
CDeX
MASTER
YOUR
CYBER SKILLS

DO YOU FEEL SAFE?

INTERNET CRIMES CAUSED $1.42 BILLION LOSSES IN 2017.

Source: FBI/IC3/US Department of Justice

THE FINANCIAL DAMAGE CAUSED BY A DATA BREACH HAS SPIKED BY MORE THAN 6 PERCENT SINCE 2017 AND NOW COSTS COMPANIES AN AVERAGE OF $3.86 MILLION EACH.

Source: Cost of a Data Breach Report 2018 IBM Security/Ponemon Institute LLC

WORLDWIDE IT SECURITY SPENDING WILL REACH $1.5 BILLION IN 2018.

Source: Gartner

THE QUICKER A BREACH CAN BE DEALT WITH, THE LOWER THE COST TO REPAIR THE DAMAGE.

COMPANIES THAT CONTAINED A BREACH IN LESS THAN 30 DAYS SAVED OVER $1 MILLION AS COMPARED TO THOSE THAT TOOK MORE THAN 30 DAYS TO RESOLVE.

Source: Cost of a Data Breach Report 2018 IBM Security/Ponemon Institute LLC/nbcnews.com

THE KEY COST SAVER IS HAVING AN INCIDENT RESPONSE TEAM READY TO ACT.


A HIGHLY SKILLED
CYBER SECURITY TEAM
IS YOUR
BEST WEAPON.

WHAT'S THE RESPONSE?

CYBER DEFENCE EXERCISE PLATFORM

A unique, hands-on cyber security training system, which helps to boost your incident response team performance in simulated cyber attacks.

Fully adaptable Cyber Security Lab
On-demand & cost-effective solution
Hyper-realistic environment

Hands-on, real time training
Rich training scenarios
Own scenarios development tool

Advanced customization tools
Team performance evaluation
Azure cloud deployment

SIMULATE.
DETECT.
RESPOND.
EVALUATE.

Train your team in simulated cyber attacks with multiple complexity scenarios to increase real life capability.

HOW DOES IT WORK?

COLLECTIVE TRAINING
BLUE VERSUS RED TEAM

Skills developed

- Cognition needs
- Integration
- Communication – how to properly pass information
- Team work
- Acting under time pressure

Scenarios simulated

- DMZ
- Internal Servers
- Office
- Finance
- Developers
- Admin Network
- Windows – Exchange attacks
- Windows – Active Directory attacks
- Windows – Client Side attacks
- Windows – Backdooring
- Linux – Attacks on DNS
- Linux – Attacks on network services

AUTOMATED TRAININGS
BLUE TEAM MEMBER

Skills developed

- Detecting cyber attacks
- Detecting non-standard behaviours
- Responding to incidents
- Counteracting of data leaks and thefts
- Acting under time pressure

WE FOCUS ON


MILITARY & DEFENCE


GOVERNMENTS


WATER & ENERGY

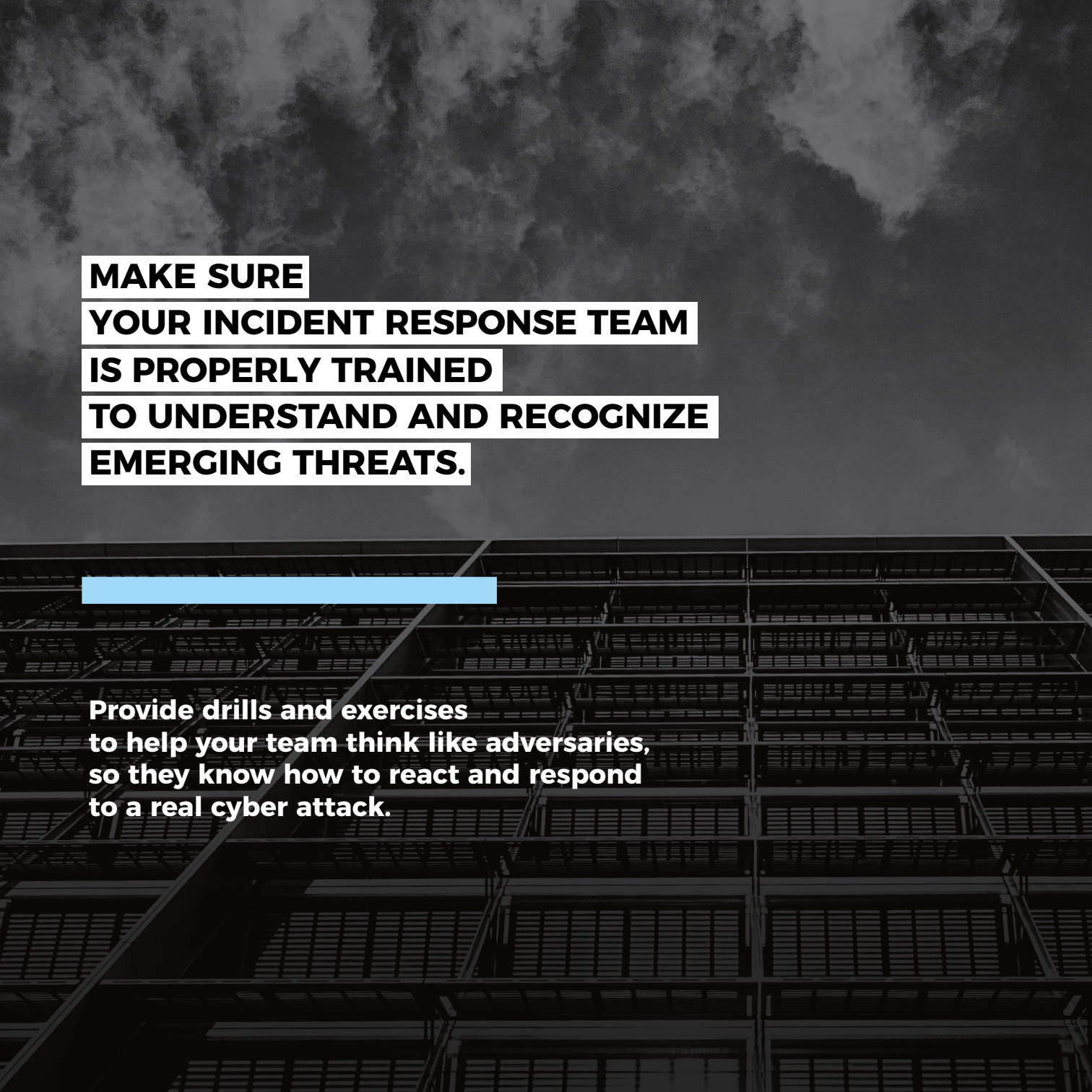

LOGISTICS
MAERSK
MAERSK SEALAND


ICT SECTOR


HUMAN RESOURCES

Protecting data, services & infrastructure
Discovering weak points in the IT ecosystem
Sharpening skills
Shortening reaction time
Developing internal IT procedures
Developing company wide procedures
Training team communication
Forensic & post breach analysis
Vulnerability assessment
Keeping cyber-warriors in shape

SOC Analyst
Malware Analyst
Incident Responder
Cyber Security Service/PM
Forensic Analyst
Penetration Tester
Security administrator & Engineer
Network administrator
Windows/Linux administrator



MAKE SURE YOUR INCIDENT RESPONSE TEAM IS PROPERLY TRAINED TO UNDERSTAND AND RECOGNIZE EMERGING THREATS.

Provide drills and exercises to help your team think like adversaries, so they know how to react and respond to a real cyber attack.

WHAT YOU GAIN?

TECHNICAL

- 24/7 & worldwide platform access
- Azure cloud deployment
- Flexible and scalable working environment

BUSINESS & MANAGEMENT

- Evaluation & motivation tool – performance reports right after the training
- Development tool – strengthening team work & capabilities within cyber defence scope
- Constant knowledge & capability review of the cyber defence team

CYBER SECURITY

- Testing new solutions and configuration changes in a realistic environment
- In-depth individual cyber security training
- Improving technical skills, communication and procedures in the cyber defence team

vectorsynergy

Awarded with
2016 NCI Agency Innovation Challenge
Top 10 Innovators

OUR PARTNERS

Large Tech Companies

Polish Naval Academy

Innovative Startups Community

Vector Synergy Sp. z o.o.
ul. Marcelińska 90, 60-324 Poznań, Poland
e-mail: cdex@vectorsynergy.com
phone: +48616670744