Empowering National Cybersecurity Projects

kaspersky

Introduction

Our lives are highly dependent on the internet. The low cost and high speed of the communications it provides make it an integral and critical component that lies at the very foundation of successful government, business and individual operations. Dynamic and inter-connected environments provide various important functions that have the power to improve communications, protect personal, confidential and other data and provide oversight and control for critical systems and business processes, all while stimulating overall competitiveness.

In this environment, cybersecurity should no longer be considered separate from general privacy, health and economic risks. And as reliance on the internet continues to grow, cyberthreats – also on the increase - can spread across the globe in minutes disregarding regional, national or other boundaries.

Kaspersky has become a trusted partner for major CERTS, government bodies and law enforcement agencies around the world, sharing our up-to-the-minute knowledge on cyberthreats and helping to find and implement effective defensive mechanisms. We acknowledge that there are no "silver bullet" solutions in a world of rapidly developing technologies, the constantly changing threat landscape and a lack of cybersecurity knowledge. However, we strongly believe that intelligence sharing, development of the corresponding legislation and close collaboration on cybersecurity topics between governments, professional communities and commercial organizations can significantly improve overall defenses that in turn have the potential to drive further technological development to the economic and social benefit of all nations.

Taking into account the diverse nature of cybersecurity problems and varying levels of cybersecurity awareness and knowledge among organizations and individuals, we believe that an effort centralized at the national level will help to significantly increase and improve a nation's overall cybersecurity posture. The contents of this document are based on our experience and participation in complex national cybersecurity projects around the world and are aimed at sharing these acquired best practices. The document does not constitute a complete list of recommendations as it's subject to constant development and evolution together with the constantly changing cybersecurity requirements. It's intended to serve as a reference point and provide some guidance on how to develop and implement national cybersecurity projects - and how Kaspersky can help by providing specific expertise, technologies and services.

Planning the national CERT

The ever-growing number of high-profile cyber incidents clearly demonstrates that, in order to protect national economies and public safety, governments must withstand more complex challenges than ever before. The main purpose of creating a national CERT is to ensure national resilience to cyber risks which may negatively impact on the national economy, public health and safety or affect overall competitiveness of the nation through the disclosure of sensitive information, theft of intellectual property or even the complete breakdown of ICT infrastructures critical to government, civilian and business operations. If it's to succeed, such a complex project requires careful preliminary planning and the involvement of a team with expertise across disciplines. Activities at this stage include:

- Defining and formulating the mission and vision of the national CERT - in other words, determining high-level goals to be achieved, by what means, and the values, once incorporated, that will support the achievement of these goals
- Defining and describing CERT constituency, responsibilities and mandate
- Identifying the communities and individuals involved in project discussions including those from government bodies, commercial organizations, security and law enforcement agencies, technology vendors, etc.
- Determining communication channels that will be used during not only the development phase but for further coordination once the CERT is fully operational
- Determining a set of services that will be provided by the national team (external and internal monitoring and alerting, incident response coordination, forensic analysis, security assessment and audits, security awareness training, etc.)
- Determining the specific regulations and policies affecting CERT development, implementation and operations
- Defining possible funding strategies which support its development, implementation and operation.

Institutional authority

A national CERT needs to have influence over a range of stakeholders. Depending on the government structure and taking into account current cross-sector accountability framework, it should be housed in a body or office with well-established contacts in key sectors, having enough authority among involved parties, and the ability to establish and enforce security policies and attract sufficient funding when needed. If not, it will be very difficult to execute the various tasks required to accomplish its mission.

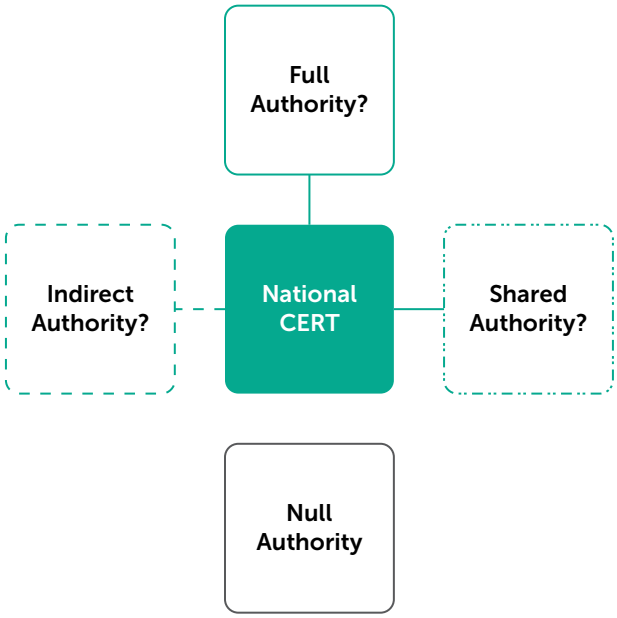

Figure 1. Institutional Authority

National CERT may have a full mandate to disable vulnerable or compromised services or have a shared or null authority providing only recommendations, advice or exerting indirect pressure (for example, through enforcing regulatory requirements). In some countries, this kind of team exists within the Ministry of Defense while in others it can operate from the Ministry of Communications and Technology or from within another structure, agency or sector.

Organizational framework

The initial set of functions national CERT should carry out includes incident management, engineering, research and development, etc. Certain functional areas will most likely be incorporated as it matures, such as policy, regulation and compliance. It will facilitate leading the development, implementation and alignment of cybersecurity policies to the specifics of various critical infrastructures while enforcing and overseeing their compliance to the regulations developed. (However, the compliance function requires separate and in-depth discussion, which is not in the scope of this document.)

National CERT coordinates and oversees incident management across various industries and organizations and can serve different communities depending on the existence of local response teams. It's common practice to have existing industrial or other CERTs be a part of the target community that national CERT serves. To ensure the effectiveness of monitoring and reporting and community coverage, the hierarchical structure shown on Figure 2 may be considered.

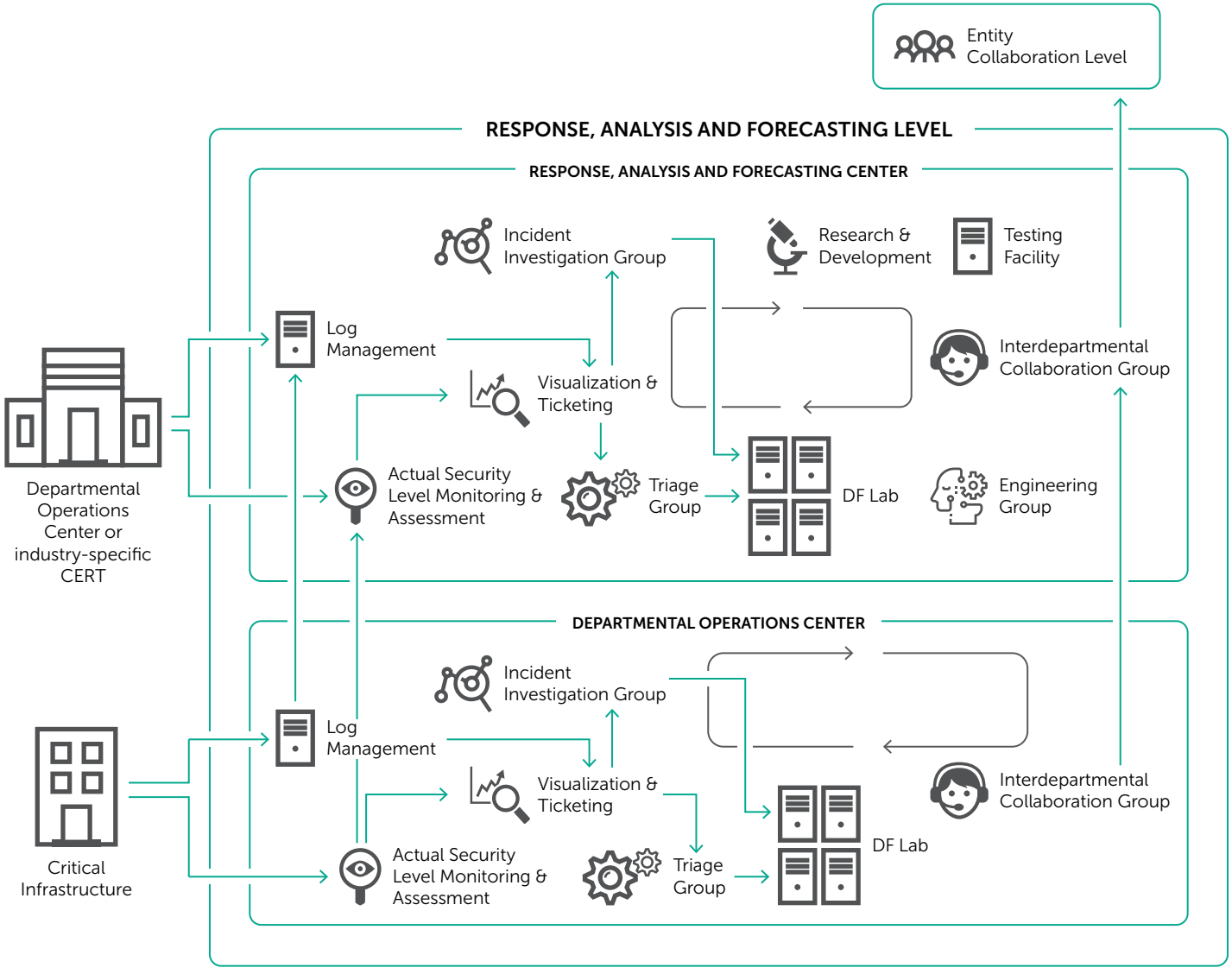

Figure 2. Organizational Framework

On the Critical Infrastructure level, sensors and communication channels allow effective and timely information exchange between monitored facilities and the Operation Center higher up the hierarchy.

Departmental Operation Centers (these may be industry-specific CERTs inside the country or dedicated teams within the national CERT itself) as an intermediate level in the hierarchy enable industry-specific characteristics of critical infrastructures to be taken into account. They also balance workloads during massive cyber outbreaks. They should provide:

- Continuous monitoring of the security of critical infrastructures, which have specific departmental affiliations or belong to a specific industry (e.g. banking, public transportation, telecommunications, energy, etc.)

- Information about cyberattacks against subordinate organizations to the response, analysis and forecasting center
- Coordination of critical infrastructure staff responses during a cyberattack
- Information on the overall security status of the respective subordinate organizations to the response, analysis and forecasting center

Accumulating the security assessment results of subordinate organizations at Departmental Operations Center level enables its staff to identify shortcomings in existing security controls and make appropriate managerial decisions in a timely manner. At the same time, accumulating information on security events enables preliminary diagnostics and evidence collection, guiding further investigation without the need for the Operation Center's experts to be onsite.

Departmental Operation Centers forward the received information further up the hierarchy, where it undergoes similar processing. As a result, the Response, Analysis and Forecasting Center has full information on the security levels of all critical infrastructures within the country and related security events, with the ability to step in if necessary and lead any investigation and response.

Group	Functions
Triage Group	This group is responsible for security event monitoring, incident identification and preliminary investigation. True positives requiring further, more in-depth investigation are transferred to the incident investigation group.
Incident Investigation Group	This group conducts in-depth incident investigation and initiates responses to complex incidents.
Engineering Group	The Engineering Group is responsible for maintaining CERT's ICT infrastructures, updating event collection and incident detection policies as well as automated event processing rules.
Research & Development Group	Conducts ongoing research into cybercriminals' tactics, techniques and procedures, developing effective detection, prevention and mitigation methods.
Interdepartmental Collaboration Group	Communicates with internal Departmental Operation Centers and external stakeholders including industry-specific CERTs.
Administration Group	This group includes roles responsible for CERT management, legal support, finance, PR and external communications.

The Response, Analysis and Forecasting Center performs the following functions:

- Initiating and coordinating complete or selective security assessments for monitored infrastructures while managing and overseeing subordinate departmental operations centers
- Coordinating response actions for cyberattacks that pose a significant threat to subordinate critical infrastructures or responses to massive attacks executed simultaneously against infrastructures of different departmental affiliation
- Systematizing security assessment results, identifying typical shortcomings in the existing security controls and developing remedial recommendations
- Investigating cyber incidents causing significant damage to subordinate organizations or for other reasons necessitating its experts to be involved
- Accumulating and analyzing information on tactics, techniques and procedures used by cybercriminals, conducting advanced research in the field, forecasting attacker trends, assessing actual and potential implications of cyberattacks
- Developing specific recommendations for further security improvements across the nation
- Suggesting adjustments to regulatory guidelines.[1]

With rapidly changing cybersecurity conditions, collaboration on information security becomes critical not only between individual organizations but at a national level too. Cyberthreats have no boundaries so a national CERT should be responsible for establishing efficient information exchange with professional communities and CERTs inside as well as outside the country. The Collaboration Center of the national CERT is responsible for:

- Informing ICT operators about critical vulnerabilities in popular versions of systems and applied software, as well as available mitigation methods
- Informing ICT operators about typical cyberattacks and providing recommendations on blocking them
- Informing vendors about newly discovered vulnerabilities in software supplied by them;
- Coordinating joint activities related to counteracting cyberattacks with similar centers in other countries (e.g. within the framework of CERT collaboration).

1 Please note that incident analysis and compliance functions need to be completely separated in order to ensure effective incident reporting, as most organizations will be concerned about sharing all the details with the organization that has the power to impose penalties.

Recommendations on incident management

A high-level view on the incident management process is shown in the below Figure:

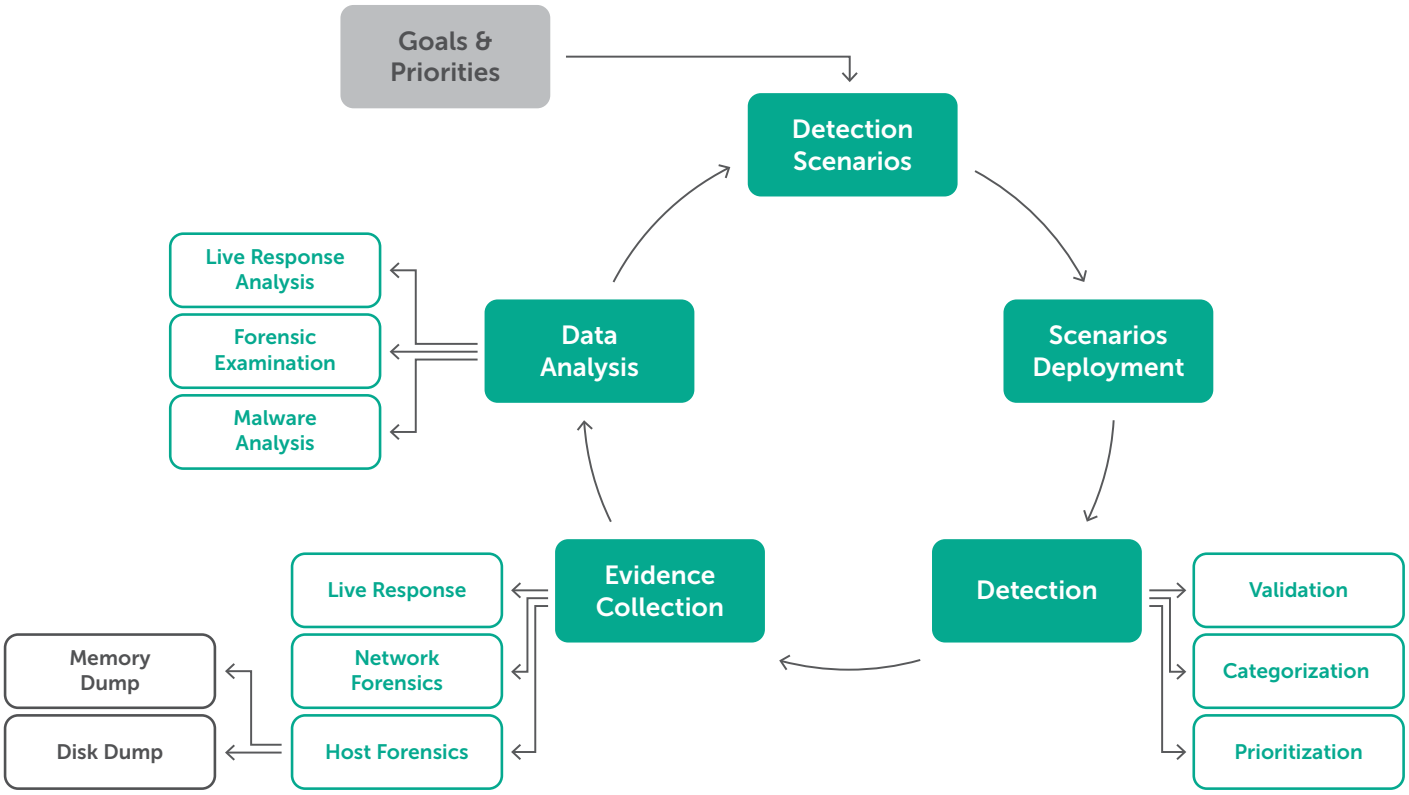

Figure 3. Incident Management Workflow

Group	Functions
Goals and priorities	• Learn what critical resources, assets and networks exist within the nation. Given that resources are often limited, focus should be maintained on the most critical information assets and business processes, finding those areas where 80% of the result can be achieved through 20% of the efforts. • Take a look at the types of incidents currently being reported and identify those that must be reported. • Identify, discuss and create basic response plans considering a variety of interdependencies across major sectors.
Detection scenarios and scenarios deployment	• Gain an understanding of the threat actors that could target critical institutions in your country, their motives and the exploitation vectors they could potentially use. • Map identified critical systems and networks to the threat vectors revealed. • Develop corresponding detection scenarios for distribution throughout the constituency.
Event classification and triage	In order to ensure optimum resource allocation, each detection event needs to go through: • Event validation – gaining assurance that the event being observed is not a false detection. • Event categorization – placing each event detected into one category or another in order to define further response. • Event prioritization – determining whether a specific event in the queue requires immediate response or warrants additional examination.
Evidence collection	For events categorized as incidents, further evidence collection is initiated, including gathering information on active processes, network status, dynamic libraries loaded, OS and application events, etc., and ending with the most labor-intensive efforts – computer forensics, including the analysis of memory and drive images, and network forensics, including the analysis of network traffic dumps.
Data analysis	A cycle of evidence collection followed by data analysis can result in the identification of new artifacts. If so, the entire environment should be checked for their presence. The cycle needs to be repeated as many times as new indicators are discovered.

The results of the investigation should be used to develop new detection scenarios or adjust existing ones. Those scenarios which don't produce false positives can be implemented into the automatic detection rules like, for example, signatures for preventive security controls, including anti-malware engines or IDS.

Incident investigation group

Incident investigation and management on a national level requires a team of diverse competencies and knowledge. An Incident Investigation Group should be divided into units, each responsible for specific knowledge on:

- Malicious software
- Vulnerabilities in software and protocols
- Methods of operation
- Software configuration errors
- User errors

Members of the team should also have some knowledge of the basic network protocols (IP, ICMP, TCP, UDP, FTP, HTTP, DNS and SMTP).

For the incident response team to become fully operational, several functions should be undertaken (by a single employee at the initial stage or distributed throughout the team). The team should have:

- Malware analysis experts
- Incident response experts
- Incident investigation experts

Challenges and solutions

Each step of the effective incident management process requires technical capability and expertise to answer a specific set of questions, as shown in the Figure below.

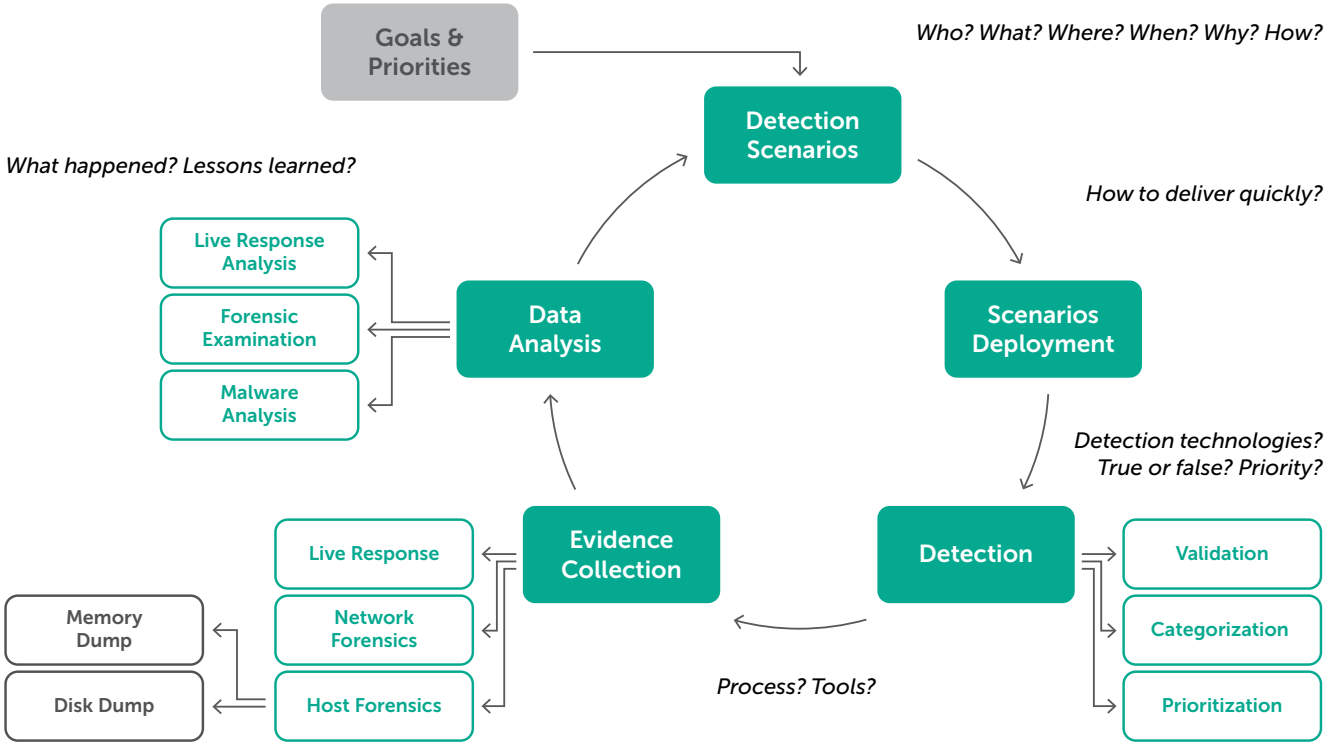

Figure 4. Challenges of the Incident Management Process

In an effort to address the challenges that a national CERT team might face while building an incident management capability, Kaspersky provides access to its global expertise and leading technologies:

Question	Explanation	Solutions
Who? When? Why? What? How?	Who are the potential attackers? When were they last seen? What is their motivation? What capabilities do they have? How do they use them?	Having an overview of the current attack surface and the current trends in malware and hacker attacks targeting your country allows you to focus your defense strategy on those areas identified as prime targets for cybercriminals. This means you can act fast and with precision to repel intruders and minimize the risk of a successful attack. Leveraging various approaches ranging from Open Source Intelligence (OSINT) to deep analysis of proprietary, globally distributed, data gathering and analysis networks, and our extensive expertise and knowledge of the underground cybercriminal communities, **Kaspersky Country-specific** and **APT Intelligence reports** provide a detailed view of the threats targeting your country. **Kaspersky Penetration Testing** and **Security Assessment** services will allow you to obtain information on vulnerabilities in key services and components, understand the possible consequences of their exploitation, evaluate the effectiveness of existing security controls, and plan further actions to fix identified flaws and improve security overall.
How to deliver quickly?	How can you quickly distribute detection logic across extensive IT networks? The tools and command-and-control centers used in attacks change rapidly (e.g. the lifespan of a server distributing malware can be only a few minutes), so speed is essential.	Kaspersky technologies and services ensure rapid detection logic delivery: **Kaspersky Security Network** (KSN) – Kaspersky's global cloud threat reputation database. **Kaspersky Private Security Network** – a private replica of KSN deployed at the customer's premises. **Kaspersky Security Center** – a centralized management console for Kaspersky products. **Kaspersky Threat Data Feeds** - up-to-the-minute and immediately actionable cyberthreat data integrated into existing security controls help to mitigate threats more effectively and defend against attacks even before they are launched.
What detection technologies should we use? How do we assign priority? True or False Positive? Tailored or commoditized?	What technologies should be used for detection? Detection at the endpoint or on the network? Which events should we analyze? How do we decide whether the detection is a True Positive or a False Positive? Is it tailored to my organization?	**Kaspersky Sandbox** complements Kaspersky Endpoint Security for Business and supports large organizations with distributed networks and CERT constituencies,without the need for information security analysts, to improve defenses against unknown and evasive threats, significantly increasing the number of automatically blocked ones. **Kaspersky Research Sandbox** is the instrument of choice for national digital forensics laboratories requiring detection and analysis of unknown threats without exposing confidential data outside the organization. Cloud deployment option is also available. **Kaspersky Threat Attribution Engine** is based on the biggest repository of APT threats in the industry and quickly establishes links between any new attack to known APT malware, previous targeted attacks and hacker groups helping to ensure timely and effective threat mitigation. **Kaspersky Anti Targeted Attack Platform** is a specialized platform that includes a set of technologies (web analysis, mail traffic analysis, endpoint event analysis, sandboxing), designed for proactive detection of known and new threats. **Kaspersky Endpoint Detection and Response** provides comprehensive visibility across all endpoints on the corporate network, advanced detection of complex threats and simplified automated response with centralized incident management. **Kaspersky Managed Detection and Response** delivers continuous 24/7 protection from the growing volume of threats designed to circumvent automated prevention and detection systems.
How do we collect evidence? What tools should we use?	Effective incident investigation requires a correctly organized process using the right tools. A mistake can lead to highly undesirable consequences causing significant damage, while incorrect conclusions will result in adaptation errors, including the wrong priorities and expectations being set.	**Kaspersky Cybersecurity Training** program offers a broad curriculum in cybersecurity topics and techniques, integrating a full range of specific skills, functionalities and competencies into a single body of knowledge. The program has been designed by the recognized experts who helped build ivirus labs, and who now inspire and mentor the next generation of global experts. **Kaspersky Threat Lookup** is designed to reveal the relationships between various artifacts (hashes, IP address and URLs), boosting incident response and threat hunting activities while providing broader context. **Kaspersky Incident Response** offers all the assistance needed to effectively manage the aftermath of a security breach by bringing the full weight of our expertise onsite to bear on the resolution and mitigation of your cyber security incident.

Conclusion

Government bodies and national critical infrastructures are natural targets for cyber-warfare. While attacks on major corporates result primarily in material losses, hacking government institutions or backbone enterprises can result in catastrophic consequences, wreaking havoc on a country's entire digital infrastructure and leading to disruption of government operations, national financial crises and even impairment of national defenses. There is a rapidly growing, urgent need for the coordination of incident analysis and response efforts between governments, law enforcement, commercial organizations, the research community and practitioners with experience in responding to modern threats.

A complex national cybersecurity framework incorporates the development of the corresponding policies and regulations while establishing trusted collaboration and communication channels with all involved. Cooperation is the key to success in a world of rapidly changing cyberthreats. To ensure efficient information exchange, national CERT has to gain trust from the community by constantly promoting its role and the services it provides. Once it's recognized as a source of help, the national team can significantly improve the overall cybersecurity of the nation to its social and economic benefit.

To strategically address national cybersecurity challenges, we recommend careful assessment of the following initiatives:

- Establish a single coordination point for incident handling activities
- Analyze, validate and consolidate incident and vulnerability information coming from vendors, industry experts and other teams to provide actionable recommendations to the respective audiences
- Organize, regulate and facilitate sharing of information about cybersecurity issues across multiple sectors, including government, finance, industrial, academic, etc., to raise awareness and improve overall national cybersecurity
- Develop the corresponding mechanisms for trusted information sharing between all involved entities
- Create incident management and response capabilities within critical infrastructures that support local economies while overseeing and promoting their maximum efficiency
- Create a pool of trusted experts qualified to provide technical insights into cyber incidents and vulnerabilities while sharing expertise with less mature organizations
- Increase and nurture awareness in every aspect of cybersecurity among the personnel involved and broader audience
- Facilitate communications at domestic and international levels, taking into account the absence of geographical and national borders for cyberthreats.

These initiatives should provide an understanding of the underlying security issues and emerging threats and result in building resilient infrastructures capable of protecting and recovering essential services and assets and creating a clearly defined and repeatable set of incident management and response coordination processes.

Annex

Profiles and required skills for incident investigation group

Malware analysis expert

Main responsibilities:

- Analysis of malicious objects
- Participation in incident investigations
- Development of automation tools for internal use

Requirements for the candidate:

- Higher education (preferably in the field of Information Technology)
- Experience with static and dynamic file analysis tools (debuggers and disassemblers)
- Experience in analyzing malicious files of different types
- Knowledge of executable file formats for various platforms (Windows, Linux)
- Assembler language knowledge
- Scripting experience and knowledge (Python / Ruby / Perl / PowerShell)
- C, C ++ programming experience
- Technical English with good verbal skills

Additional preferable skills:

- Professional certificates (GIAC, EC-Council)
- Practical experience in targeted attack investigation
- Experience in developing reporting and analytical documents
- Experience in analysis of code for mobile devices

Incident investigation expert

Main responsibilities:

- Participation in projects to investigate computer incidents
- Analysis of malicious objects

Requirements for the candidate:

- Higher education (preferably in the field of Information Technology)
- Experience in investigating computer incidents in large corporate networks for at least 3 years
- Good knowledge of various OS (at the administration level)
- Understanding of modern types of threats and principles of the main types of attacks
- Scripting experience (Python/Ruby/Perl/PowerShell)
- Experience in developing reporting and analytical documents on projects
- Possession of basic tools for digital forensic, threat intelligence, network forensic, reverse engineering
- Experience with host-based and network IoC (Yara, OpenIOC, STIX)
- Technical and spoken English

Additional preferable skills:

- Availability of professional certificates (GIAC, EC-Council)
- Experience in the practical of targeted attack's investigation
- Experience in analysis of malicious code
- C, C++ programming experience
- Experience with static and dynamic file analysis tools (debuggers and disassemblers)

Incident response expert

Main responsibilities:

- Participation in projects to investigate computer incidents
- Research in the field of automated detection of targeted attacks

Requirements for the candidate:

- Higher education (preferably in the field of Information Technology)
- Understanding of indicators of compromise of information systems and methods
- Scripting experience (Python/Ruby/Perl/PowerShell)
- Possession for basic tools for digital forensic, threat intelligence, network forensic, reverse engineering
- Experience with host based and network IoC (Yara, OpenIOC, STIX)
- Experience in developing reporting and analytical documents on projects
- Experience with sandboxes and other dynamic analysis tools
- Technical and spoken English

Additional preferable skills:

- Availability of professional certificates (GIAC, EC-Council)
- Experience with static and dynamic file analysis tools (debuggers and disassemblers)
- Experience in investigating computer incidents in large corporate networks for at least 3 years
- Practical experience in the targeted attack's investigation
- Experience in analysis of malicious code
- C, C ++ programming experience

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Cybersecurity for SMB: kaspersky.com/business
Cybersecurity for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Known more at kaspersky.com/transparency

Proven.
Transparent.
Independent.