COVA CCI • KEYNOTE

Building Cyber Resilience Together

Cyber Ranges, Deception, and Maritime Security

Opportunities for Collaboration



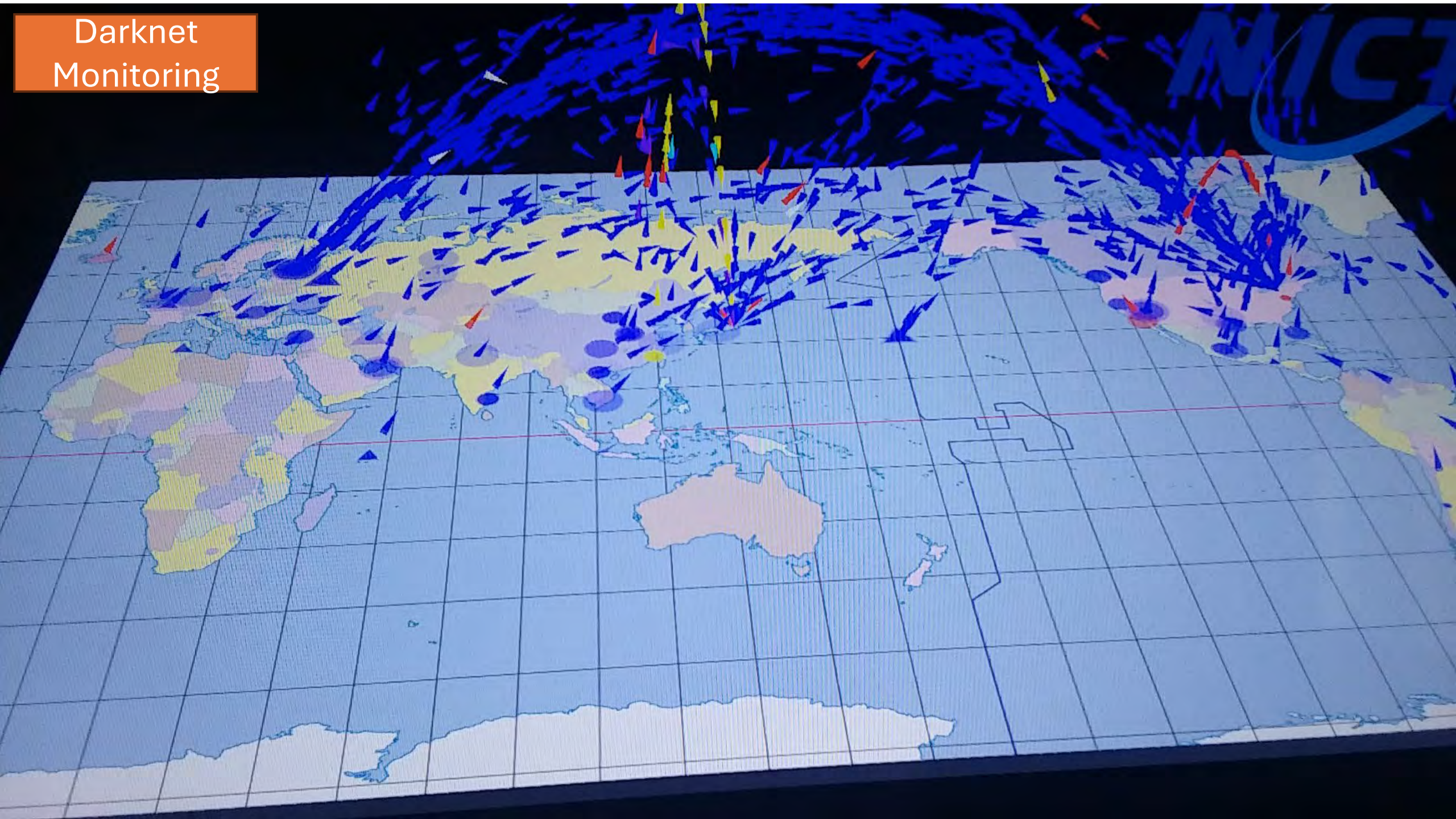
Dr. Hossein Sarrafzadeh

Professor of Electrical and Computer Engineering
Associate Dean of Research and Innovation
Frank Batten College of Engineering and Technology
Old Dominion University

Email: asarrafz@odu.edu
Cell: 716-790-0771

October 30, 2026

Darknet/Livenet Monitoring

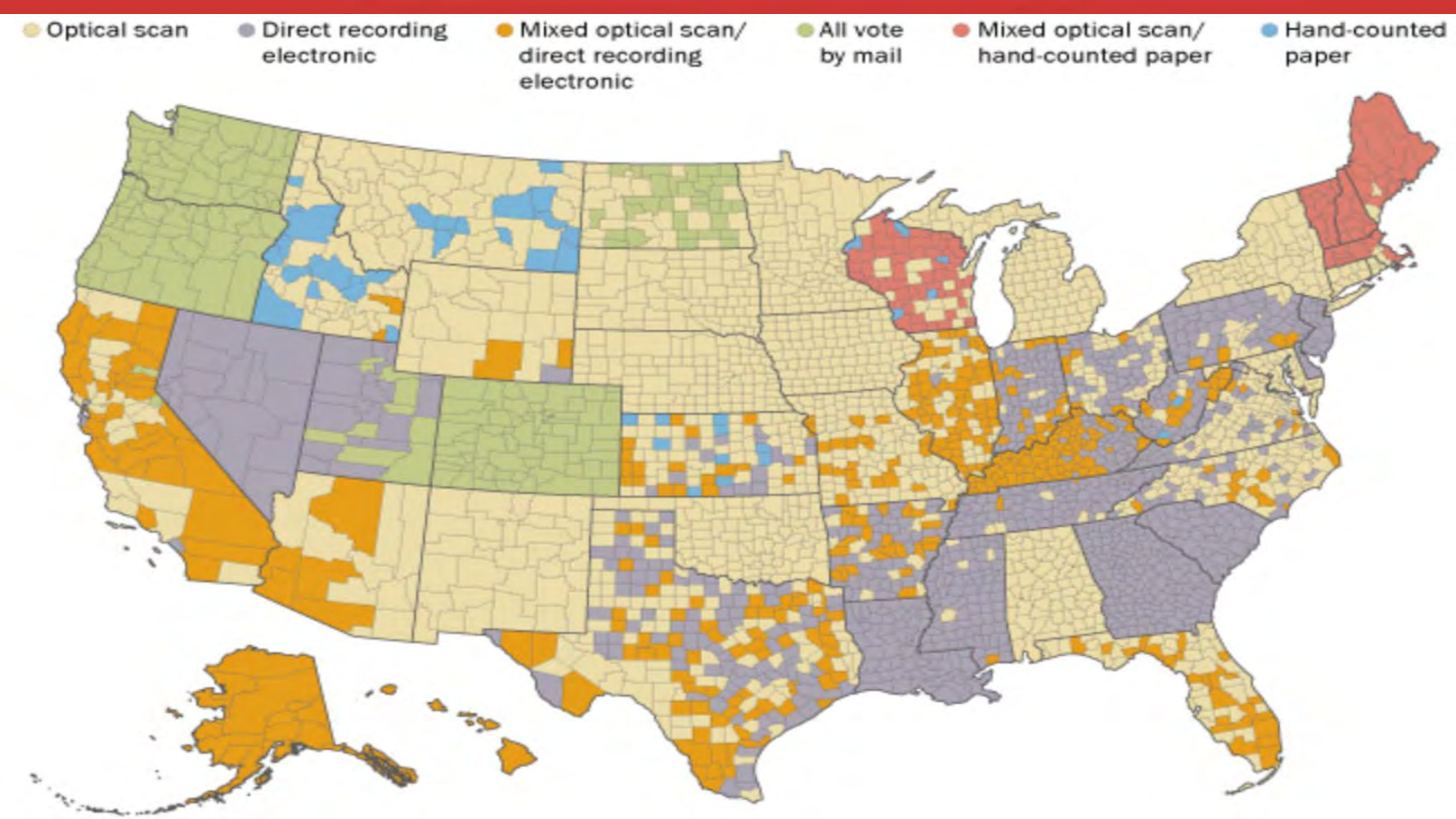

Darknet
Monitoring

Alert System



ODU Deceptive Security Lab

Election Security

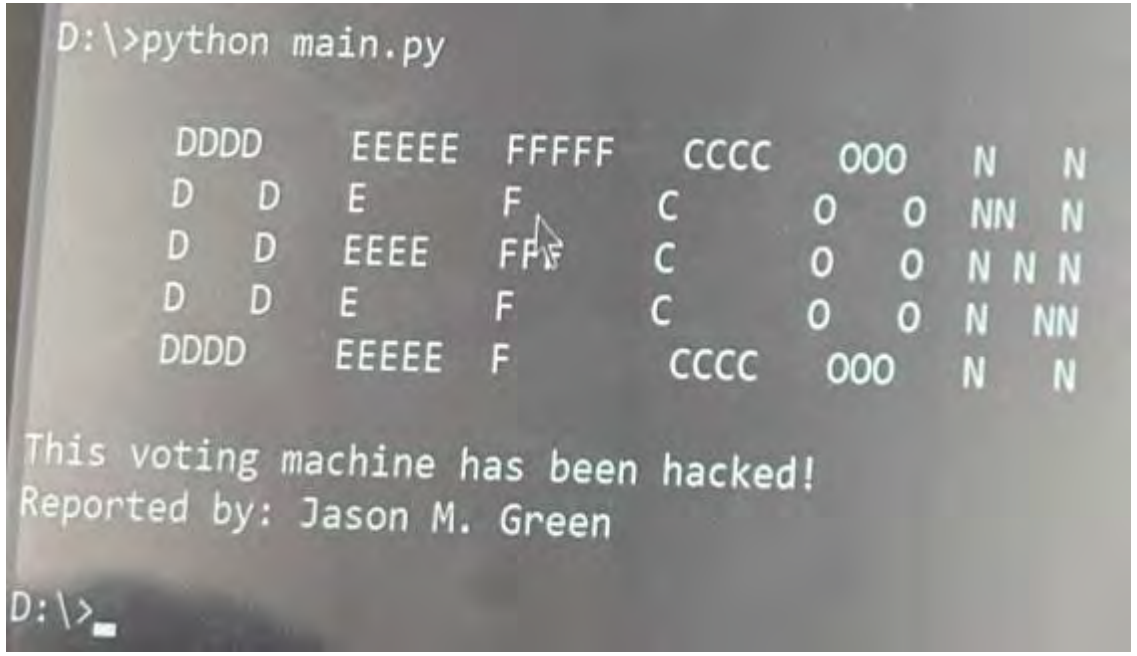

Optical scan
Direct recording electronic
Mixed optical scan/ direct recording electronic
All vote by mail
Mixed optical scan/ hand-counted paper
Hand-counted paper

Honeynet for Election Security

POLITICO

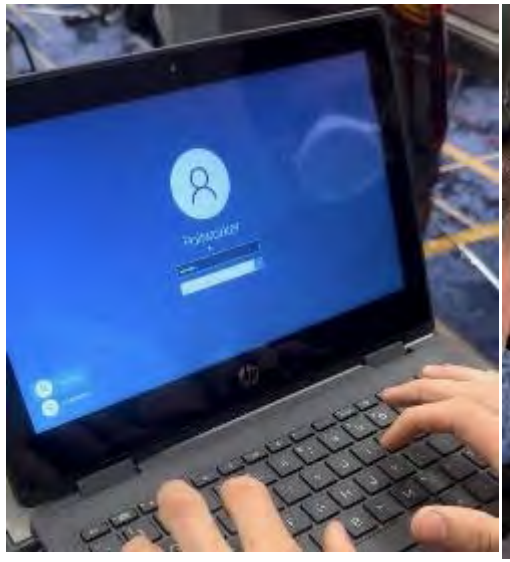
CYBERSECURITY

The nation's best hackers found vulnerabilities in voting machines — but no time to fix them



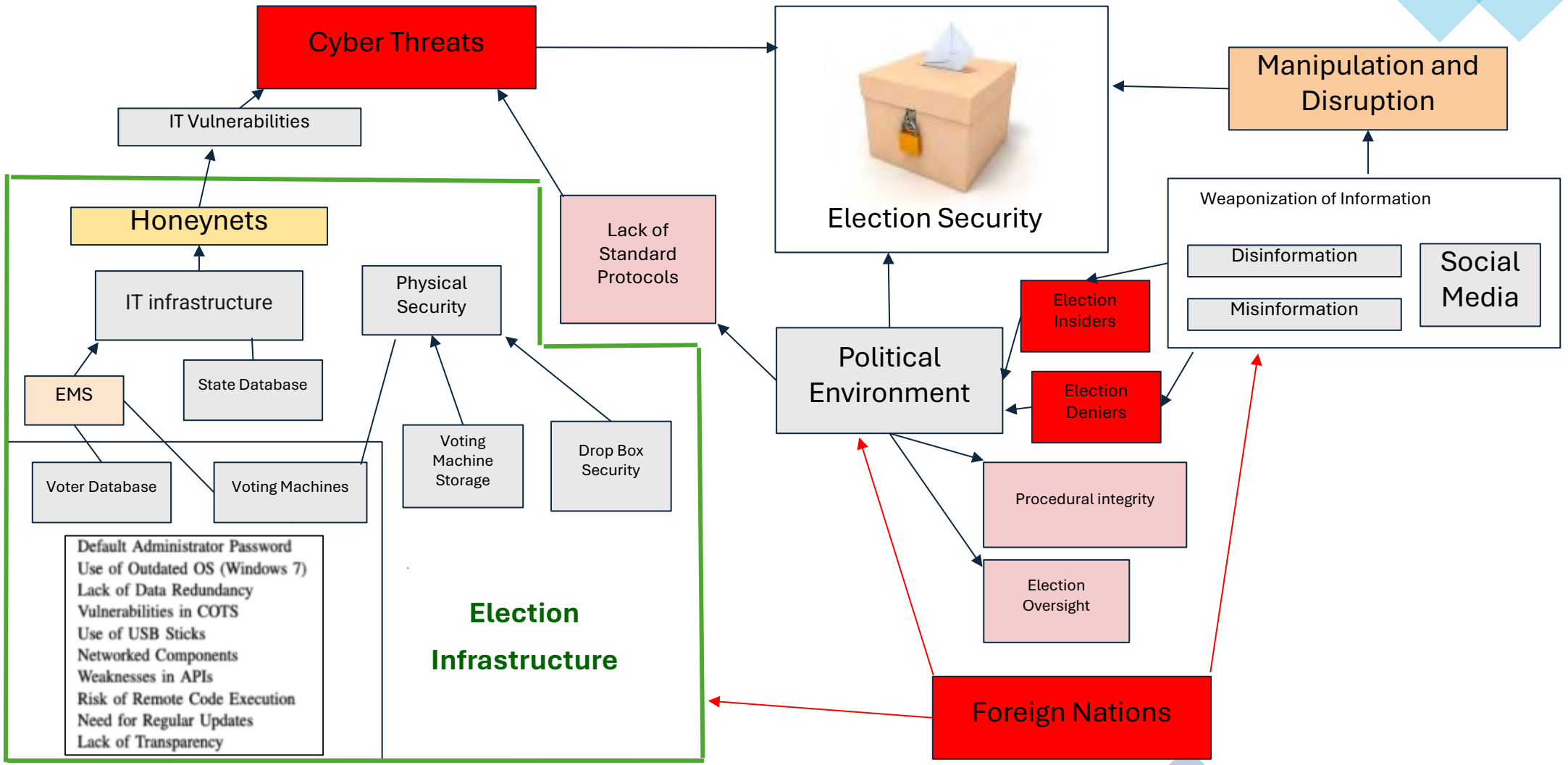
Hacking Voting Machines







The State of Election Security:



```
NAME                STATUS                    PORTS
adbhoney            Up 10 hours (healthy)     0.0.0.0:5555->5555/tcp
ciscoasa            Up 10 hours               0.0.0.0:5000->5000/udp, 0.0.0.0:8443->8443/tcp
citrixhoneypot      Up 10 hours               0.0.0.0:443->443/tcp
conpot_guardian_ast Up 10 hours (healthy)     0.0.0.0:10001->10001/tcp
conpot_iec104       Up 10 hours (healthy)     0.0.0.0:161->161/udp, 0.0.0.0:2404->2404/tcp
conpot_ipmi         Up 10 hours (healthy)     0.0.0.0:623->623/udp
conpot_kamstrup_382 Up 10 hours (healthy)     0.0.0.0:1025->1025/tcp, 0.0.0.0:50100->50100/tcp
cowrie              Up 10 hours               0.0.0.0:22-23->22-23/tcp
ddospot             Up 10 hours               0.0.0.0:19->19/udp, 0.0.0.0:53->53/udp, 0.0.0.0:123->123/udp, 0.0.0.0:1900->1900/udp
dicompot            Up 10 hours               0.0.0.0:11112->11112/tcp
dionaea             Up 10 hours (healthy)     0.0.0.0:20-21->20-21/tcp, 0.0.0.0:42->42/tcp, 0.0.0.0:81->81/tcp, 0.0.0.0:135->135/tcp, 0.0.0.0:445->445/tcp, 0.0.0.0:1433->1433/tcp, 0.0.
0.0:1723->1723/tcp, 0.0.0.0:1883->1883/tcp, 0.0.0.0:3306->3306/tcp, 0.0.0.0:27017->27017/tcp, 0.0.0.0:69->69/udp
elasticpot          Up 10 hours               0.0.0.0:9200->9200/tcp
elasticsearch       Up 10 hours (healthy)     127.0.0.1:64298->9200/tcp
ewsposter           Up 10 hours
fatt                Up 10 hours
heralding           Up 10 hours               0.0.0.0:110->110/tcp, 0.0.0.0:143->143/tcp, 0.0.0.0:465->465/tcp, 0.0.0.0:993->993/tcp, 0.0.0.0:995->995/tcp, 0.0.0.0:1080->1080/tcp, 0.0.
0.0:5432->5432/tcp, 0.0.0.0:5900->5900/tcp
honeytrap           Up 10 hours
ipphoney            Up 10 hours               0.0.0.0:631->631/tcp
kibana              Up 10 hours (healthy)     127.0.0.1:64296->5601/tcp
logstash            Up 10 hours (healthy)
mailoney            Up 10 hours               0.0.0.0:25->25/tcp
map_data            Up 10 hours
map_redis           Up 10 hours
map_web             Up 10 hours               127.0.0.1:64299->64299/tcp
medpot              Up 10 hours               0.0.0.0:2575->2575/tcp
nginx               Up 10 hours
p0f                 Up 10 hours
redishoneypot       Up 10 hours               0.0.0.0:6379->6379/tcp
sentrypeer          Up 10 hours               0.0.0.0:5060->5060/udp
snare               Up 10 hours               0.0.0.0:80->80/tcp
spiderfoot          Up 10 hours (healthy)     127.0.0.1:64303->8080/tcp
suricata            Up 10 hours
tanner              Up 10 hours
tanner_api          Up 10 hours
tanner_phpox        Up 10 hours
tanner_redis        Up 10 hours
```

Honeypot Attacks - Top 10

11,282	9,261	4,056	321	205	171
Ddospot - Attacks	Cowrie - Attacks	Dionaea - Attacks	Tanner - Attacks	Honeytrap - Attacks	Adbhoney - Attacks

89	68	64	32
CitrixHoneypot - Attacks	ConPot - Attacks	Ciscoasa - Attacks	Mailoney - Attacks

Attacks by Honeypot



Attacks - Dynamic

3,305,313 Attacks

7,983 Unique Src IPs

NGINX Events

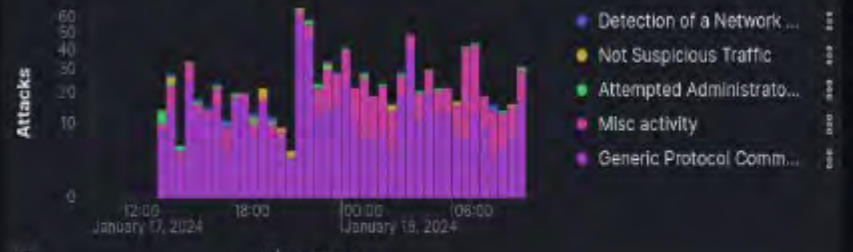
14,698 Events

Attack Map - Dynamic



Suricata Alert Category Histogram

Last 1 day



Honeypot Attacks Bar



Attacker AS/N - Top 10

AS	ASN
14061	DIGITALOCEAN-ASN
45899	VNPT Corp
38136	Akari Networks
140499	Khan Telecom
396982	GOOGLE-CLOUD-PLATFORM

1

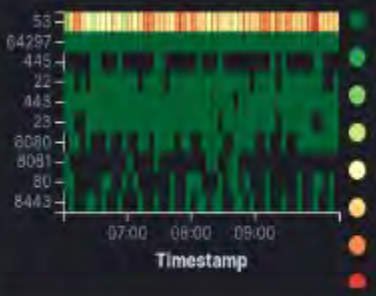
Attacker Source IP - Top 10

Source IP	Count
14.233.187.141	3,154
170.64.153.123	2,051
170.64.214.143	2,045
106.14.166.232	978
34.150.119.172	971

1

Heatmap Destination Ports - Dynamic

Last 4 hours rounded to the hour



Attacks Bar - Dynamic



Password Tagcloud

abc123 (empty) user test 123456 12 root 1 123 admin ubnt data 1234 www

Attacks by Country



P0f OS Distribution



Attacker Src IP Reputation - Dynamic

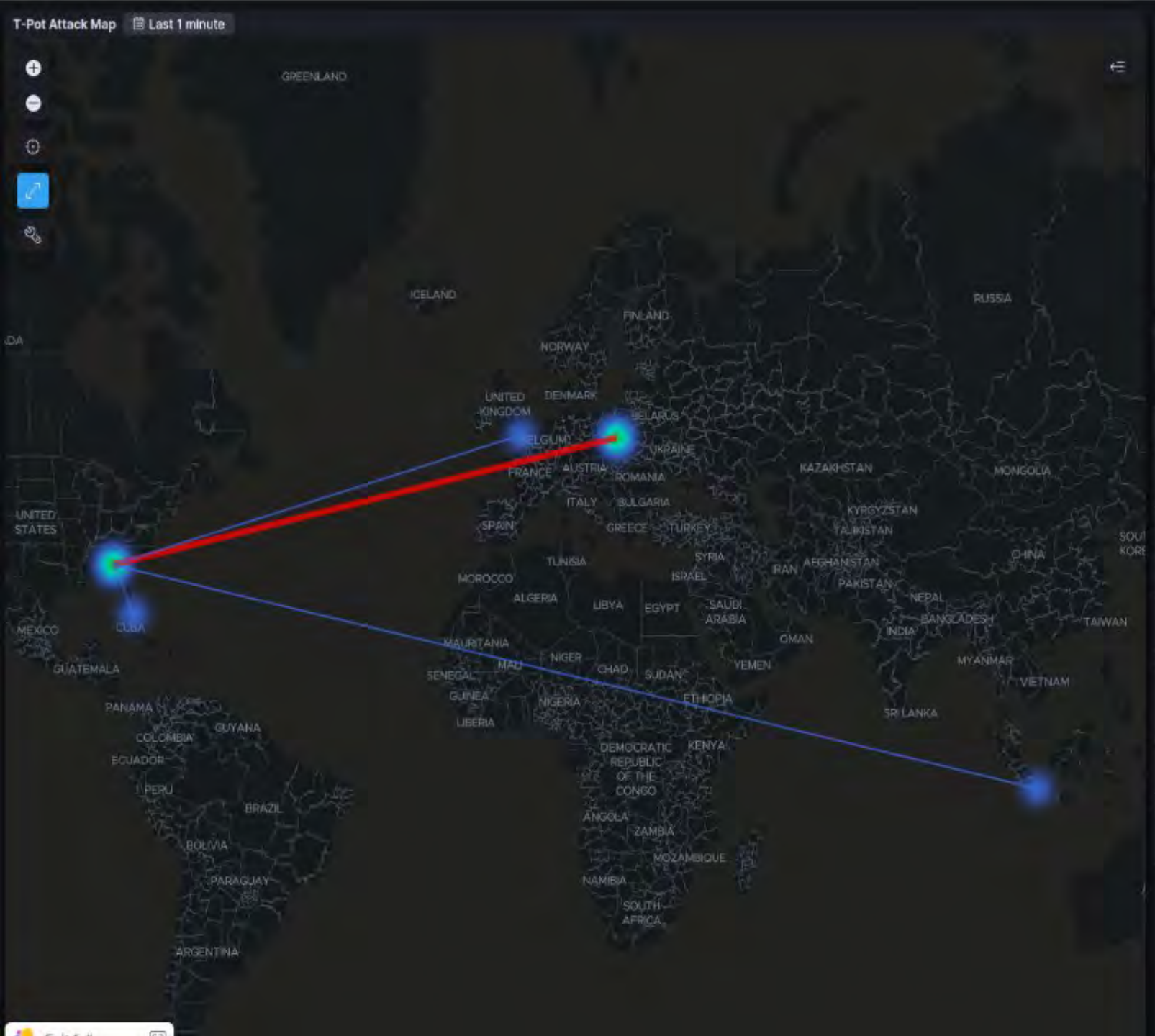


NSM-Logs

3255733 documents

1 field sorted

@timestamp	Document
Jan 18, 2024 @ 10:19:48.578	Type Suricata @timestamp Jan 18, 2024 @ 10:19:48.578 @versio n 1 dest_ip 12.13.141.253 DestPort 53 dns_id 61,928 dns.rrnam e s1 dns_rrtype ANY dns.tx_id 162 dns.type query event_typ…
Jan 18, 2024 @ 10:19:48.548	Type Suricata @timestamp Jan 18, 2024 @ 10:19:48.548 @versio n 1 dest_ip 12.12.141.253 DestPort 53 dns_id 61,928 dns.rrnam e s1 dns_rrtype ANY dns.tx_id 877 dns.type query event_typ…



Last 1 minute

6
Attacks

Last 1 hour

1,648
Attacks

Last 1 day

25,638
Attacks

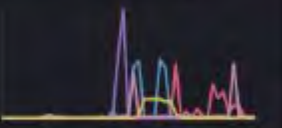
Attacks Last 1 day



Ports Last 1 day



Countries Last 1 day



T-Pot Attack Log Last 1 minute

6 documents

Columns 1 field sorted

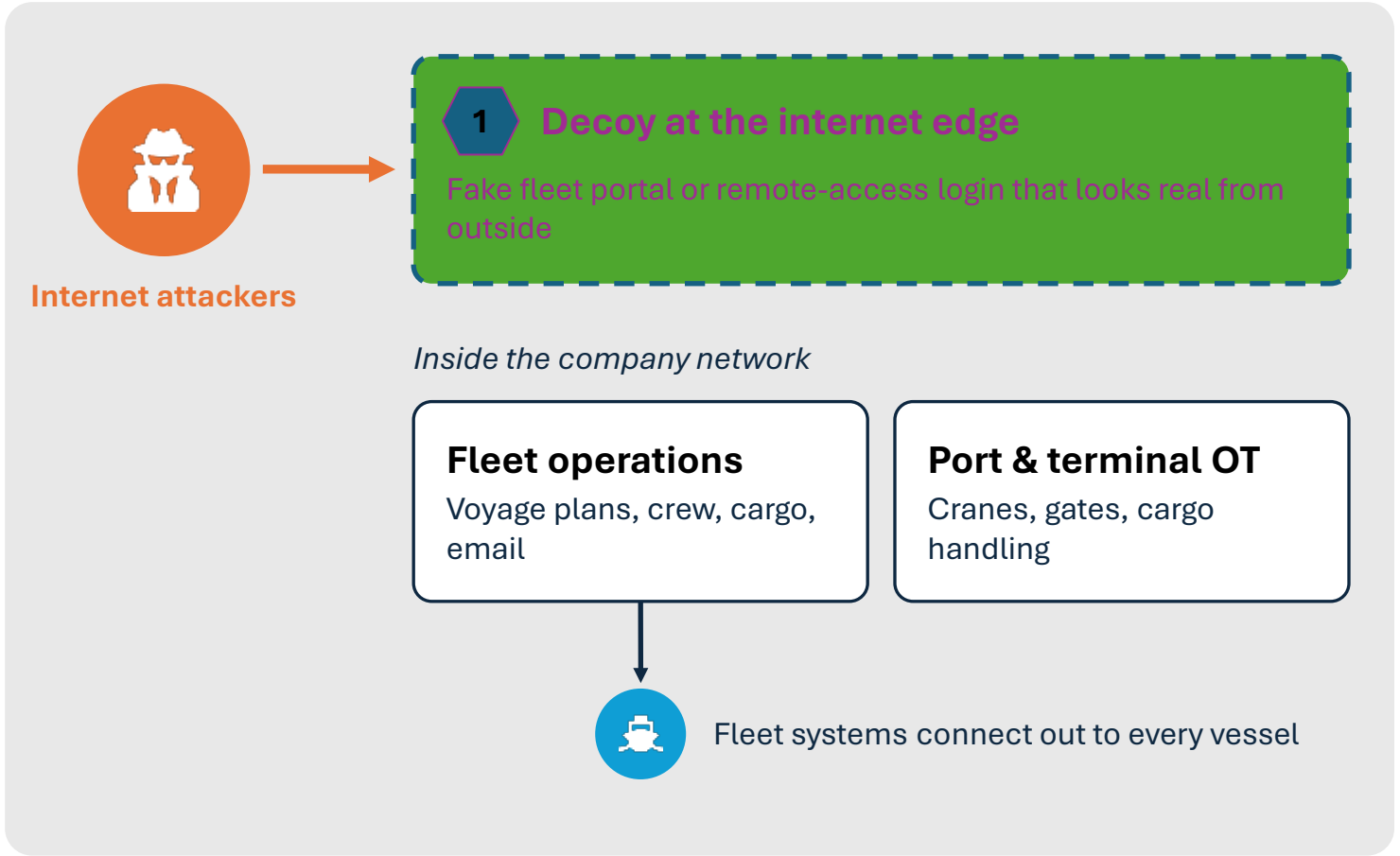
@timestamp	T-Pot Hostn...	Type	DestPort	Country
Jan 18, 2024 @ 10:20:07.090	giganticvolcano	Cowrie	23	GB
Jan 18, 2024 @ 10:20:05.738	giganticvolcano	Ddospot	53	PL
Jan 18, 2024 @ 10:19:56.982	giganticvolcano	Ddospot	53	US
Jan 18, 2024 @ 10:19:53.428	giganticvolcano	Ddospot	53	ID
Jan 18, 2024 @ 10:19:36.876	giganticvolcano	Ddospot	53	PL
Jan 18, 2024 @ 10:19:17.130	giganticvolcano	Ddospot	53	PL

Maritime Security

ZONE 1 · SHORE

Shore: catch attackers at the internet edge

Company HQ, fleet operations and the port all face the internet, and fleet systems reach every ship



Why put a decoy here

1 First thing attackers find

Fleet portals and remote-access logins sit on the open internet, so scanners reach them first.

2 Warning before a ship is hit

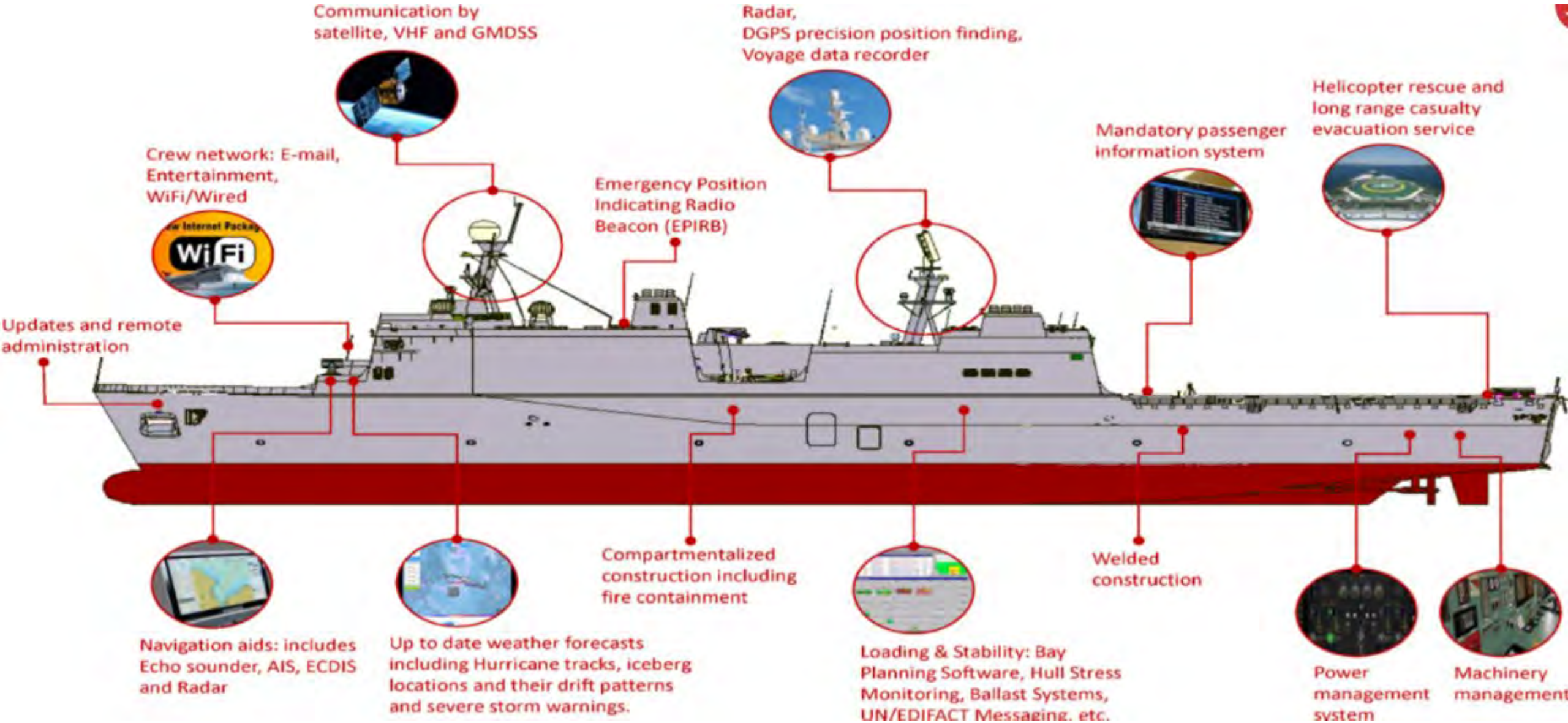
A touch on the decoy flags an intruder before they can pivot through fleet servers to vessels.

3 See what they are after

Logged attempts show which logins, ports and maritime services are being targeted.

Real system Decoy (honeypot)

Deceptive Maritime Security





HONEYNETS

Virginia Honeynet Chapter?

Explorations in Computing

DNA for Security

Consideration of memory, power and heat

Reverse Engineering

Offering new security countermeasures through technology shift

Humanity will generate an estimated 33 zettabytes of data by 2025—that's 3.3 followed by 22 zeros. DNA storage can squeeze all that information into a ping-pong ball! (ScientificAmerican.com)

Workforce Development


Pentesting
CiSO
Pentester



Skills

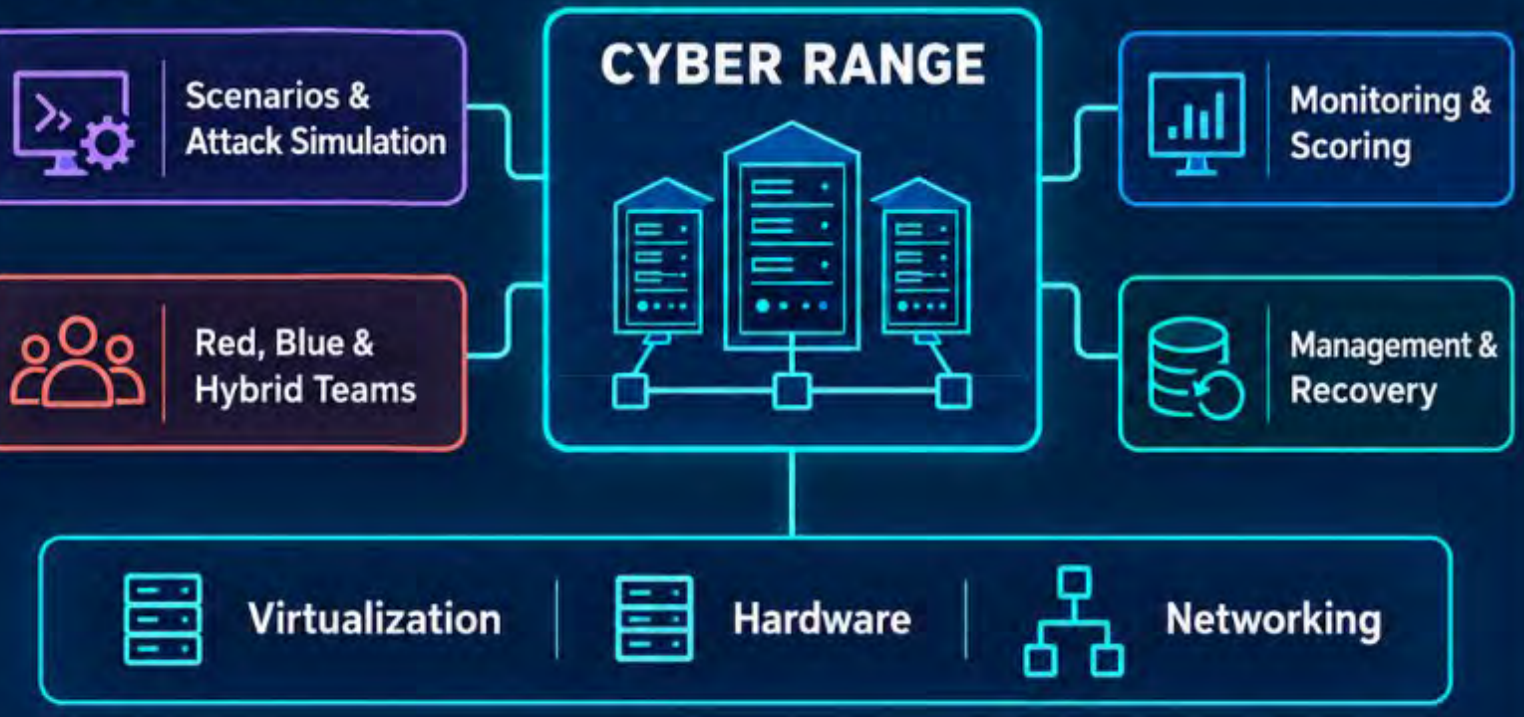
Experience

Earn As You Learn

Cyber Ranges for Research, Education & Training

Realistic environments for experimentation, skills development and defense validation

Core capabilities



RESEARCH

- Vulnerability analysis
- Test and validate defenses

EDUCATION & TRAINING

- Hands-on learning
- Team exercises and CTF competitions

EMERGING ENVIRONMENTS

- Maritime and industrial systems
- Smart grids, vehicles and wireless networks

OPPORTUNITIES FOR COVA CCI COLLABORATION

Shared, affordable access | Open, reusable scenarios | Joint domain-specific testbeds

Security Operations Center (SOC)



Security Operations Center



http://www.cio.co.nz/article/613823/how-build-an-army-cybersecurity-experts/



www.cio.co.nz/article/613823/how-build-an-army-cybersecurity-experts/

Most Visited Getting Started

MENU

CIO FROM IDG

HUAWEI SAP HANA BREAKFAST BRIEFING'S
▶ Motivate / Experience / Implement
Auckland 27 March 2017 | Christchurch 29 March 2017 | Wellington 31 March 2017
Register

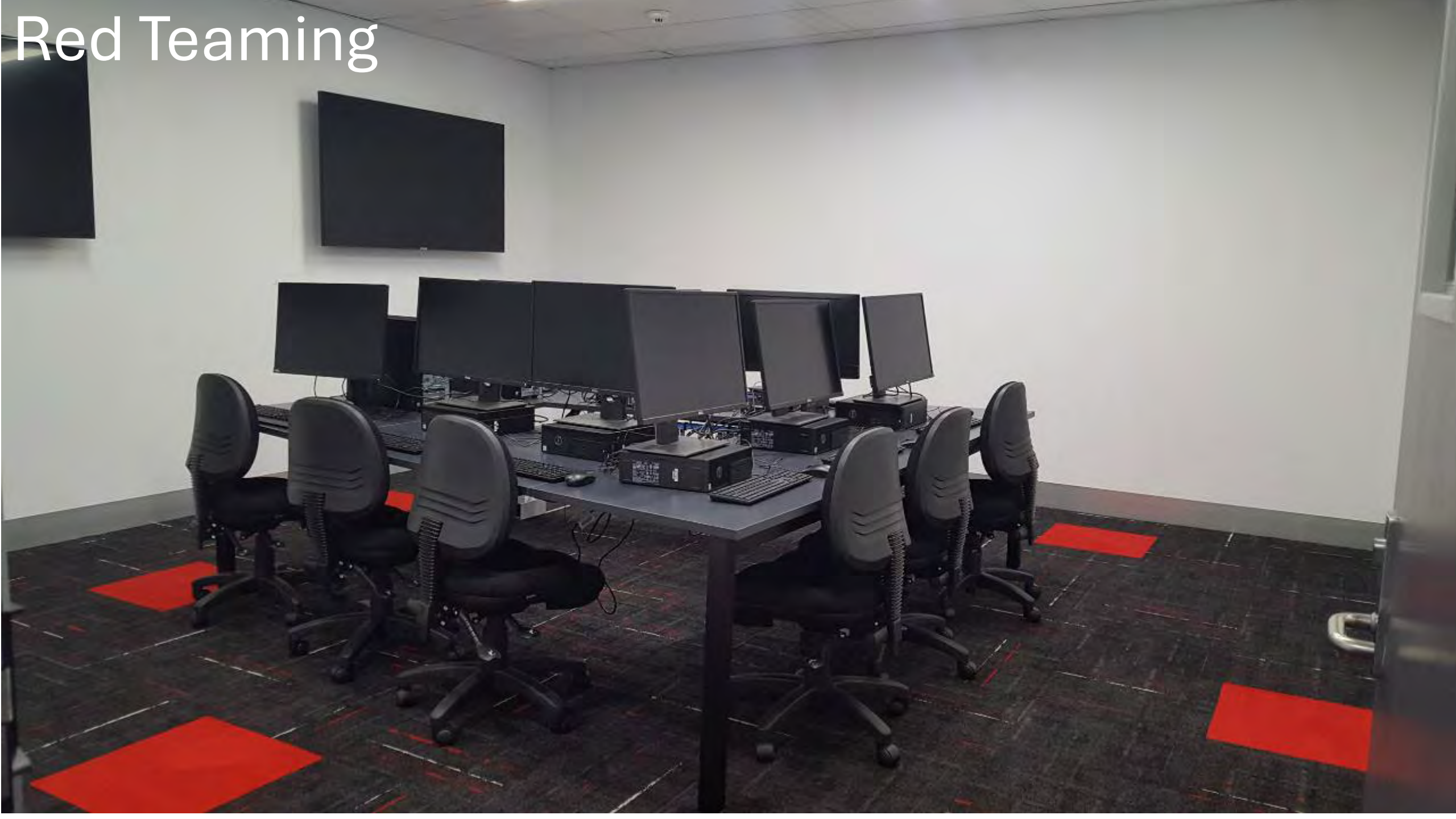
How to build an army of cybersecurity experts

Dr Hossein Sarrafzadeh of Unitec has a game plan for developing the next generation of cybersecurity experts across New Zealand



Divina Paredes (CIO New Zealand)
09 February, 2017 06:30

Red Teaming




Thank you