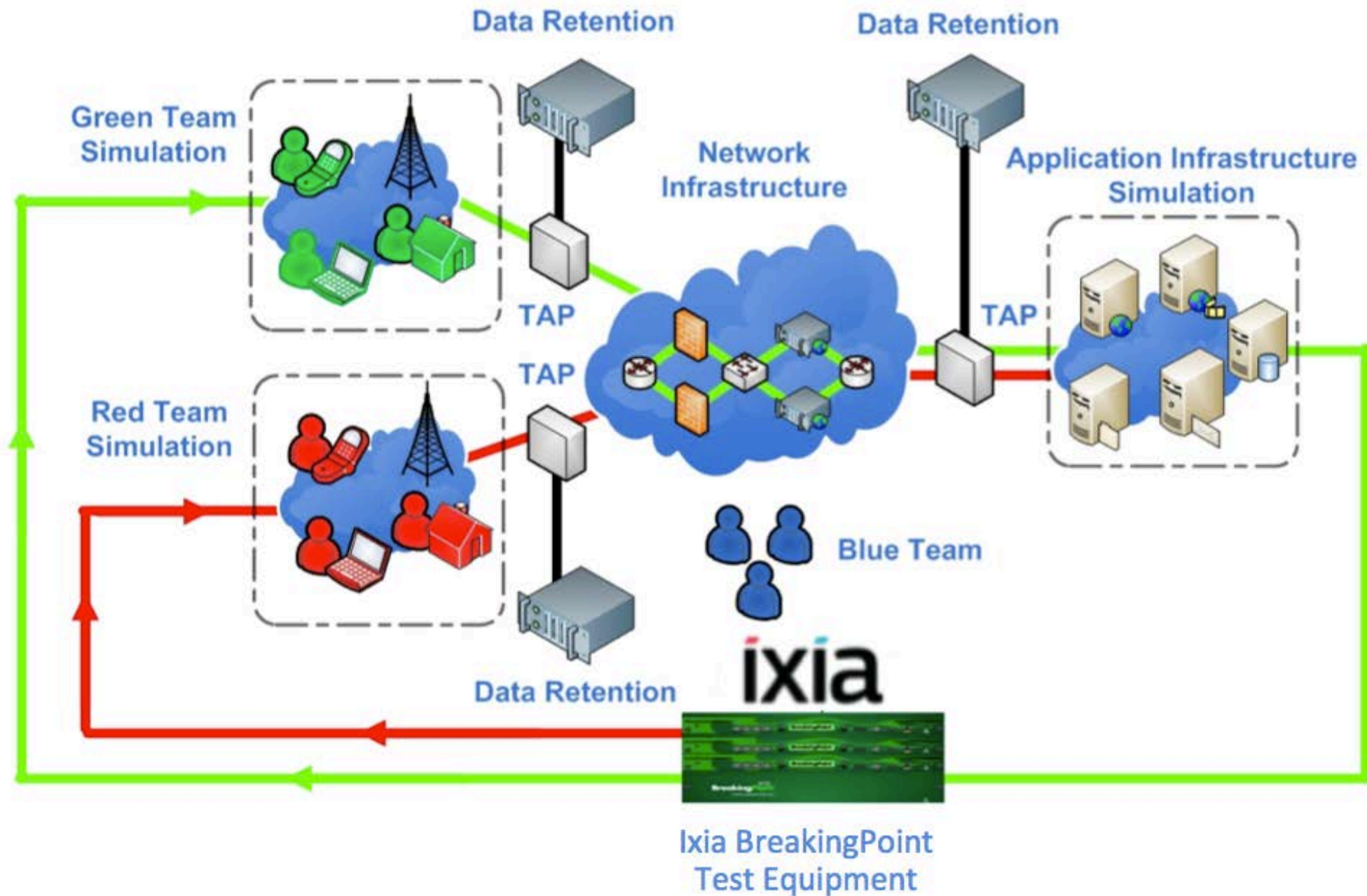
Cyber ranges help security staff build the skills and experience necessary to combat modern cyber threats

TRAIN LIKE YOU FIGHT!

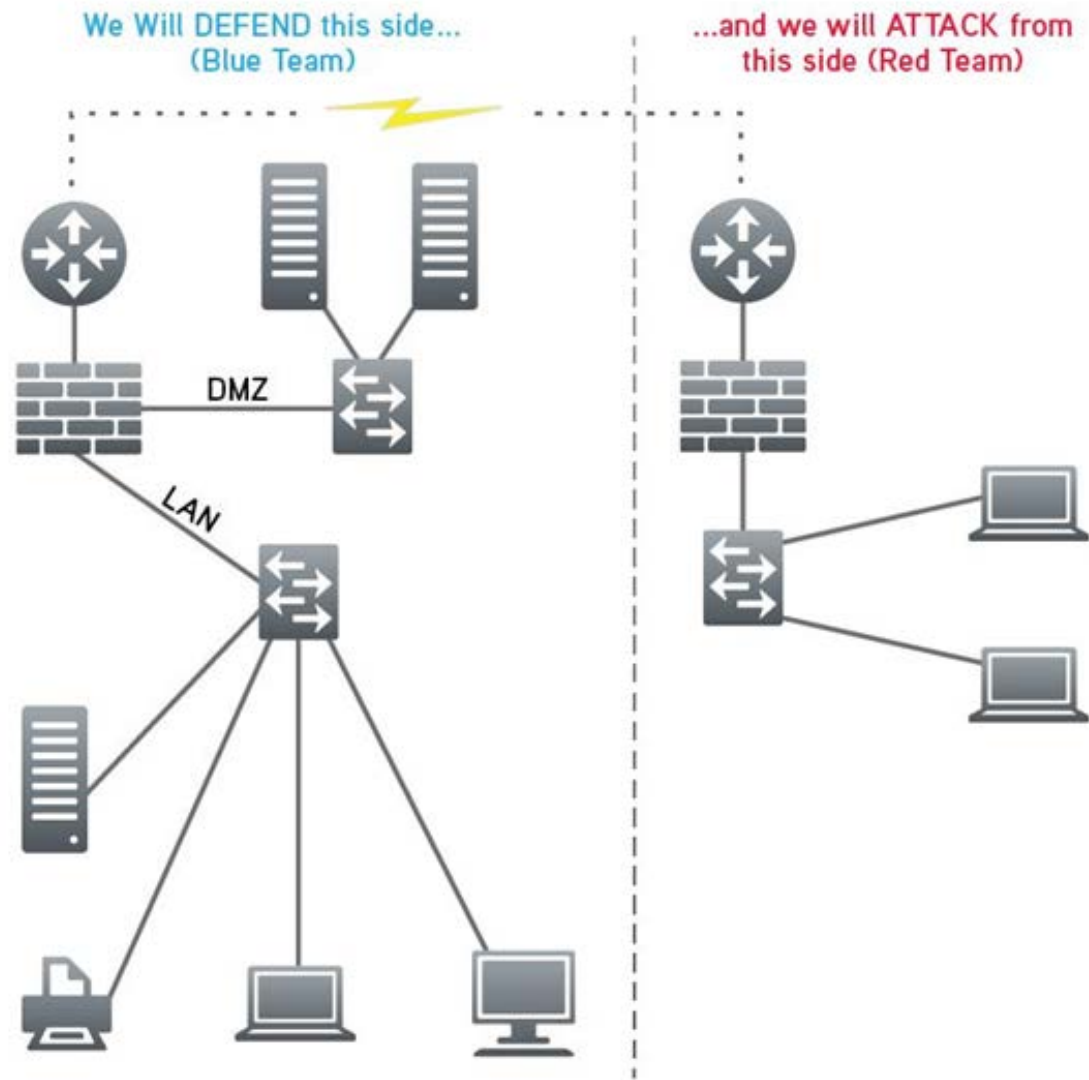


- No more “hearers and seers” protecting our networks and critical infrastructures
- How do we manage in a complex and ever changing environment?
- Education and Training Afforded by Realistic Cyber Ranges Can Stem the Gap

CYBER RANGE INTEGRATION



CYBER RANGE ENVIRONMENTS



Physical / Virtual / Hybrid Cyber Range

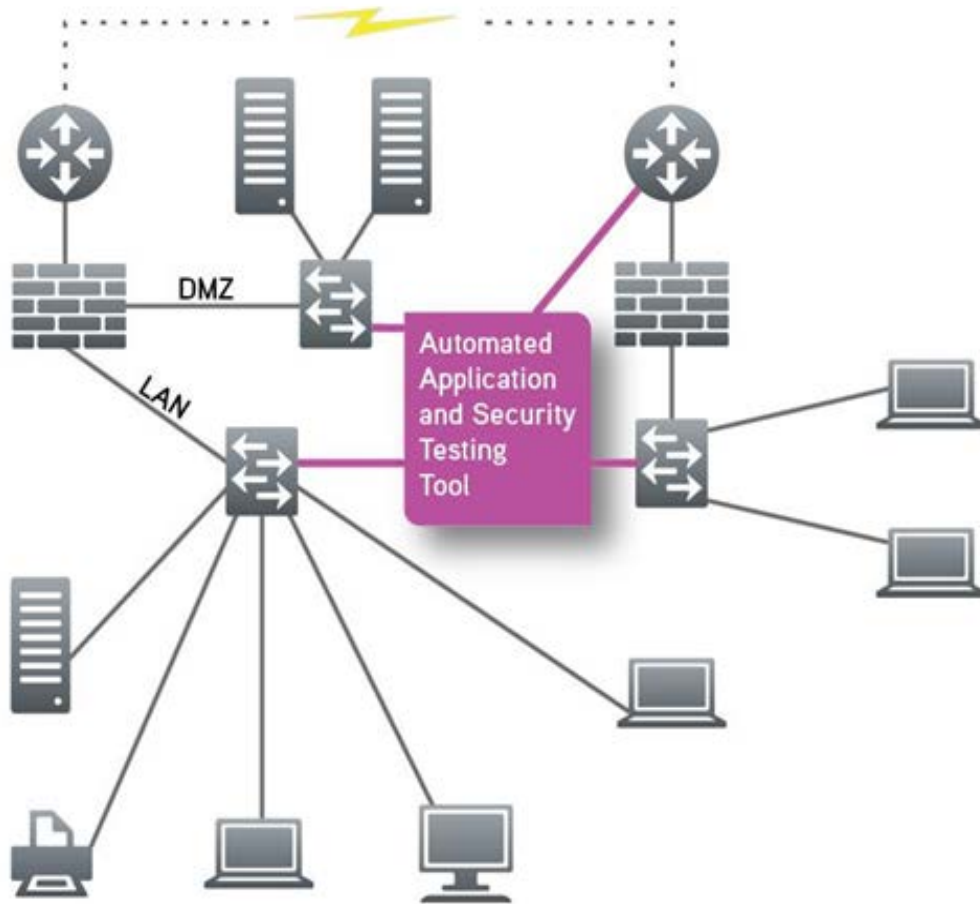
- Physical Cyber Range: Very realistic but has a huge financial cost and long time to set up.
- Virtual Cyber Range: Low cost, but limited in emulating full performance of security devices
- Hybrid Cyber Range: Balanced approach. Combine flexibility with performance



THE KEY IS REALISM

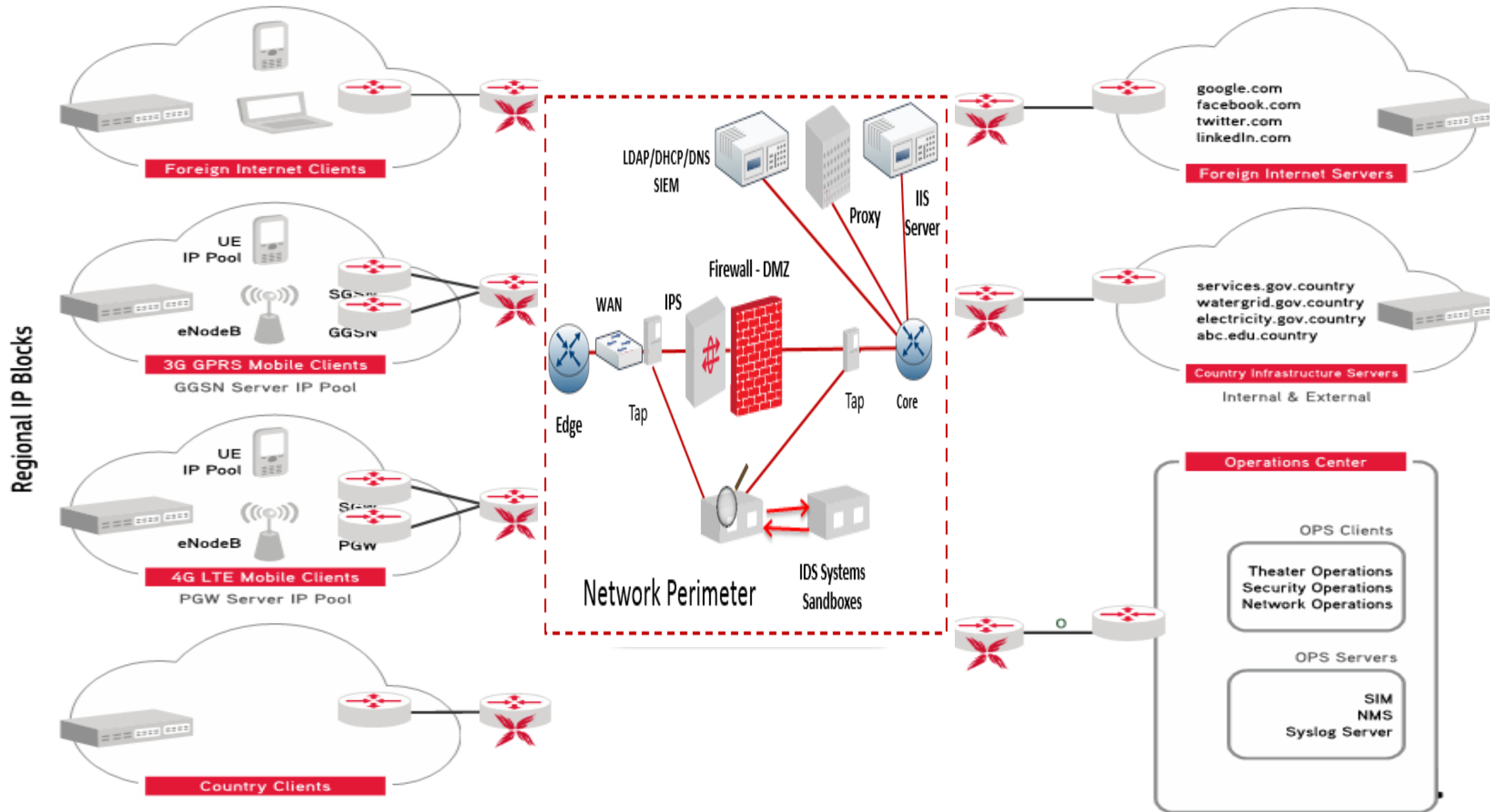
- How do you manage realism?
- To encourage realism, your range configuration will have many critical considerations
 - Human capital
 - Different attack/defense paradigms
 - Scale
- Many challenges
 - How do you model tens, hundreds, thousands, or more employees and the constantly changing applications and data they use on a day to day basis
 - How to gain expertise to generate effective attack scenarios to stress network defenses in your range (internal personnel, outside resources, etc.)
 - How do you scale those attack vectors when you don't have the computing resources of a worldwide botnet at your disposal?

CREATING AND MANAGING REALISM – TRAIN LIKE YOU FIGHT!



- Employ actual people on the range – doesn't scale to more than a few people
- Capture and replay production network traffic – don't allow for real world data randomness over time
- Use a set of automated tools to quickly and efficiently pick and choose what you want your background traffic mixes and attack traffic mixes to look like
- **Or you could do the smart thing, and use a hybrid approach of all of these, and in doing so, create the Next Generation Cyber Range**

HIGH LEVEL TOPOLOGY



BLUE TEAM – SIX STEPS OF INCIDENT RESPONSE



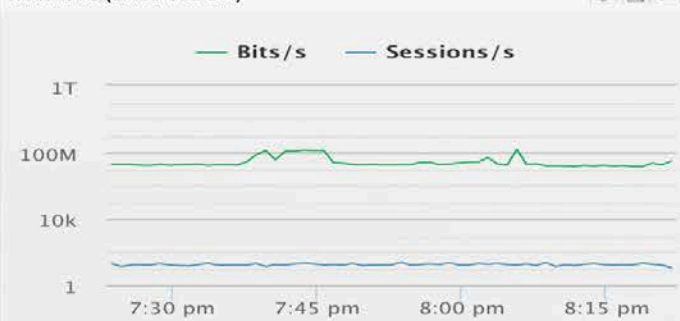
- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned (follow-up)

GAIN INSIGHT AT THE APPLICATION LEVEL

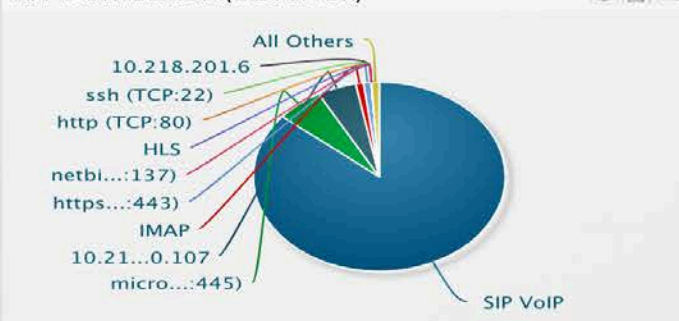
NEW FILTER +

- Facebook
- India Australia
- Russia
- USAdd

TRAFFIC (LAST HOUR)



APP DISTRIBUTION (LAST HOUR)



LATEST DYNAMIC APPS (LAST HOUR)

App	Sessions	Total B...	Discove...
10.218.21.14	10	2.9 KB	12/07/15
10.218.36.20	8	2.1 KB	12/07/15
10.218.36.43	7	1.8 KB	12/07/15
10.218.36.41	5	1.3 KB	12/07/15
10.219.117.214	47	34.4 KB	12/07/15
ustx-nas1	24	23.1 KB	12/07/15
10.218.201.6	14	49.7 MB	12/07/15
10.218.20.239	86	36.6 KB	12/07/15
10.218.201.199	17	510.4 KB	12/07/15
ixiacom.com	12	119.1 KB	12/07/15

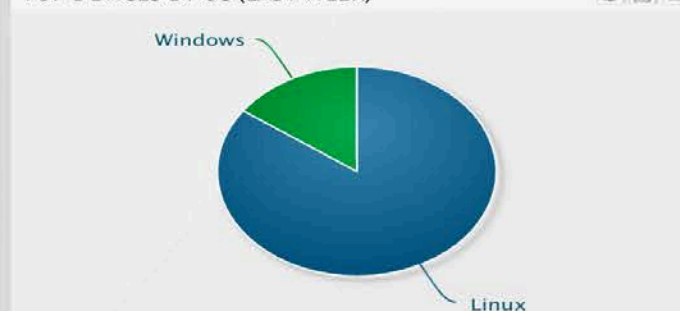
TOP COUNTRIES (LAST HOUR)

Country	Sessions	Total B...	Sha...
United States	104,675	13.6 GB	100%
Private-IP	1,984	13.5 MB	0%
Unknown	19,672	1.3 MB	0%
Canada	41	1.1 MB	0%
Ireland	14	904.9 KB	0%
Romania	161	65.3 KB	0%
United Kingdom	64	8.4 KB	0%
Europe	1	6.7 KB	0%
Chile	1	920 bytes	0%
India	3	834 bytes	0%

WORLD (LAST HOUR)



TOP DEVICES BY OS (LAST WEEK)



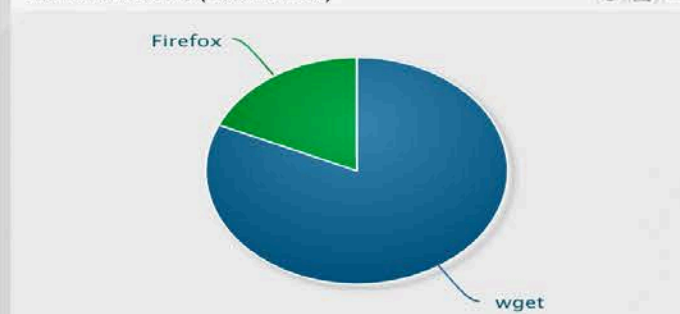
TOP FILTERS (LAST HOUR)

Filter	Sessions	Total B...	Sha...
USAdd	60,604	13.6 GB	100%
India Australia	3	834 bytes	0%
Russia	5	362 bytes	0%

TOP APPS (LAST HOUR)

App	Sessions	Total B...	Sha...
SIP VoIP	14	11.8 GB	86%
microsoft-ds (TCP:445)	2,579	800.2 MB	6%
10.218.200.107	17	700.6 MB	5%
IMAP	2	143.6 MB	1%
https (TCP:443)	3,694	115.4 MB	1%
10.218.201.6	15	49.8 MB	0%
ssh (TCP:22)	110	37.1 MB	0%
http (TCP:80)	196	11.8 MB	0%
HLS	3	11.5 MB	0%
netbios-ns (UDP:137)	8,245	7.8 MB	0%

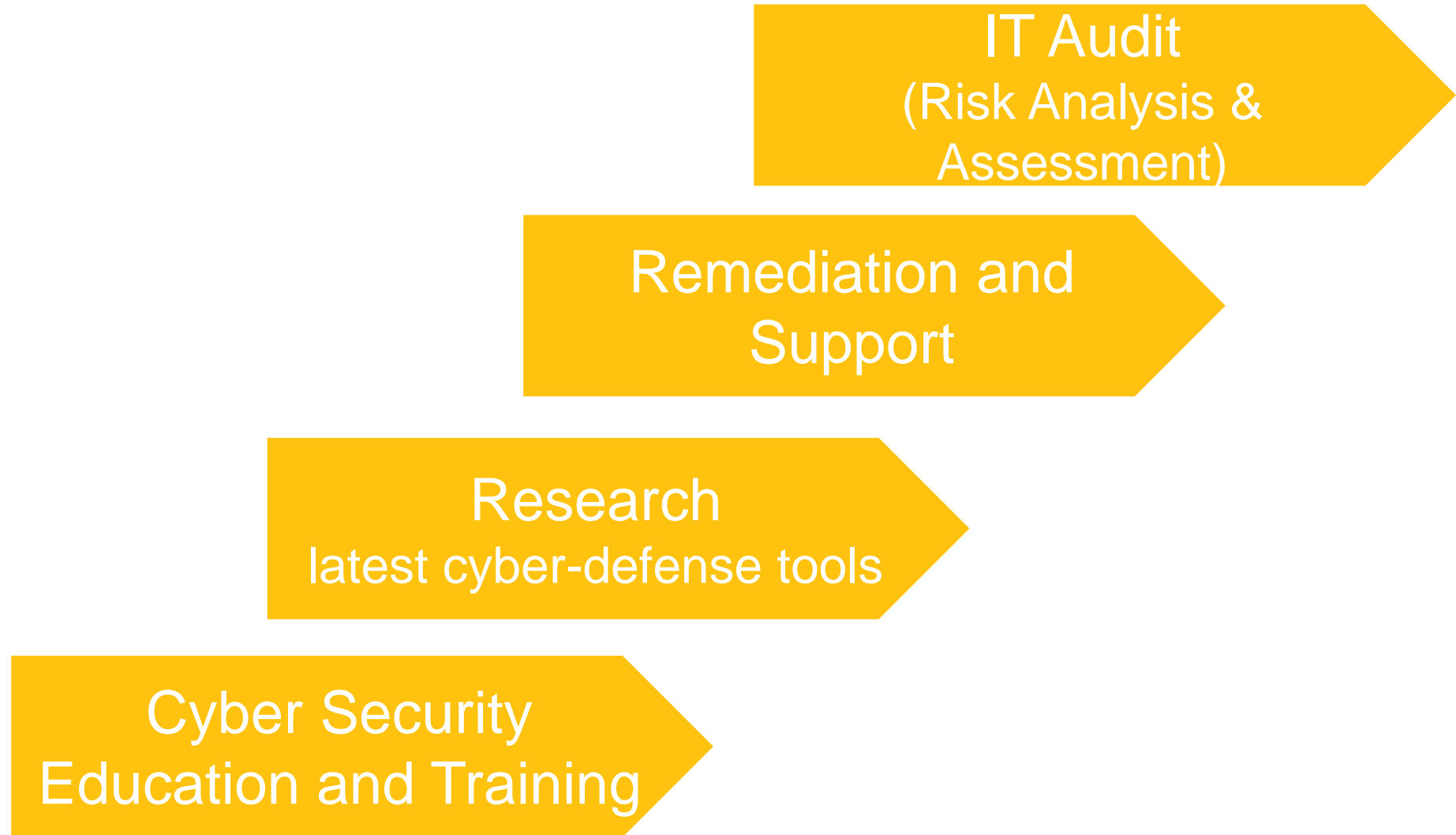
TOP BROWSERS (LAST WEEK)



NETFLOW METADATA TO REGENERATE THE DYNAMICS OF PRODUCTION NETWORKS FOR MORE REALISTIC CYBER RANGE SCENARIOS



Building value with Cyber Ranges



WHY CYBER RANGES?

- Why do organizations need Cyber Ranges:
 - Constantly test SOC/NOC personnel
 - Test network infrastructure
 - Test security devices/policies
 - Research
- Industry can no longer rely on “On The Job” training and shoulder surfing
- Traditional vendor training focuses on HOW to operate device, not HOW TO REACT and DAY TO DAY OPERATION

WHO NEEDS A CYBER RANGE?

- Enterprises
- Service Providers
- Network Equipment Manufacturers
- Government organizations

Cyber Attack Readiness – How a Cyber Range Solution Can Help

Remarkably
like your production network

A sandbox to test network
infrastructure without
causing problems on
production network

Puts people under test



BAE SYSTEMS



NORTHROP GRUMMAN

Internet-Scale Cyber Range Environment

- Realistic target simulations
- Realistic exploit simulations
- Realistic evasion simulations
- Realistic traffic simulation
- Population and country user base
- Mobile subscriber user base
- Data of interest or “needle in a haystack” for data loss prevention (DLP)
- Enterprise and IT services
- Internet IPv4 and IPv6 infrastructure

Ixia Cyber Range Solution

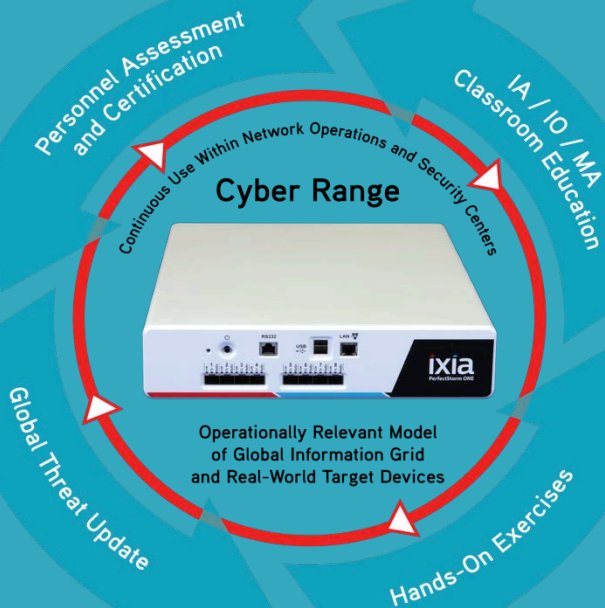
Training Services

Cyber Attack Tools

Cyber Warfare Scenarios

Network Infrastructure Model

Network Traffic Visibility





1 Tbps DDoS Attack

Powered By 150,000 Hacked IoT Devices

<http://thehackernews.com/2016/09/ddos-attack-iot.html>

The logo for ixia is displayed in white lowercase letters on the front face of a 3D cyan cube. The cube is centered on the slide. The background is a solid cyan color with a faint, repeating pattern of hexagons.

ixia

Thank you

alenache@ixiacom.com