Blue Team Level 1 Certification (Standard)

3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

○ TI1) Introduction to Threat Intelligence
● 7 Topics

○ TI2) Threat Actors & APTs
● 6 Topics | 2 Quizzes

○ TI3) Operational Threat Intelligence
● 7 Topics | 1 Quiz

○ TI4) Tactical Threat Intelligence
● 7 Topics | 1 Quiz

○ TI5) Strategic Threat Intelligence
● 5 Topics | 1 Quiz

○ TI6) Malware and Global Campaigns
● 6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

○ DF1) Introduction to Digital Forensics
● 5 Topics

○ DF2) Forensics Fundamentals
● 10 Topics | 5 Quizzes

○ DF3) Digital Evidence Collection
● 8 Topics | 1 Quiz

○ DF4) Windows Investigations
● 3 Topics | 3 Quizzes

○ DF5) Linux Investigations
● 4 Topics | 2 Quizzes

○ DF6) Volatility
● 3 Topics | 1 Quiz

○ DF7) Autopsy
● 4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

○ SI1) Introduction to SIEM
● 7 Topics | 1 Quiz

○ SI2) Logging
● 6 Topics | 2 Quizzes

○ SI3) Aggregation
● 2 Topics | 1 Quiz

○ SI4) Correlation
● 6 Topics | 1 Quiz

○ SI5) Using Splunk
● 5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

○ IR1) Introduction to Incident Response
● 8 Topics | 1 Quiz

○ Section Introduction, Incident Response
○ What is Incident Response?
○ Why is Incident Response Needed?
○ Security Events vs Security Incidents
○ Incident Response Lifecycle (NIST SP 800 61r2)
○ CSIRT and CERT Explained

CSIRT and CERT Explained

Blue Team Level 1 Certification (Standard) > IR1) Introduction to Incident Response > CSIRT an... IN PROGRESS

With the number of cyber-attacks that happen daily, many companies and governmental bodies needed to develop a team of specialized individuals that could respond to these attacks. That is where the Cyber Emergency Response Team (CERT) or Cyber Security Incident Response Team (CSIRT) was introduced. Their core responsibilities are coordinating and responding to IT security incidents and determining how these incidents can impact the organization or government entity. CSIRTs often contain key stakeholders from different business units, such as; infrastructure, networking, legal and public relations, communications, security, and more, providing the CSIRT the ability to address all aspects of the company in an emergency.

WHY ARE THEY IMPORTANT?

CSIRTs are important because they provide vital functions in our digital world. For most businesses, this is divided into:

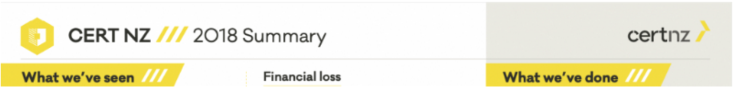
- Having a central communication point or command center where all incident information is handled.
- Promotes Security Awareness and Training (Such as Phishing Exercises) for a company.
- Act as the emergency contact group for an organization in all things related to cybersecurity.
- Investigating new security vulnerabilities and threats and develop plans to mitigate and respond to these incidents if exploited at their company.
- Determine the MTTR & MDT for a company's assets.
- Provide useful information to other CSIRTs and the Cyber Security community.

PUBLIC vs. PRIVATE

Since the creation of CERTs and CSIRTs, a lot of confusion has surrounded how they are named. Many organizations tend to use different names such as CERT, Security Incident Response Team (SIRT), Incident Response Team (IRT), or Computer Security Incident Response Centre (CSIRC), but they all describe an organization that has the same goals. The term CERT has often been used to describe teams in countries such as Australia (AusCERT), Brazil (CERT.br), New Zealand (CERTNZ), South Korea (KrCERT), the United Kingdom (CERT-UK) and the United States (US-CERT). The term CSIRT is more often associated with teams that businesses adopt for internal cybersecurity breaches and not designated as nationally recognized response teams.

CASE STUDY: NEW ZEALAND CERT

Since CERTs started to develop in the early 2000s, most developed countries contain some type of government-sponsored CERTs. The goal of these CERTs are to protect business and individuals in their home country, as well as helping other CERTs respond to incidents where their people could be affected. Many of these CERTs try to maintain visibility to the public and publish quarterly and annual reports on both the activity that was reported and what they have done to respond to issues. A great example of this is the New Zealand CERT. They publish annual reports that detail incidents that they saw for that year, as well as ways they responded to them. Below is an example of an infographic on their website:



○ Further Reading Material, Incident Response

○ Incident Response Glossary

Activity) End of Section Review, Incident Response

○ IR2) Preparation Phase

● 10 Topics | 2 Quizzes

○ IR3) Detection and Analysis Phase

● 7 Topics | 4 Quizzes

○ IR4) Containment, Eradication, and Recovery Phase

● 5 Topics | 1 Quiz

○ IR5) Lessons Learned and Reporting

● 7 Topics

○ IR6) MITRE ATT&CK

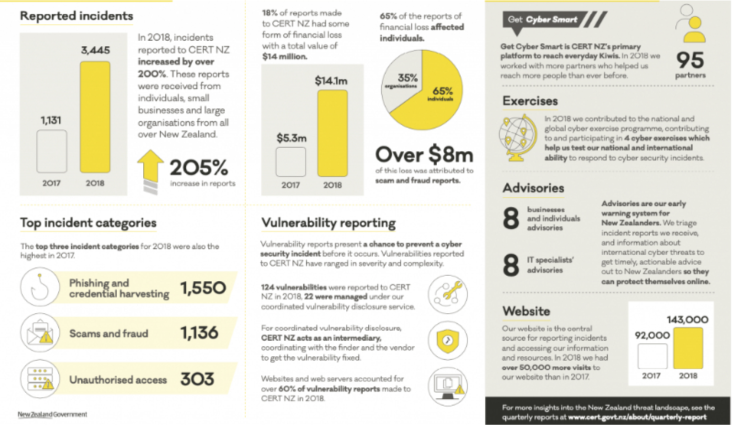
● 13 Topics | 2 Quizzes

BTL1 EXAM

○ Exam Preparation

○ Using RDP and SSH

○ How to Start Your Exam



Reported incidents

In 2018, incidents reported to CERT NZ **increased by over 200%**. These reports were received from individuals, small businesses and large organisations from all over New Zealand.

205%
increase in reports

18% of reports made to CERT NZ had some form of financial loss with a total value of **$14 million.**

65% of the reports of financial loss **affected individuals.**

Over $8m
of this loss was attributed to **scam and fraud reports.**

Top incident categories

The **top three incident categories** for 2018 were also the highest in 2017.

Phishing and credential harvesting	1,550
Scams and fraud	1,136
Unauthorised access	303

New Zealand Government

Vulnerability reporting

Vulnerability reports present **a chance to prevent a cyber security incident** before it occurs. Vulnerabilities reported to CERT NZ have ranged in severity and complexity.

124 vulnerabilities were reported to CERT NZ in 2018, **22 were managed** under our coordinated vulnerability disclosure service.

For coordinated vulnerability disclosure, **CERT NZ acts as an intermediary,** coordinating with the finder and the vendor to get the vulnerability fixed.

Websites and web servers accounted for over **60% of vulnerability reports** made to CERT NZ in 2018.

Get *Cyber Smart* ///

Get Cyber Smart is CERT NZ's primary platform to reach everyday Kiwis. In 2018 we worked with more partners who helped us reach more people than ever before.

95
partners

Exercises

In 2018 we contributed to the national and global cyber exercise programme, contributing to and participating in **4 cyber exercises which help us test our national and international ability** to respond to cyber security incidents.

Advisories

8 businesses and individuals advisories

8 IT specialists' advisories

Advisories are our early warning system for New Zealanders. We triage incident reports we receive, and information about international cyber threats to get timely, actionable advice out to New Zealanders **so they can protect themselves online.**

Website

Our website is the central source for reporting incidents and accessing our information and resources. In 2018 we had **over 50,000 more visits** to our website than in 2017.

For more insights into the New Zealand threat landscape, see the quarterly reports at **www.cert.govt.nz/about/quarterly-report**

< Previous Topic

Mark Complete ✓

Next Topic >

Back to Lesson

Privacy - Terms

Privacy & Cookies Policy