NRD Cyber Security

Улучшение Кибер безопасности на национальном уровне

Romualdas Lečickis

Business Development Director

NRD Cyber Security, Lithuania

Kyrgyzstan 2018-08-29

Cyber Security сегодня

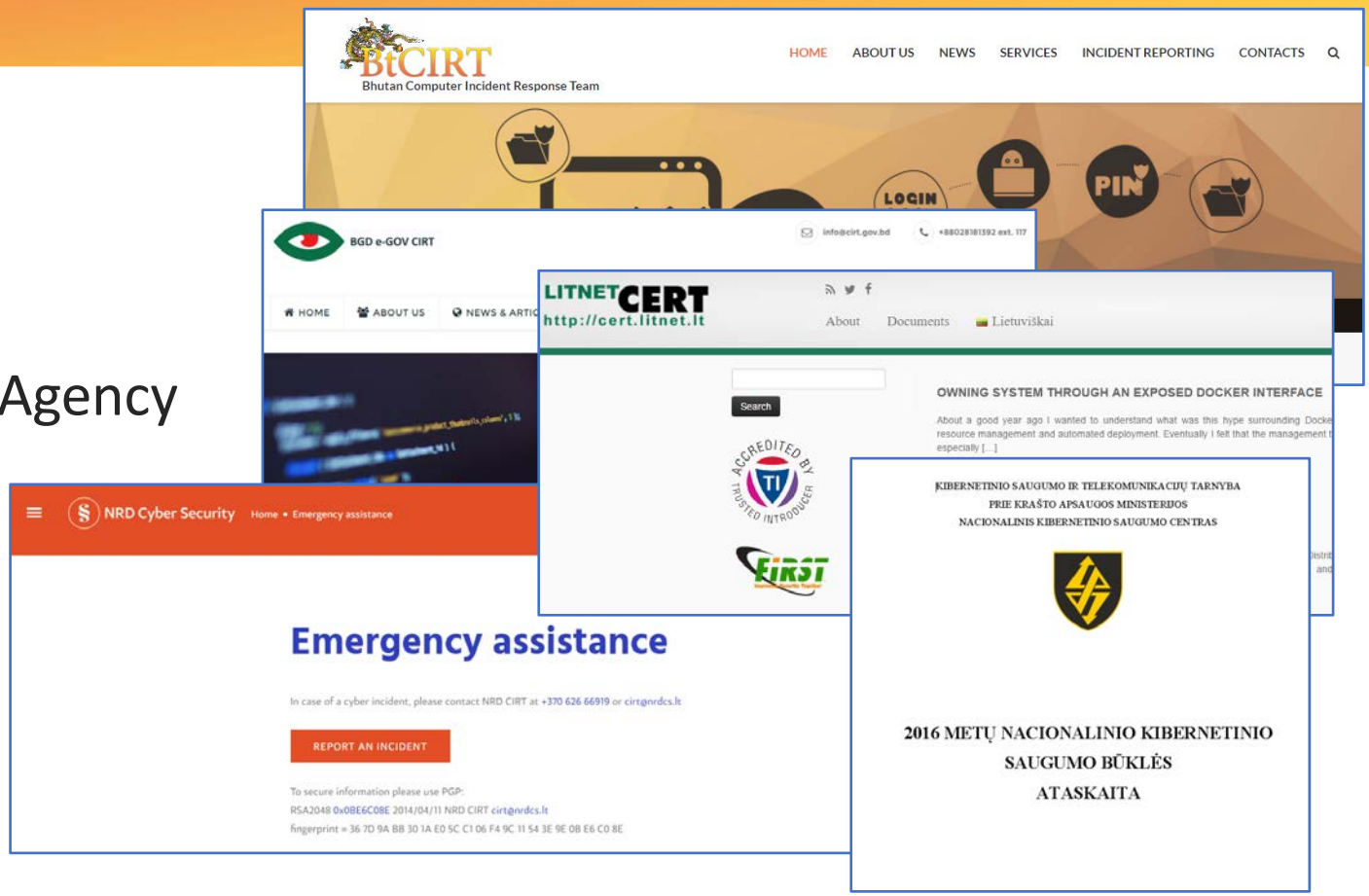
- Нету границ
- Разное правовое регламентирование
- Криминальные группы
- Группы финансируемые другими странами
- Возможность собрать деньги анонимно
- Возможность остаться анонимным

Важно доверие

Каким образом увеличить доверие?

Опыт NRD Cyber Security по созданию CIRT

- National CSIRTs
- Government CSIRT
- Private CSIRT
- Gov. Cyber Security Agency
- Military CIRT
- Academic CIRT



NRD CYBER SECURITY

создание CSIRT / SOC,
технологический консалтинг,
реагирование на инциденты,
прикладные исследования

NRDCS.LT

NRD Cyber Security

Превенция кибер-инцидентов

- Всесторонняя проверка безопасности
- Управление рисками информации и кибербезопасности
- Оценка уязвимости сети и тестирование на проникновение
- Тестирование социальной инженерии
- Мониторинг национальной критической инфраструктуры

Обнаружение и обработка кибер-инцидентов

- Обнаружение кибер-инцидентов
- Установка кибер-датчиков
- Настройка и обслуживание лабораторий Cyber Security
- Аналитика правоохранительных органов и автоматизация разведывательных служб
- Решения для более быстрого проведения судебно-медицинской экспертизы

Создание потенциала

- Создание возможностей CIRT / SOC
- Решения OSINT
- Интеллектуальные решения данных

Управление безопасностью

- Цифровое картографирование экосистем, создание мандатов и отношений
- Эффективное смягчение мошенничества - для защиты от мошенничества
- Критическая методология информационной инфраструктуры

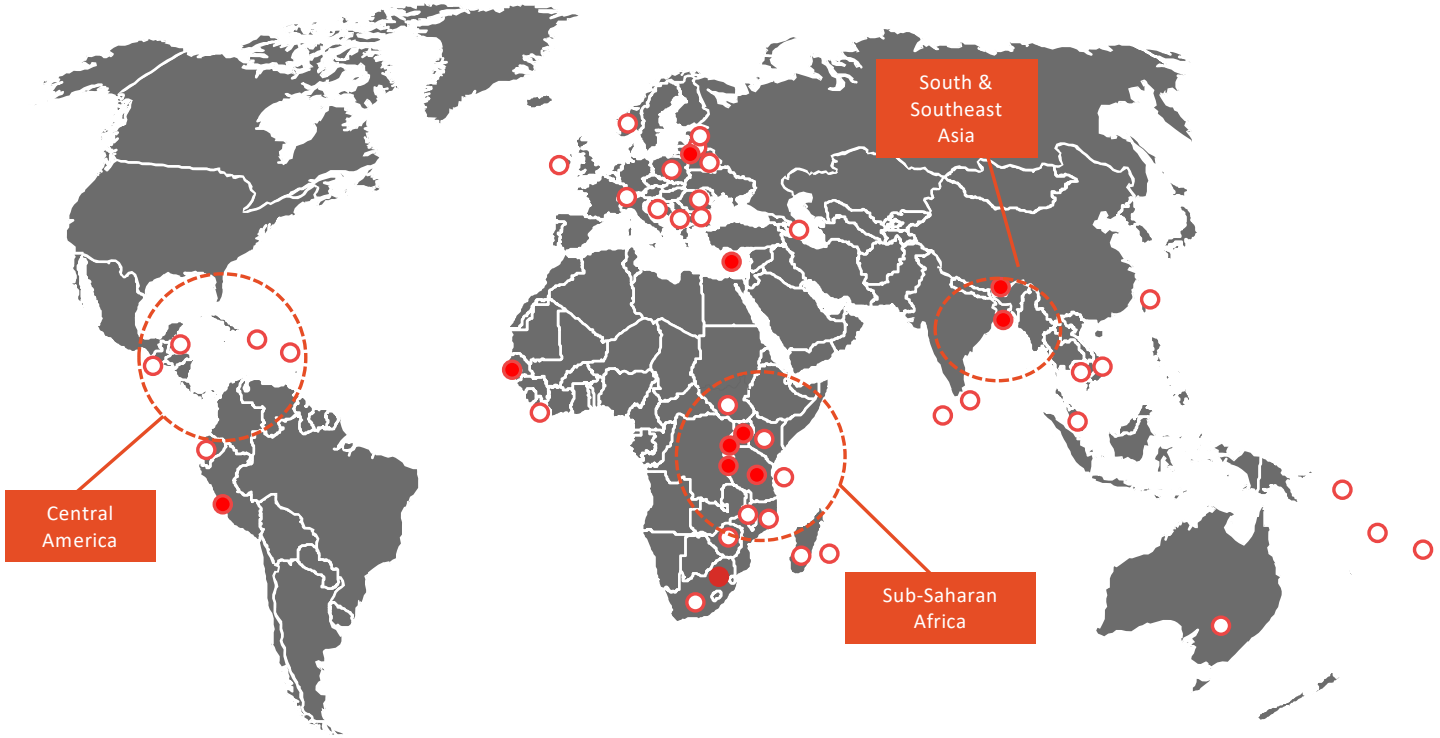
Обучение Cyber Security и Cyber Intelligence

- OSINT
- Аналитика данных

ГЕОГРАФИЯ ПРОЕКТОВ

СОЗДАЕТ ЦЕНТРЫ **КИБЕР БЕЗОПАСНОСТИ** (CSIRTS) НАЧИНАЯ С **1998 ГОДА**

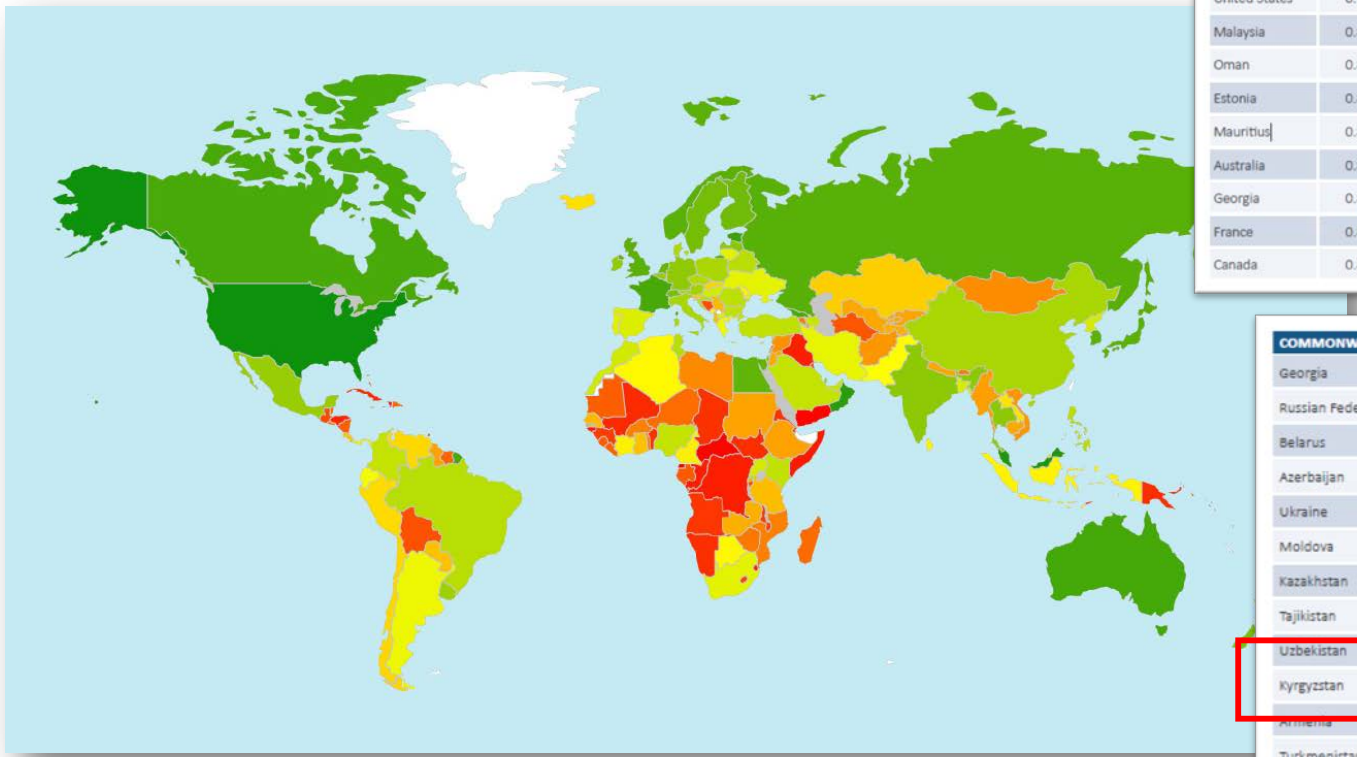
МЕЖДУНАРОДНЫЕ CSIRT/SOC КОМАНДЫ ПРЕДОТВРАЩАЮТ КИБЕР АТАКИ И КИБЕР ПРЕСТУПЛЕНИЯ



NRD Cyber Security контролируется фондом INVL Technology, LTU.
INVL Technology компании внедрили проекты в **50+ странах**.

ПАРТНЕРЫ ПО СОЗДАНИЮ ЦЕНТРОВ КИБЕР-БЕЗОПАСНОСТИ

ITU Global Cybersecurity Index



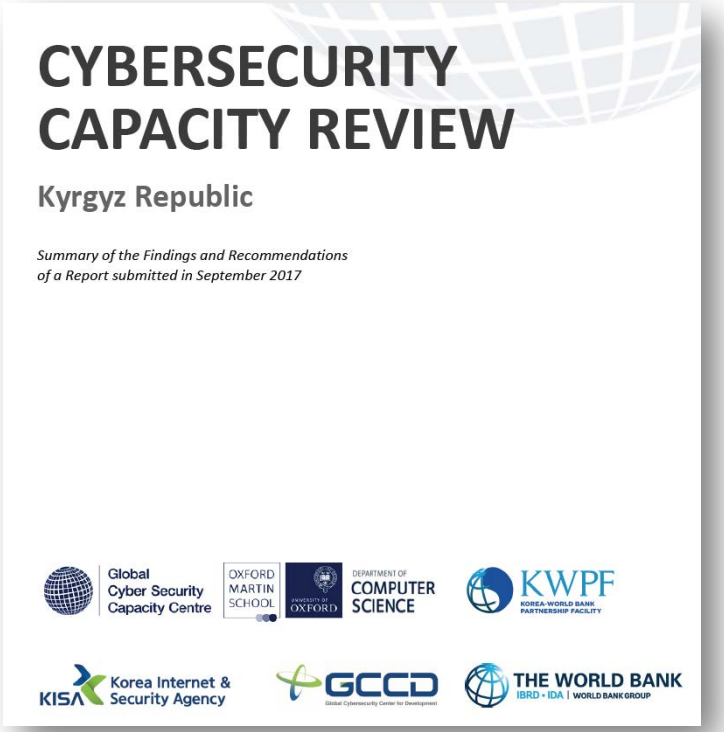
Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

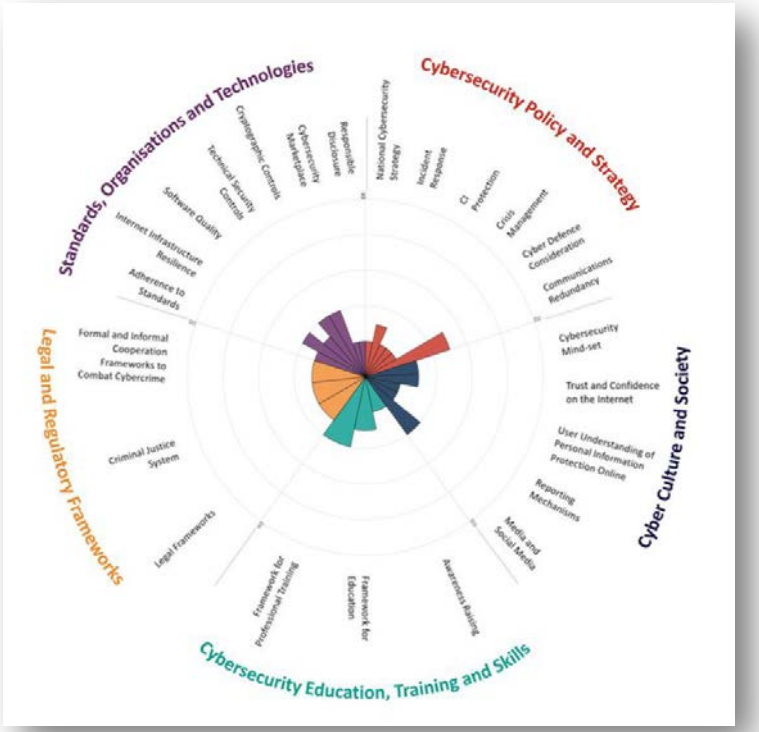
COMMONWEALTH OF INDEPENDANT STATESCIS Region	Score	Global Rank
Georgia	0.819	8
Russian Federation	0.788	10
Belarus	0.592	39
Azerbaijan	0.559	48
Ukraine	0.501	59
Moldova	0.418	73
Kazakhstan	0.352	83
Tajikistan	0.292	91
Uzbekistan	0.277	93
Kyrgyzstan	0.270	97
[illegible]	[illegible]	[illegible]
Turkmenistan	0.133	132

National Cyber Security Index

ncsi.ega.ee/country/bd/

Cybersecurity Capacity Review by Oxford





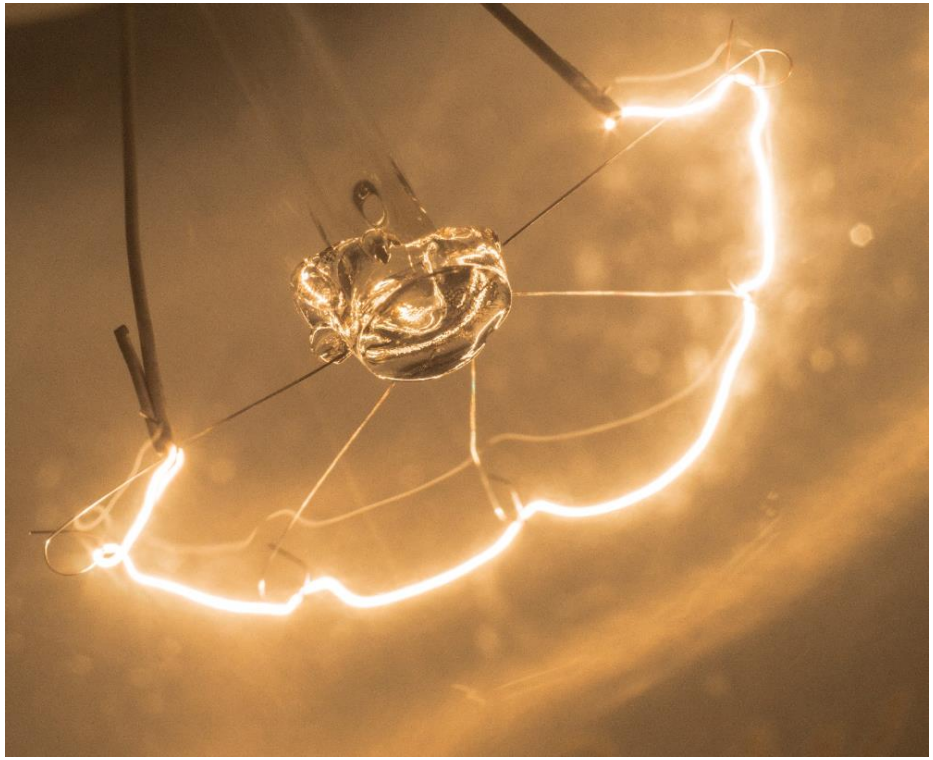
Опыт по улучшению кибер безопасности

1. Разработка Национальной кибер-стратегии
2. Разработка фреймворка по безопасности критической инфраструктуры
3. Внедрение систем сенсоров для обеспечения безопасности
4. Создание CSIRT/SOC команд
5. Создание кибер-лабораторий

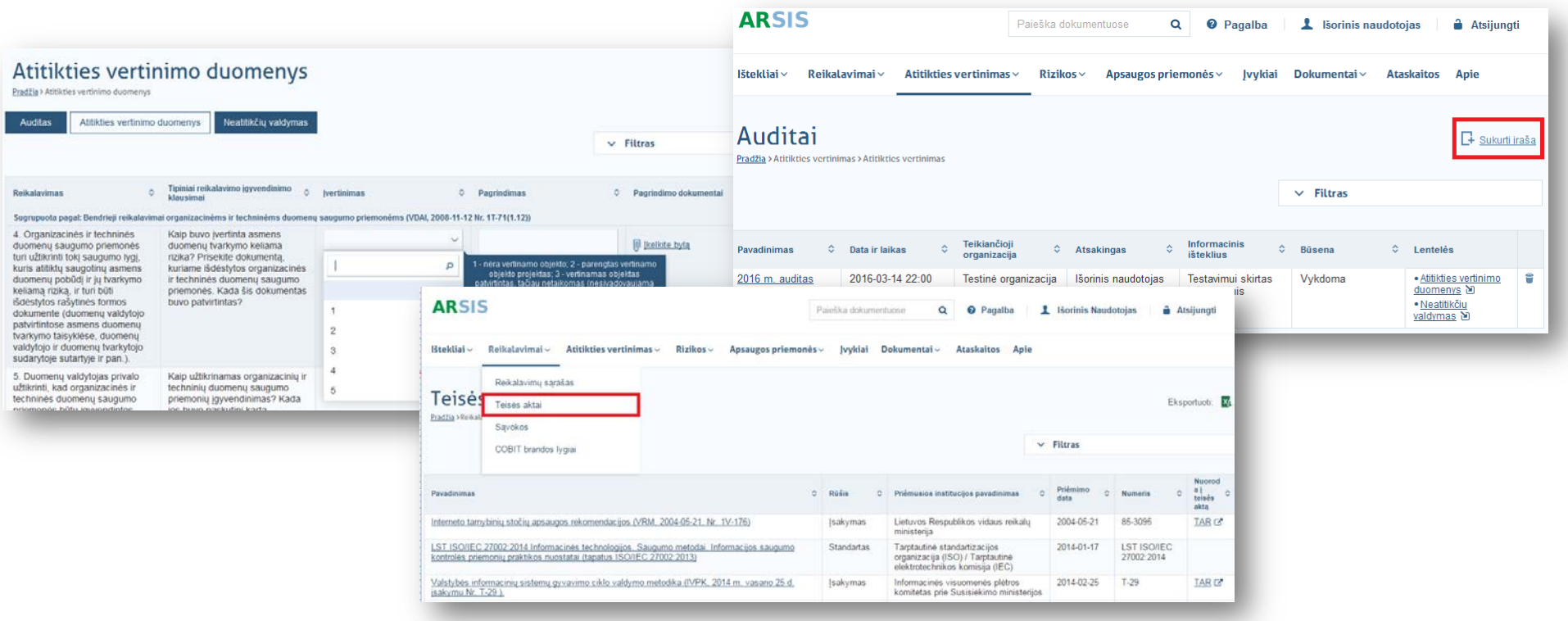
1. Разработка Национальной кибер стратегии

- Понять заинтересованные стороны
- Получить мандат и разделить обязанности
- Обеспечение независимости по разработке политики и осуществлению
- Включение критической инфраструктуры
- Определение роли частного сектора
- Подготовление действующего плана реализации

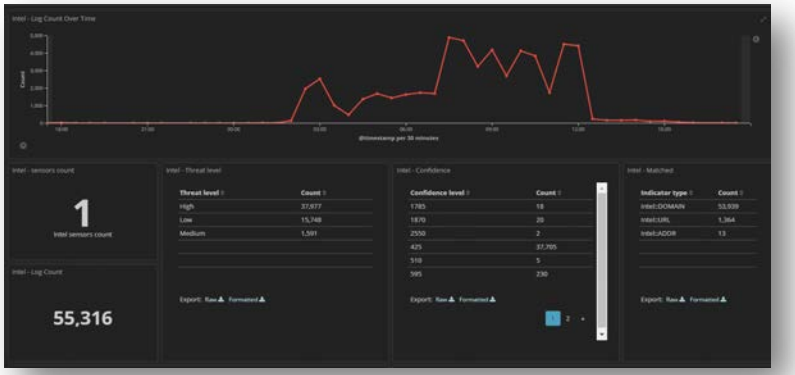
2. Разработка фреймворка по безопасности критической инфраструктуры



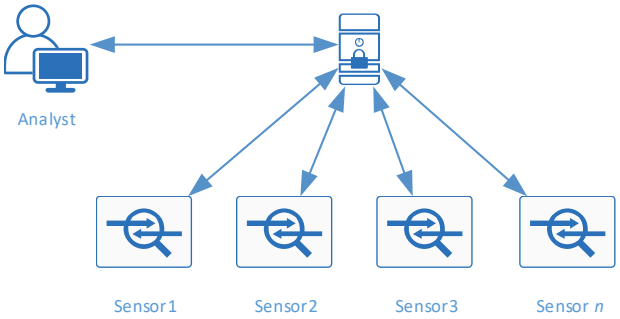
- Определение четкой методики
- Назначение ответственных сторон
- Определение требований для обеспечения безопасности
- Обеспечение поддержки для выполнения требований
- Разработка и внедрение систем оценки риска кибербезопасности
- Постоянный мониторинг

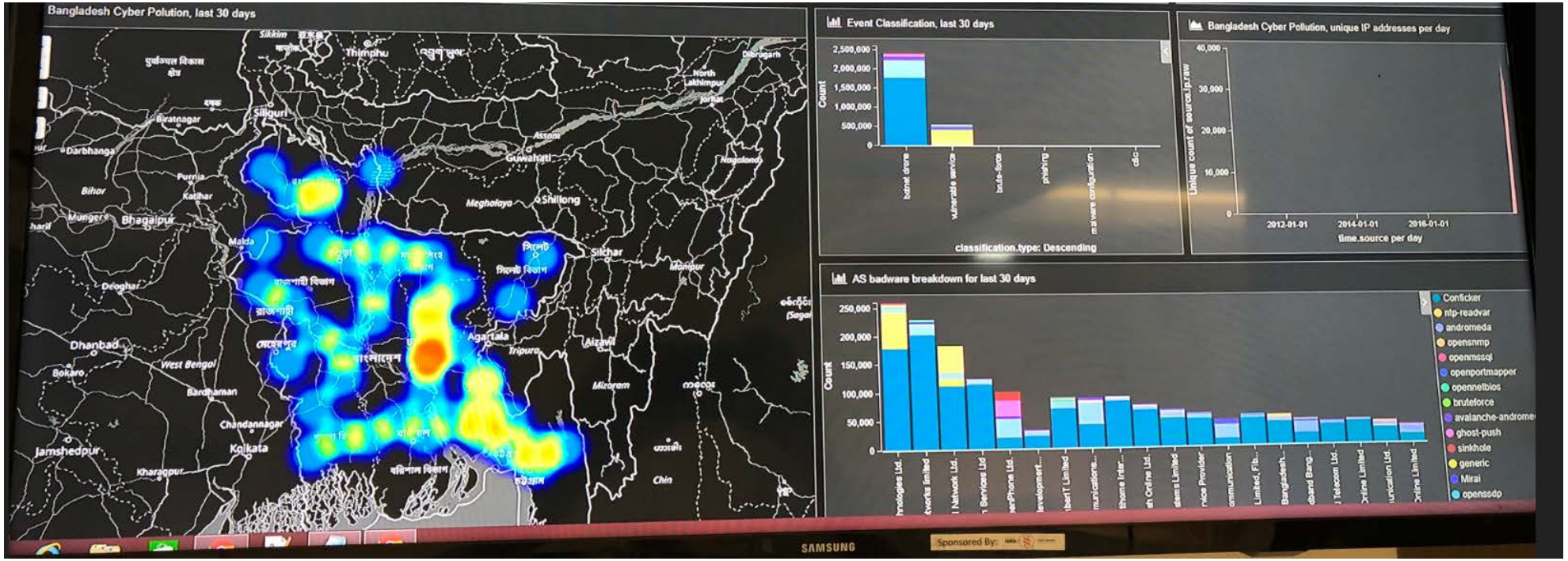

Atitikties vertinimo duomenys
Auditas
Atitikties vertinimo duomenys
Neatitikčių valdymas
Filtras
ARSIS
Paieška dokumentuose
Pagalba
Išorinis naudotojas
Atsijungti
Ištekliai
Reikalavimai
Atitikties vertinimas
Rizikos
Apsaugos priemonės
Įvykiai
Dokumentai
Ataskaitos
Apie
Auditai
Sukurti įrašą
Filtras
Pavadinimas
Data ir laikas
Teikiančioji organizacija
Atsakingas
Informacinis išteklius
Būsena
Lentelės
2016 m. auditas
2016-03-14 22:00
Testinė organizacija
Išorinis naudotojas
Vykdoma
Atitikties vertinimo duomenys
Neatitikčių valdymas
Reikalavimų sąrašas
Teisės aktai
Sąvokos
COBIT brandos lygiai
Eksportuoti
Pavadinimas
Rūšis
Priėmusios institucijos pavadinimas
Priėmimo data
Numeris
Įsakymas
Standartas
TAR

3. Внедрение систем сенсоров для обеспечения безопасности



- Разработка и внедрение датчиков контроля безопасности в критической инфраструктуре и других организациях
- Интеграция различных технологий
- Предоставление обучений и поддержки




Bangladesh Cyber Polution, last 30 days
Event Classification, last 30 days
botnet drone
vulnerable service
brute-force
phishing
malware configuration
ddo
classification.type: Descending
Bangladesh Cyber Pollution, unique IP addresses per day
Unique count of source.ip.raw
2012-01-01
2014-01-01
2016-01-01
time.source per day
AS badware breakdown for last 30 days
Count
Conficker
ntp-readvar
andromeda
opensnmp
openmssql
openportmapper
opennetbios
bruteforce
ghost-push
sinkhole
generic
Mirai
openssdp
SAMSUNG
Sponsored By:

4. Создание CSIRT/SOC команд

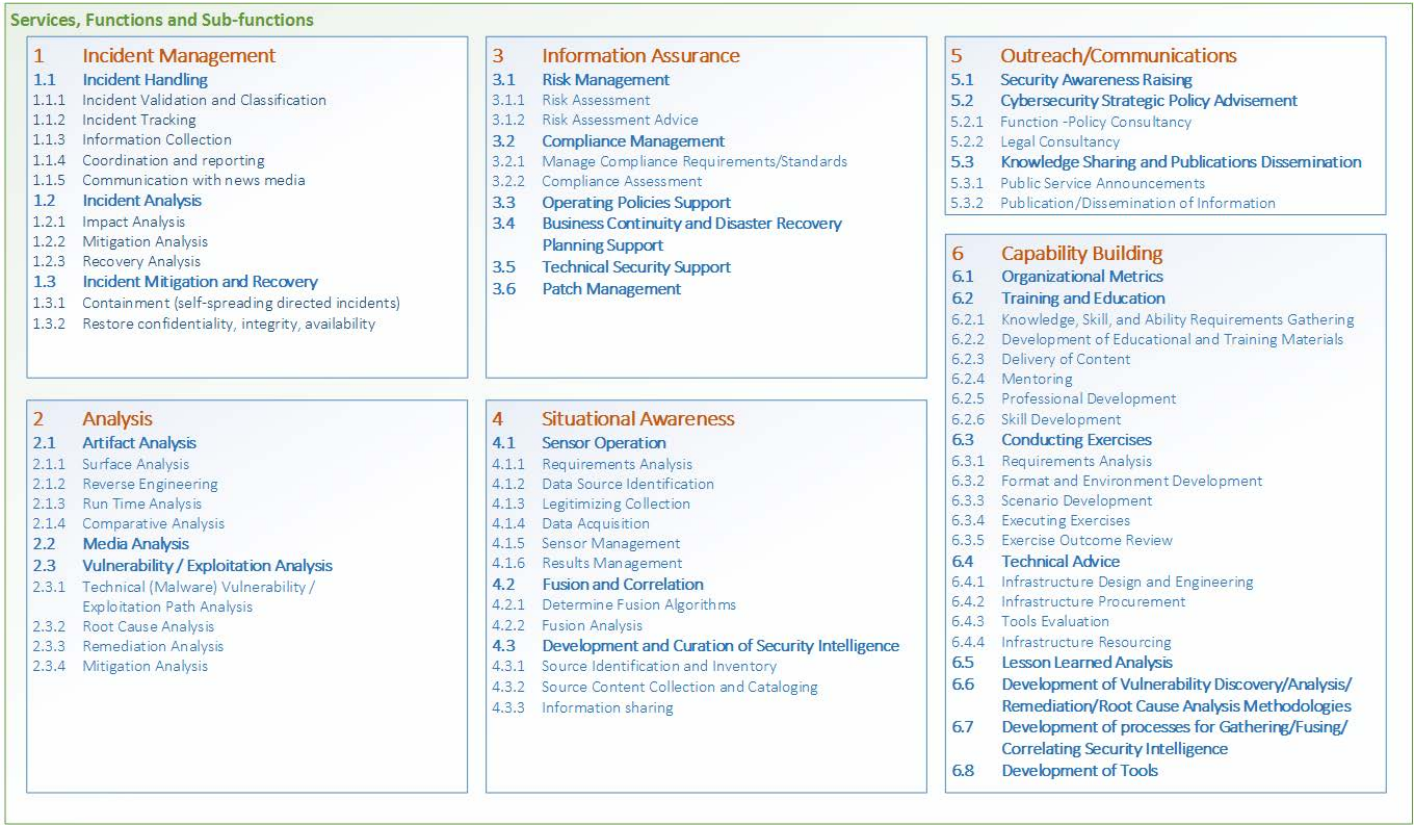
CSIRT / SOC позволяет решать кибер-проблемы на разных уровнях:

- Национальном
- Правительственном
- Отраслевом (банки, энергетика)
- Внутреннем (SOC)
- Частные CSIRT

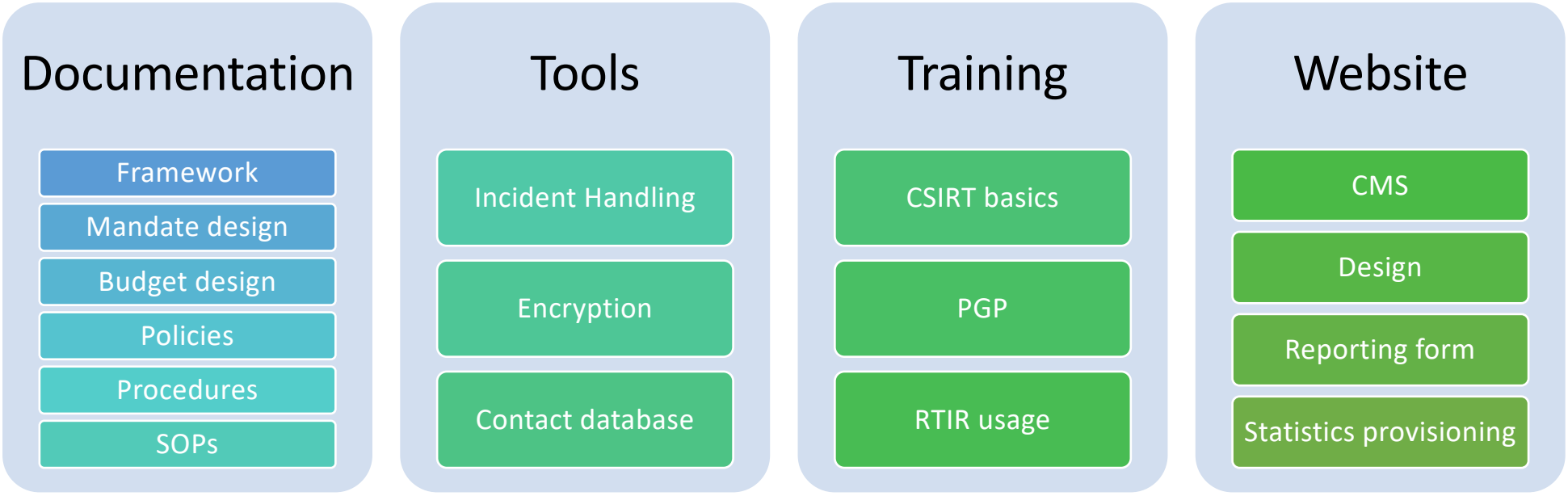
NRD Cyber Security CSIRT/SOC варианты

	Mini	Basic	Effective	Full Scale
Governance	• Mandate definition • FIRST.org membership • Roadmap & Strategy	• Mandate definition • FIRST.org membership • Roadmap & Strategy	• Mandate definition • FIRST.org membership • Roadmap & Strategy • Orgchart buildout	• Mandate definition • FIRST.org membership • Roadmap & Strategy • Orgchart buildout
People	• Featured CSIRT training • Limited remote support	• Relevant CSIRT training • Remote support • SOPs • Study mission tours	• Relevant CSIRT training • Remote support • SOPs • Study mission tours	• Relevant CSIRT training • On-site and remote support • SOPs • Study mission tours
Processes and services	• Incident handling service • Incident handling process	• Incident handling and outreach • Infrastructure support • Standard reporting	• Incident handling, outreach, digital forensics, vulnerability management • Process automation • Infrastructure support • Standard reporting	• Full scale CSIRT/SOC services • Process automation • Automated custom reporting • Maturity progress assessment • Infrastructure support
Measurements	• A few KPIs • No SLAs	• Basic KPIs • SLAs for processes	• KPIs system • SLAs for processes • SIM3 successful audit	• KPIs system • SLAs for services and automation • Annual reviews, SOC-CMM L3 C1.5
Technological Capability	• Incident registration and handling • PGP	• Incident registration and handling • Outreach and visualization portal • Internal support, PGP • Simple vulnerability assessment	• Incident detection and handling • Outreach and visualization portal • Internal support, PGP • Simple vulnerability assessment • Simple video wall • Simple threat intelligence • Simple digital forensics • Simple integration with ex. tooling • Situational awareness	• Incident detection and handling • Outreach and visualization portal • Internal support, PGP • Vulnerability assessment • Video wall • Threat intelligence • Digital Forensics • Integration with existing tooling • Situational awareness and EWS • Multi-site sensing at CII
Local resources	2-5 people	5-10 people	7-15 people	15-45 people
Duration	9 months	12 months	12-24 months	24-36 months

Каталог CSIRT/SOC услуг



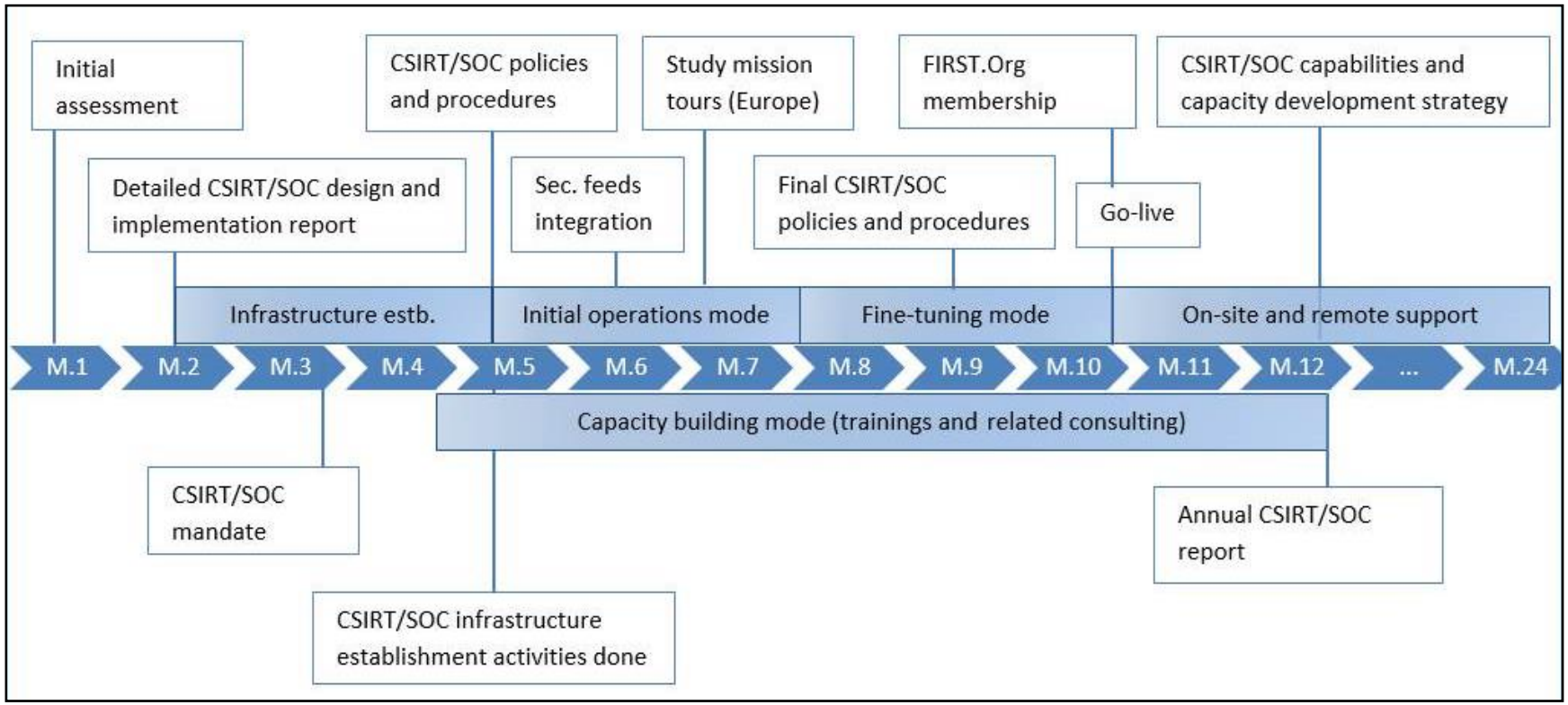
Пример создания CSIRT



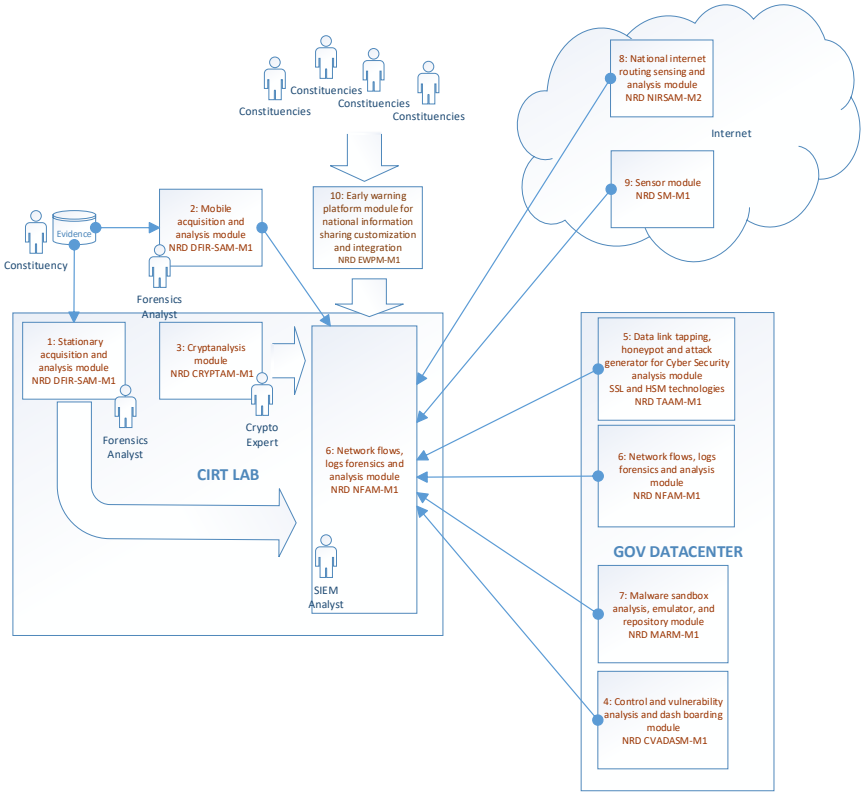
- Basic capability and capacity building
- Community acceptance readiness
  - FIRST membership

NRD Cyber Security

Пример плана создания CSIRT



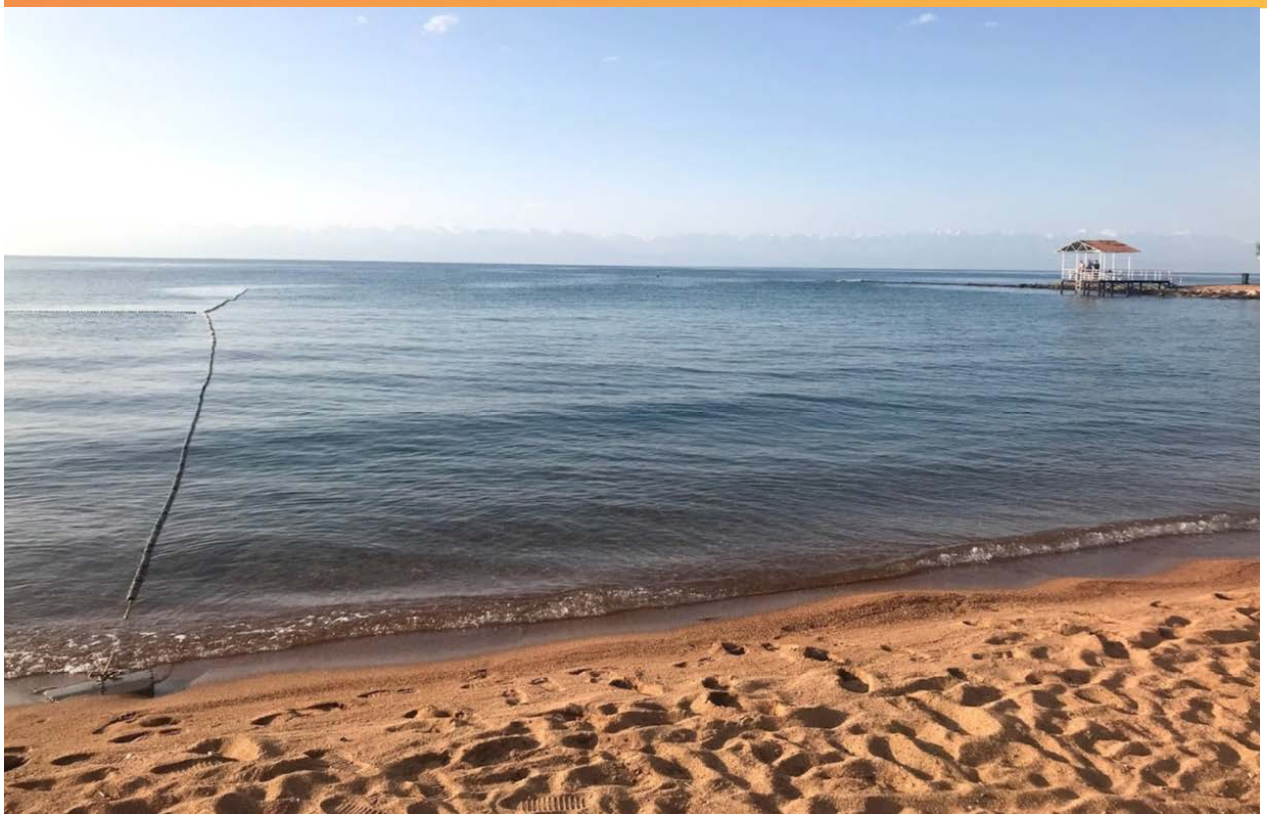
5. Создание кибер-лабораторий



Возможные модули системы:

- Stationary acquisition and analysis module
- Mobile acquisition and analysis module
- Cryptanalysis module
- Control and vulnerability analysis and dash boarding module
- Data link tapping, honeypot and attack generator for Cyber Security analysis module
- Network flows, logs forensics and analysis module
- Malware sandbox analysis, emulator, and repository module
- National internet routing sensing and analysis module
- Sensor module
- Early warning platform module for national information sharing customization and integration

Спасибо за внимание



Romualdas Lečickis

Business Development Director

rl@nrdcs.lt, +370 612 73994

NRD Cyber Security,

Lithuania