



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

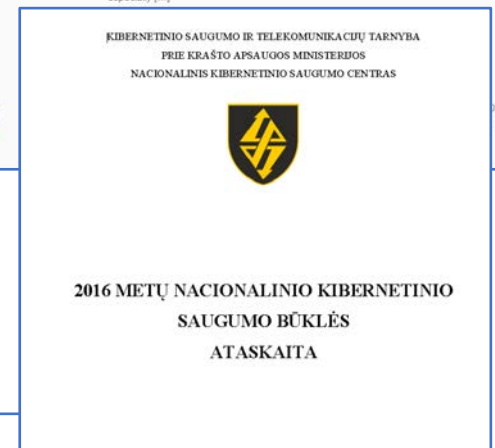
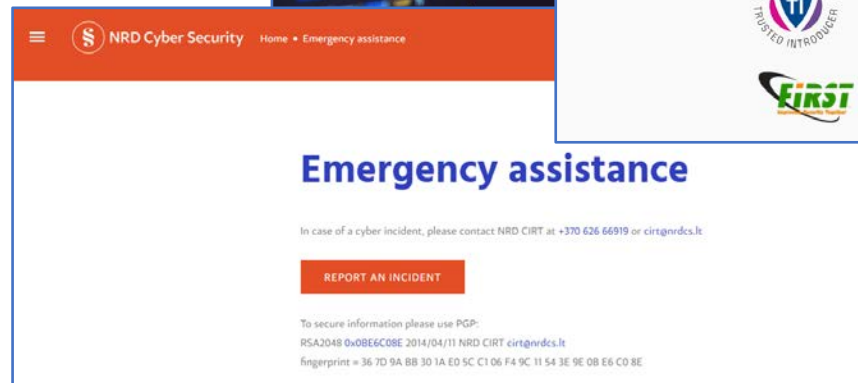
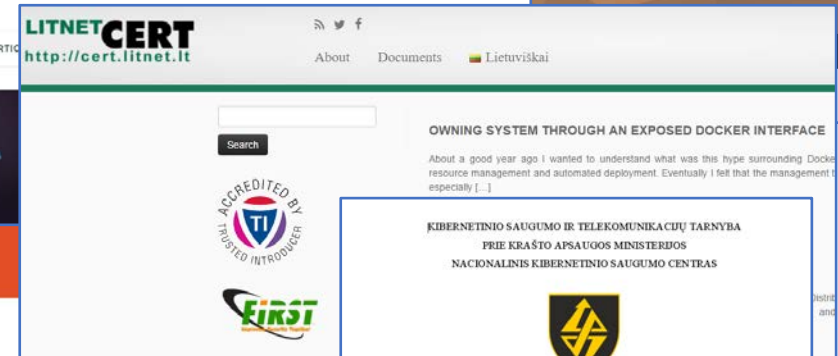
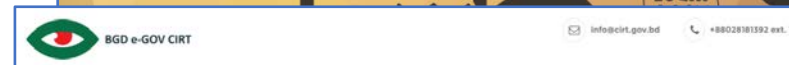
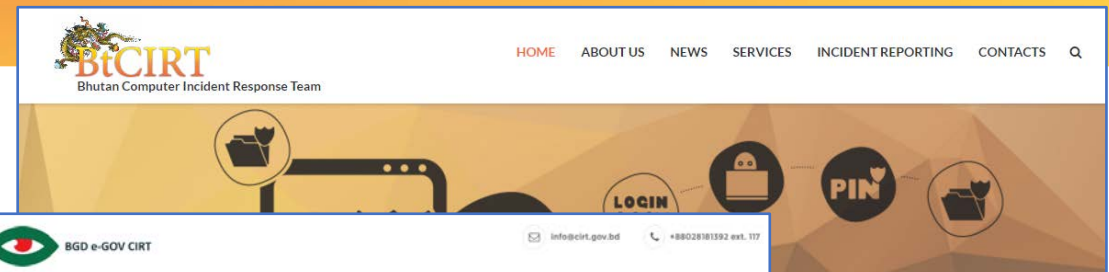


Каким образом увеличить доверие?



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

ITU Regional Workshop "National Strategies of Digital Transformation" (Kyrgyzstan, 28-29 August 2018)

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

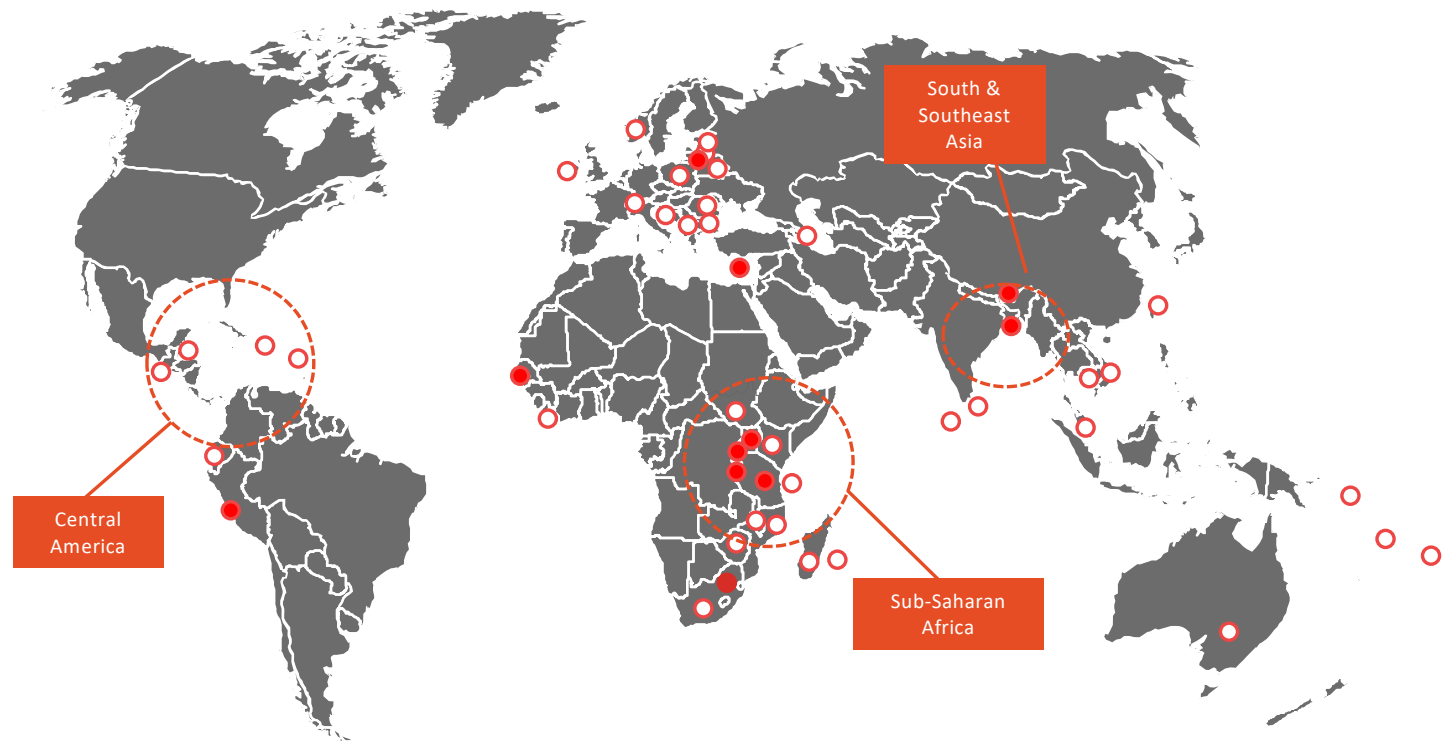
- OSINT
- Аналитика данных



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.



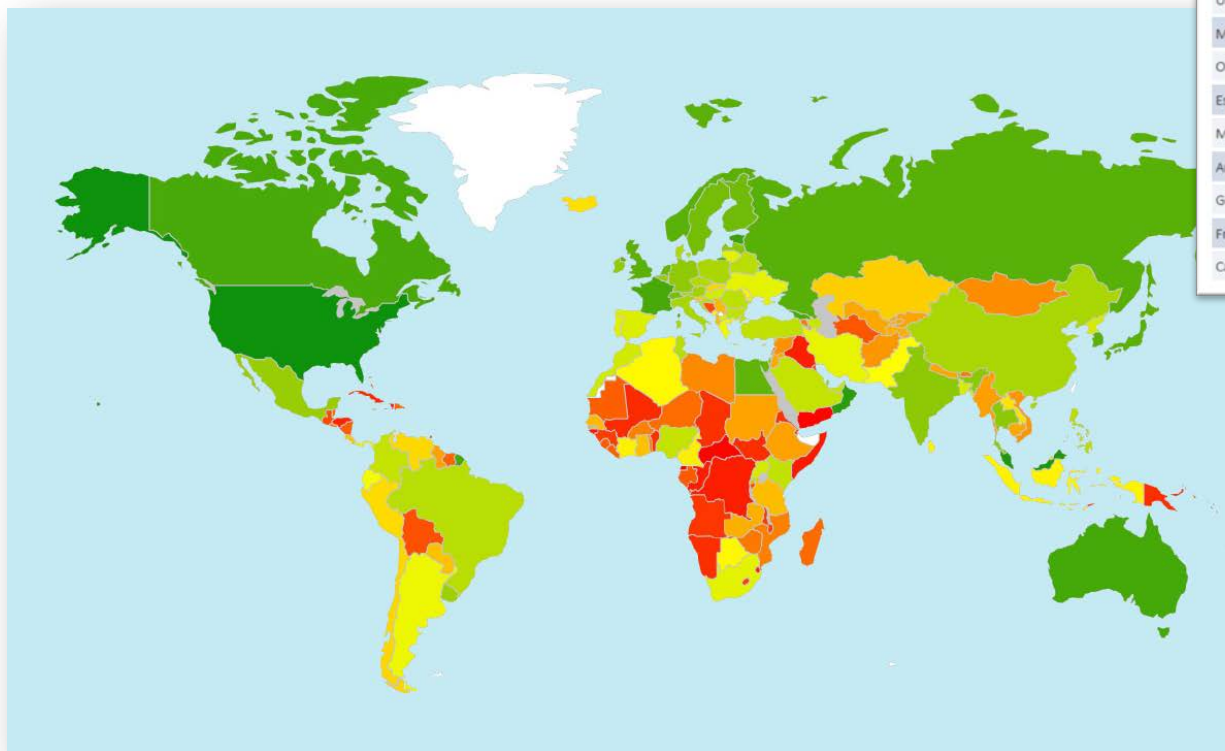
NRD Cyber Security

ПАРТНЕРЫ ПО
СОЗДАНИЮ
ЦЕНТРОВ
КИБЕР-
БЕЗОПАСНОСТИ



NRD Cyber Security

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 INDEPENDENT STATES 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
Armenia	0.190	111
Turkmenistan	0.133	132



National Cyber Security Index



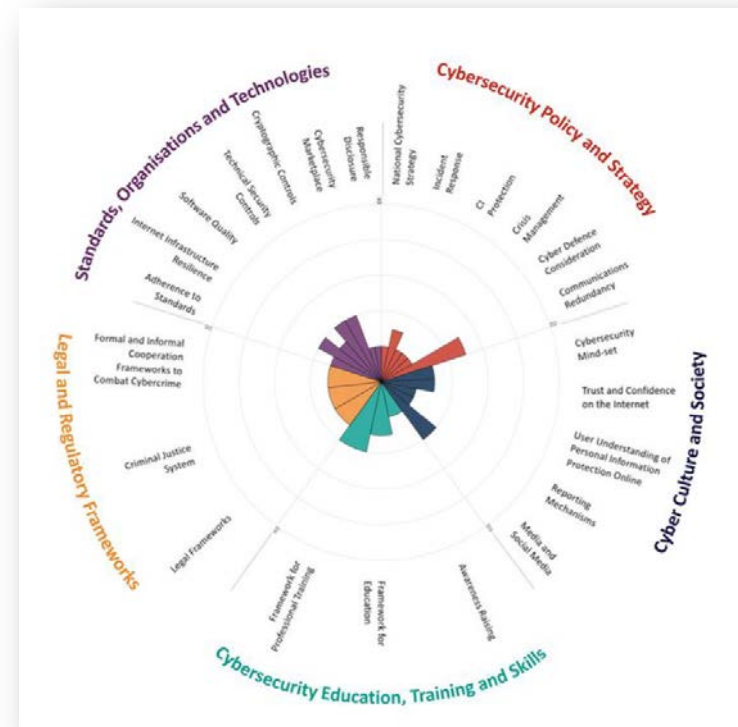
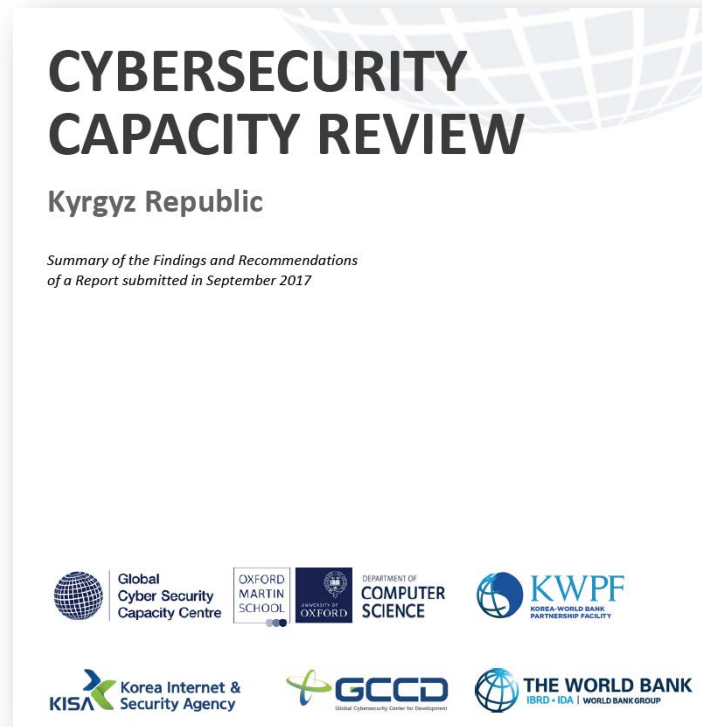
ncsi.ega.ee/country/bd/

Rank	Country	National Cyber Security Index
1.	France	83.12
2.	Germany	83.12
3.	Estonia	81.82
4.	Slovakia	80.52
5.	Finland	79.22
6.	Singapore	79.22
7.	Lithuania	77.92
8.	Spain	77.92
9.	United Kingdom	75.32
10.	Czech Republic	74.03

78.	Azerbaijan	23.38
79.	Saudi Arabia	23.38
80.	Ghana	20.78
81.	Trinidad and Tobago	20.78
82.	Kyrgyzstan	19.48
83.	Indonesia	19.48
84.	Kazakhstan	19.48
85.	Senegal	16.88
86.	Lao PDR	16.88
87.	Afghanistan	15.58



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

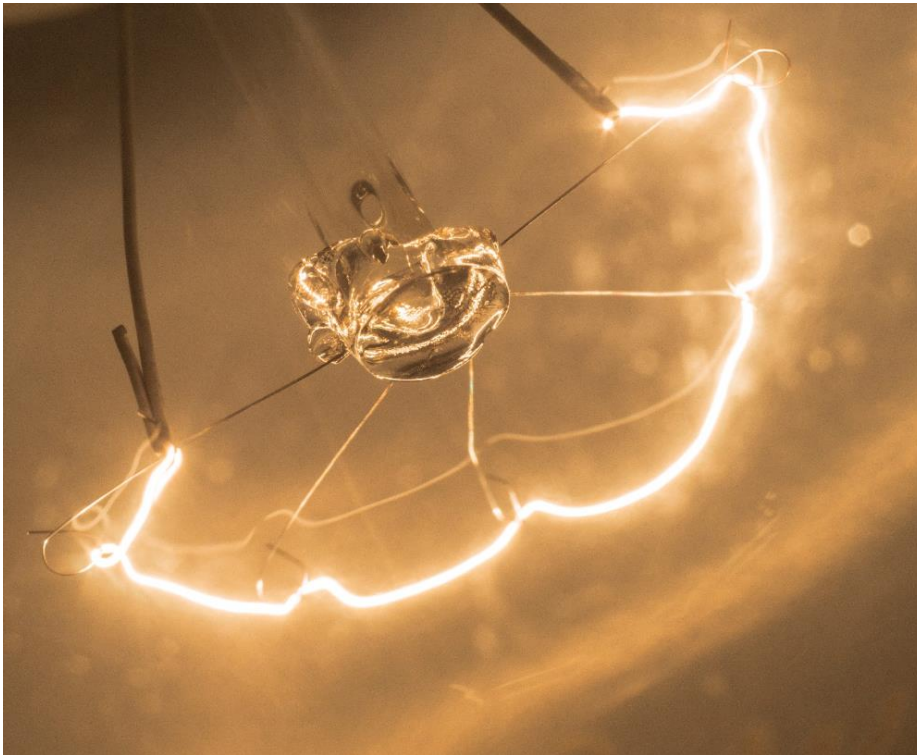


1. Разработка Национальной кибер стратегии



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

Pradžia > Atitikties vertinimo duomenys

Auditas Atitikties vertinimo duomenys Neatitiktųjų valdymas

▼ Filtras

Reikalavimas Tipiniai reikalavimų įgyvendinimo klausimai Įvertinimas Pagrindimas Pagrindimo dokumentai

Sugrupuota pagal: Bendrieji reikalavimai organizaciniams ir techninėms duomenų saugumo priemonėms (VDAL, 2008-11-12 Nr. 11-71(1,12))

4. Organizacinės ir techninės duomenų saugumo priemonės turi užtikrinti tokią saugumo lygį, kuris atitiktų saugotinų asmens duomenų pobūdį ir jų tvarkymo keliamą riziką, ir turi būti išdėstytos rašytinės formos dokumente (duomenų valdytojo patvirtintose asmens duomenų tvarkymo taisyklėse, duomenų valdytojo ir duomenų tvarkytojo sudarytoje sutartyje ir pan.).

5. Duomenų valdytojas privalo užtikrinti, kad organizacinės ir techninės duomenų saugumo priemonės būtų įgyvendintos.

Kaip buvo įvertinta asmens duomenų tvarkymo keliamą riziką? Priskirkite dokumentą, kuriame išdėstytos organizacinės ir techninės duomenų saugumo priemonės. Kada šis dokumentas buvo patvirtintas?

Kaip užtikrinamas organizacinių ir techninių duomenų saugumo priemonių įgyvendinimas? Kada tai buvo patvirtinta?

ARSIS

Paieška dokumentuose

Pagalba

Išorinis naudotojas

Atsijungti

Ištekliai Reikalavimai Atitikties vertinimas Rizikos Apsaugos priemonės Įvykiai Dokumentai Ataskaitos Apie

Auditas

Pradžia > Atitikties vertinimas > Atitikties vertinimas

Sukurti įrašą

▼ Filtras

Pavadinimas	Data ir laikas	Teikiančioji organizacija	Atsakingas	Informacinis šaltinis	Būsena	Lentelės
2016 m. auditas	2016-03-14 22:00	Testinė organizacija	Išorinis naudotojas	Testavimui skirtas	Vykdoma	<ul style="list-style-type: none">Atitikties vertinimo duomenysNeatitiktųjų valdymas

ARSIS

Paieška dokumentuose

Pagalba

Išorinis Naudotojas

Atsijungti

Ištekliai Reikalavimai Atitikties vertinimas Rizikos Apsaugos priemonės Įvykiai Dokumentai Ataskaitos Apie

Teisės

Pradžia > Reikalavimai > Teisės

- Reikalavimų sąrašas
- Teisės aktai
- Sąvokos
- COBIT brandos lygiai

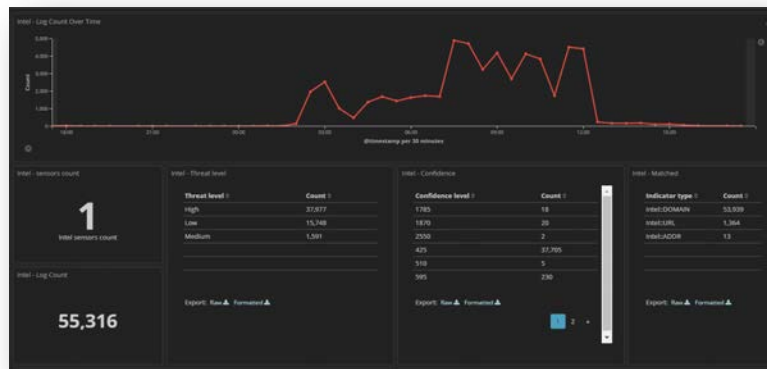
Eksportuoti

▼ Filtras

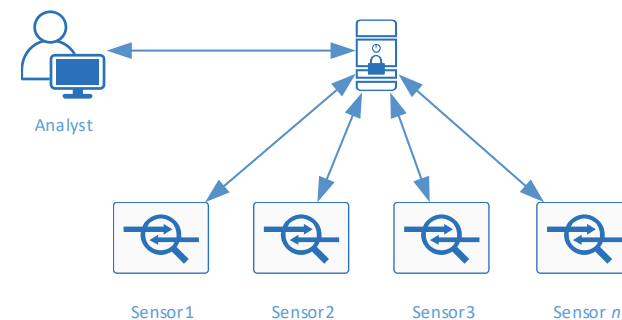
Pavadinimas	Rūšis	Priėmusios institucijos pavadinimas	Priėmimo data	Numeris	Nuoroda į teisės aktą
Interneto tarmybinių stočių apsaugos rekomendacijos (VRM, 2004-05-21, Nr. TV-176)	Įsakymas	Lietuvos Respublikos vidaus reikalų ministerija	2004-05-21	85-3095	TAR
LST ISO/IEC 27002:2014 Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai (Išpatina ISO/IEC 27002:2013)	Standartas	Tarptautinė standartizacijos organizacija (ISO) / Tarptautinė elektrotechnikos komisija (IEC)	2014-01-17	LST ISO/IEC 27002:2014	
Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika (IVPK, 2014 m. vasario 25 d. įsakymu Nr. T-29)	Įsakymas	Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos	2014-02-25	T-29	TAR

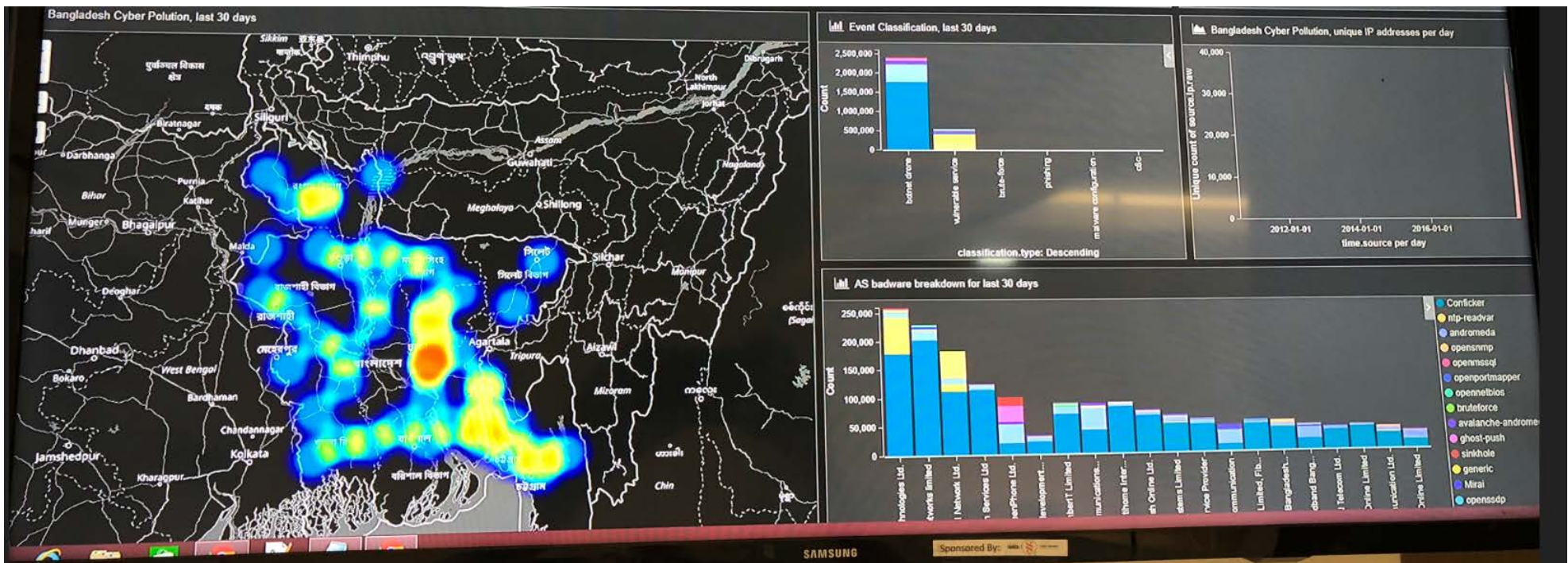


3. Внедрение систем сенсоров для обеспечения безопасности



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





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	<ul style="list-style-type: none"> Mandate definition FIRST.org membership Roadmap & Strategy 	<ul style="list-style-type: none"> Mandate definition FIRST.org membership Roadmap & Strategy 	<ul style="list-style-type: none"> Mandate definition FIRST.org membership Roadmap & Strategy Orgchart buildout 	<ul style="list-style-type: none"> Mandate definition FIRST.org membership Roadmap & Strategy Orgchart buildout
People	<ul style="list-style-type: none"> Featured CSIRT training Limited remote support 	<ul style="list-style-type: none"> Relevant CSIRT training Remote support SOPs Study mission tours 	<ul style="list-style-type: none"> Relevant CSIRT training Remote support SOPs Study mission tours 	<ul style="list-style-type: none"> Relevant CSIRT training On-site and remote support SOPs Study mission tours
Processes and services	<ul style="list-style-type: none"> Incident handling service Incident handling process 	<ul style="list-style-type: none"> Incident handling and outreach Infrastructure support Standard reporting 	<ul style="list-style-type: none"> Incident handling, outreach, digital forensics, vulnerability management Process automation Infrastructure support Standard reporting 	<ul style="list-style-type: none"> Full scale CSIRT/SOC services Process automation Automated custom reporting Maturity progress assessment Infrastructure support
Measurements	<ul style="list-style-type: none"> A few KPIs No SLAs 	<ul style="list-style-type: none"> Basic KPIs SLAs for processes 	<ul style="list-style-type: none"> KPIs system SLAs for processes SIM3 successful audit 	<ul style="list-style-type: none"> KPIs system SLAs for services and automation Annual reviews, SOC-CMM L3 C1.5
Technological Capability	<ul style="list-style-type: none"> Incident registration and handling PGP 	<ul style="list-style-type: none"> Incident registration and handling Outreach and visualization portal Internal support, PGP Simple vulnerability assessment 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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

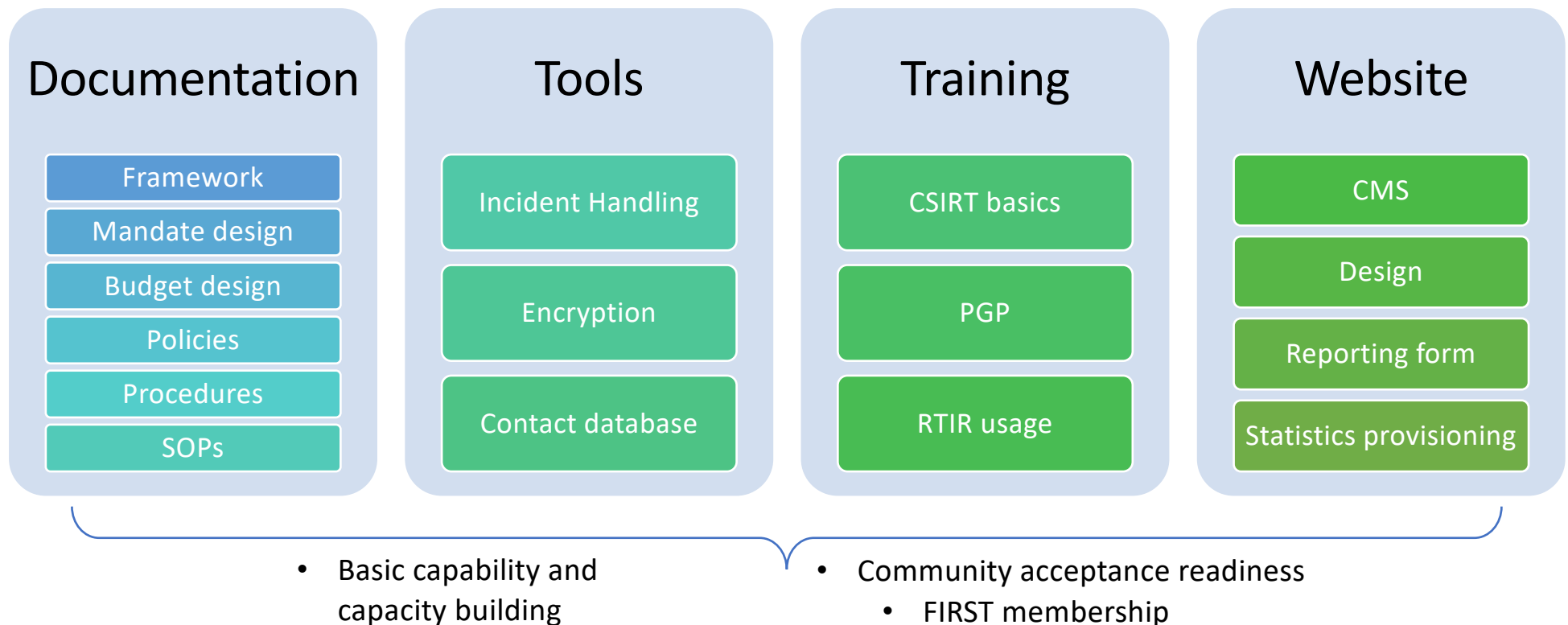


Каталог CSIRT/SOC услуг

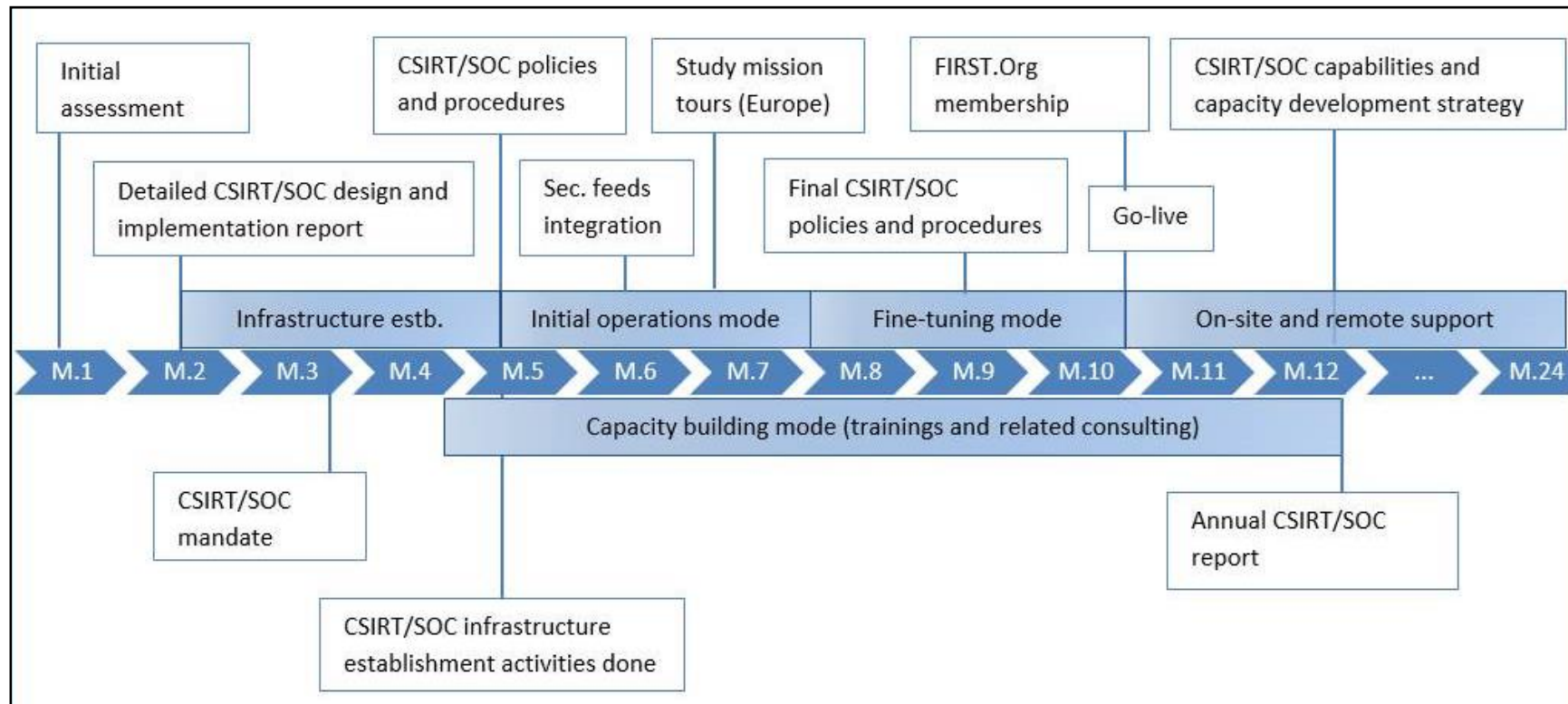
Services, Functions and Sub-functions					
1 Incident Management <ul style="list-style-type: none">1.1 Incident Handling<ul style="list-style-type: none">1.1.1 Incident Validation and Classification1.1.2 Incident Tracking1.1.3 Information Collection1.1.4 Coordination and reporting1.1.5 Communication with news media1.2 Incident Analysis<ul style="list-style-type: none">1.2.1 Impact Analysis1.2.2 Mitigation Analysis1.2.3 Recovery Analysis1.3 Incident Mitigation and Recovery<ul style="list-style-type: none">1.3.1 Containment (self-spreading directed incidents)1.3.2 Restore confidentiality, integrity, availability	3 Information Assurance <ul style="list-style-type: none">3.1 Risk Management<ul style="list-style-type: none">3.1.1 Risk Assessment3.1.2 Risk Assessment Advice3.2 Compliance Management<ul style="list-style-type: none">3.2.1 Manage Compliance Requirements/Standards3.2.2 Compliance Assessment3.3 Operating Policies Support3.4 Business Continuity and Disaster Recovery Planning Support3.5 Technical Security Support3.6 Patch Management	5 Outreach/Communications <ul style="list-style-type: none">5.1 Security Awareness Raising5.2 Cybersecurity Strategic Policy Advisement<ul style="list-style-type: none">5.2.1 Function -Policy Consultancy5.2.2 Legal Consultancy5.3 Knowledge Sharing and Publications Dissemination<ul style="list-style-type: none">5.3.1 Public Service Announcements5.3.2 Publication/Dissemination of Information			
2 Analysis <ul style="list-style-type: none">2.1 Artifact Analysis<ul style="list-style-type: none">2.1.1 Surface Analysis2.1.2 Reverse Engineering2.1.3 Run Time Analysis2.1.4 Comparative Analysis2.2 Media Analysis2.3 Vulnerability / Exploitation Analysis<ul style="list-style-type: none">2.3.1 Technical (Malware) Vulnerability / Exploitation Path Analysis2.3.2 Root Cause Analysis2.3.3 Remediation Analysis2.3.4 Mitigation Analysis	4 Situational Awareness <ul style="list-style-type: none">4.1 Sensor Operation<ul style="list-style-type: none">4.1.1 Requirements Analysis4.1.2 Data Source Identification4.1.3 Legitimizing Collection4.1.4 Data Acquisition4.1.5 Sensor Management4.1.6 Results Management4.2 Fusion and Correlation<ul style="list-style-type: none">4.2.1 Determine Fusion Algorithms4.2.2 Fusion Analysis4.3 Development and Curation of Security Intelligence<ul style="list-style-type: none">4.3.1 Source Identification and Inventory4.3.2 Source Content Collection and Cataloging4.3.3 Information sharing	6 Capability Building <ul style="list-style-type: none">6.1 Organizational Metrics6.2 Training and Education<ul style="list-style-type: none">6.2.1 Knowledge, Skill, and Ability Requirements Gathering6.2.2 Development of Educational and Training Materials6.2.3 Delivery of Content6.2.4 Mentoring6.2.5 Professional Development6.2.6 Skill Development6.3 Conducting Exercises<ul style="list-style-type: none">6.3.1 Requirements Analysis6.3.2 Format and Environment Development6.3.3 Scenario Development6.3.4 Executing Exercises6.3.5 Exercise Outcome Review6.4 Technical Advice<ul style="list-style-type: none">6.4.1 Infrastructure Design and Engineering6.4.2 Infrastructure Procurement6.4.3 Tools Evaluation6.4.4 Infrastructure Resourcing6.5 Lesson Learned Analysis6.6 Development of Vulnerability Discovery/Analysis/ Remediation/Root Cause Analysis Methodologies6.7 Development of processes for Gathering/Fusing/ Correlating Security Intelligence6.8 Development of Tools			



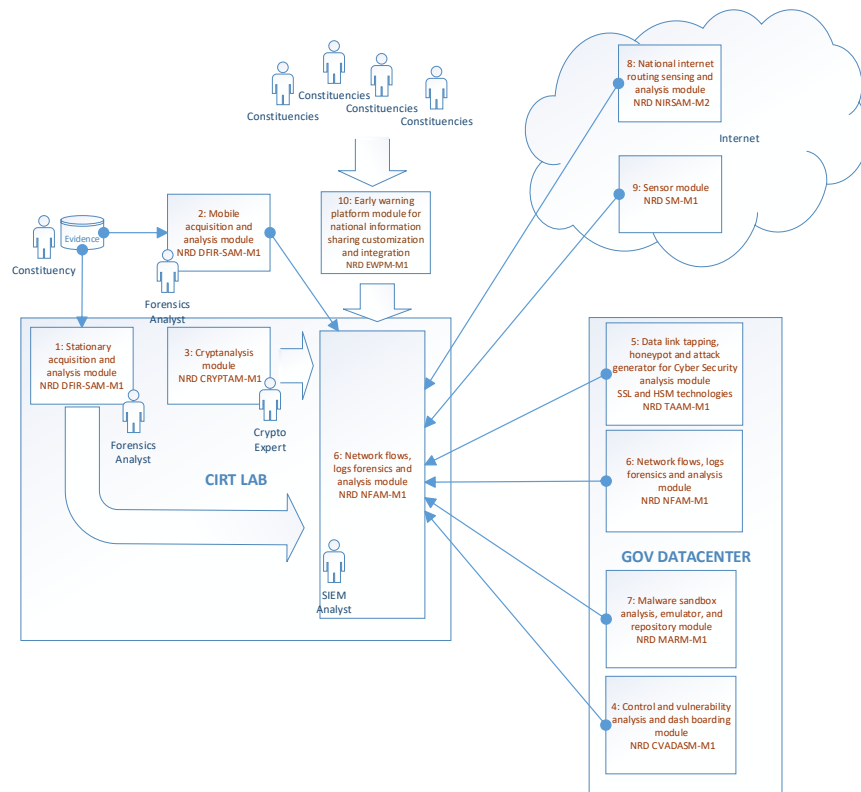
Пример создания CSIRT



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



NRD Cyber Security

ITU Regional Workshop "National Strategies of Digital Transformation" (Kyrgyzstan, 28-29 August 2018)