

PT. BANK TABUNGAN Pensiunan Nasional Tbk

RANSOMWARE PLAYBOOK

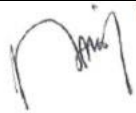







VERSION 1.0

Date: 01/11/2023



Document Sign-Off

Pengesahan Dokumen

	Name Nama	Function Fungsi	Sign & Date TTD & Tanggal
Prepared by	Mohamad Taufik	Cyber Security Governance, Risk & Compliance	 10/1/2024
	Kristo Tutuhatunewa	IT Security Assessment	 17/01/2024
	M. Lazuardi Wirananda Putra	IT Security Operation Center	 12 / 02 / 2024
Reviewed by	Christian	Cyber Security Governance, Risk & Compliance Head	 15/02/2024
	Hendra	IT Security Operation Management Head	 12/02/2024
	Mulyanto Salim	IT Risk Management Head	 26/03/2024
	Ashar Jarot Suranta	IT Infrastructure Corporate Center Head	 19/02/2024
	Ramos Matabun Rajagukguk	IT Process Assurance Head	 24/04/2024
	Johanes Surjadi	IT Service Management Head	Approved by Email, 28 May 2024
	John Pariama	ORM Assessment, ICR & BCM Head	Approved by Email, 29 Apr 2024
Approved by	Iman Triono	IT Transaction Management Head	Approved by Email, 17 May 2024
	Buyung Bachtiar	Cyber Security Risk Head	Approved by Email, 21 May 2024
	Akira Kuwata	IT Governance Management Head	Approved by Email, 21 May 2024
	Andi Febri Cahyo	IT Retail Banking Corporate Function Head	Approved by Email, 29 May 2024
	Hayato Inoue	IT Corporate Banking Enablement Head	Approved by Email, 29 May 2024
	Heru Rustanto	Operational & Fraud Risk Management Head	Approved by Email, 30 Apr 2024
	Butet Sondang Sitepu	Compliance Head	Approved by Email, 10 Jul 2024
	Andrie Darusman	Communication & Daya Head	Approved by Email, 21 May 2024

Version Control Table

Tabel Pengontrol Versi

No No	Name Nama	Change made Perubahan yang dibuat	Approved by Disetujui oleh	Date Tanggal
1	Version 1.0	First Version released	IT Security	01/11/2023
1	Versi 1.0	Versi pertama dirilis	IT Security	01/11/2023

Table of Content

1. Introduction..... 6

1.1 Overview..... 6

1.2 Purpose 6

1.3 Ransomware Definition 6

1.4 Scope 7

1.5 Review Cycle 7

2. Roles and Responsibilities 8

2.1 RACI Matrix 8

2.2 Detail of Responsibilities 9

3. Ransomware Incident Response Phase 12

3.1 Ransomware Flowchart 14

3.2 Technology Matrix 15

4. Ransomware Playbook Detail 16

4.1 Detection and Analysis 16

4.1.1 Detection 16

4.1.2 Analysis 19

4.2 Containment, Eradication and Recovery 23

4.2.1 Containment and Eradication 23

4.2.2 Recovery 25

4.3 Post Incident Activity 27

5. Appendix 30

5.1 Initial notification of Cyber Incident..... 30

5.2 Report of Cyber Incident 31

Daftar Isi

1. Pengantar	6
1.1 Ikhtisar	6
1.2 Tujuan	6
1.3 Definisi Ransomware	6
1.4 Ruang Lingkup.....	7
1.5 Siklus Tinjau Ulang	7
2. Peran dan Tanggung Jawab	8
2.1 RACI Matrix	8
2.2 Detail Tanggung Jawab	9
3. Fase Ransomware Incident Response	12
3.1 Alur Diagram Ransomware	14
3.2 Technology Matrix	15
4. Detail Ransomware Playbook	16
4.1 Detection and Analysis	16
4.1.1 Detection	16
4.1.2 Analysis	19
4.2 Containment, Eradication and Recovery	23
4.2.1 Containment and Eradication	23
4.2.2 Recovery	25
4.3 Post Incident Activity	27
5. Lampiran	30
5.1 Notifikasi Awal Insiden Siber	30
5.2 Laporan Insiden Siber	31

1. Introduction

1.1. Overview

In the event of a Ransomware incident, it is important that the organisation be able to execute an appropriate level of response to limit the impact of such a cyber threat. This playbook details the steps to be taken and individuals involved in responding to a Ransomware incident.

This Playbook describes the activities of those directly involved in managing specific cyber incidents. However, it is important to acknowledge the speed at which cyber incidents can escalate and become a significant business disruptor requiring both business continuity and consequence management considerations. Early consideration should be given to engaging Business Continuity, Resilience and Policy Area Leads in order that the wider issues can be effectively managed. Business Continuity and Resilience leads within the organisation must therefore be familiar with the Cyber Incident Response Plan or Procedure and Playbooks and link to wider incident response arrangements.

The reference of this playbook are from National Institute and Standards and Technology (NIST) and MITRE ATT&CK.

1.2 Purpose

This playbook describes the process that is required to ensure an organized approach to managing Ransomware incidents within organization and coordinating response and resolution efforts to prevent or limit damage that can be caused.

This Ransomware Playbook defines activities to be considered when detecting, analysing, and remediating a ransomware incident. The playbook also identifies the key stakeholders that may be required to undertake these specific activities.

1.3 Ransomware Definition

Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. Attackers may also steal an organization's information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public. When ransomware infects a device, it either locks the screen or encrypts the files, preventing access to the information and systems on your devices. Threat actors can also use the compromised network to spread the ransomware to other connected systems and devices.

Ransomware can be infecting systems in the following ways:

- Visiting unsafe, suspicious, or compromised websites (known as a drive-by download);
- Opening emails or files from familiar or unfamiliar sources (phishing);
- Clicking on links in emails, social media, and peer-to-peer networks;

1. Pengantar

1.1 Ikhtisar

Dalam insiden Ransomware, penting bagi organisasi untuk dapat menerapkan tingkat atau respons yang tepat untuk membatasi dampak ancaman siber tersebut. Playbook ini menjelaskan langkah-langkah yang harus diambil dan individu yang terlibat dalam menanggapi insiden Ransomware.

Pedoman ini menjelaskan aktivitas pihak-pihak yang terlibat langsung dalam mengelola insiden siber tertentu. Namun, penting untuk menyadari betapa cepatnya insiden dunia maya dapat meningkat dan menjadi pengganggu bisnis yang signifikan sehingga memerlukan pertimbangan konsekuensi manajemen dan kelangsungan bisnis. Pertimbangan awal harus diberikan untuk melibatkan *Business Continuity, Resilience and Policy Area Leads* agar permasalahan yang lebih luas dapat dikelola secara efektif. Oleh karena itu, *Business Continuity and Resilience leads* dalam organisasi harus memahami Rencana atau Prosedur dan Buku Pedoman Respons Insiden Siber dan terhubung dengan pengaturan respons insiden yang lebih luas.

Referensi pedoman ini berasal dari *National Institute and Standards and Technology (NIST)* dan *MITRE ATT&CK*.

1.2 Tujuan

Playbook ini menjelaskan proses yang diperlukan untuk memastikan pendekatan terorganisir dalam mengelola insiden Ransomware dalam organisasi dan mengkordinasikan upaya respons dan resolusi untuk mencegah atau membatasi kerusakan yang dapat ditimbulkan.

Playbook Ransomware ini mendefinisikan aktivitas yang harus dipertimbangkan saat mendeteksi, menganalisis, dan memulihkan insiden ransomware. Playbook ini juga mengidentifikasi pemangku kepentingan utama yang mungkin diperlukan untuk melakukan kegiatan-kegiatan spesifik tersebut.

1.3 Definisi Ransomware

Ransomware adalah jenis serangan berbahaya dimana penyerang mengenkripsi data organisasi dan meminta tebusan untuk memulihkan akses. Penyerang juga dapat mencuri informasi organisasi dan meminta pembayaran tambahan sebagai imbalan karena tidak mengungkapkan informasi tersebut kepada pihak berwenang, pesaing, atau publik.

Saat ransomware menginfeksi perangkat, ransomware akan mengunci layar atau mengenkripsi file, sehingga mencegah akses ke informasi dan sistem di perangkat anda. Pelaku ancaman juga dapat menggunakan jaringan yang disusupi untuk menyebarkan ransomware ke sistem dan perangkat lain yang terhubung.

Ransomware dapat menginfeksi sistem dengan cara berikut:

- Inserting an infected peripheral device (e.g.USB flash drive) into a device
- Exposing your systems to the internet unnecessarily or without robust security and maintenance measures, such as patching vulnerabilities and multi-factor authentication (MFA) in place.

Ransomware has become more sophisticated and often employs a combination of attack vectors, such as sending a phishing email to organization along with brute force attacks, where the threat actor uses extensive login attempts or password guessing to access systems and networks. Ransomware can also spread to the systems and networks of organizations connected via their supply chain. For example, an organization who provides services to their clients via inter-connected networks and client management systems could be targeted by ransomware. The threat actor could then use the inter-connected networks or client management systems to infect other organizations within the supply chain with ransomware. These organizations would then be locked out of their systems, disrupting their operations.

Once the threat actor has full control of your network, systems, and devices they will encrypt your data, delete available connected backup files, and often steal your organization's data. They may threaten to leak this data if you do not pay the ransom, or they may say they will decrypt your data and restore your access to it if you pay the ransom.

- Mengunjungi situs web yang tidak aman, mencurigakan, atau disusupi (dikenal sebagai unduhan drive-by);
- Membuka email atau file dari sumber yang dikenal atau tidak dikenal (phishing);
- Mengklik tautan di email, media sosial, dan jaringan peer-to-peer;
- Memasukkan perangkat periferal yang terinfeksi (mis. USB flash drive) ke dalam perangkat
- Mengekspos sistem Anda ke internet jika tidak perlu atau tanpa tindakan keamanan dan pemeliharaan yang kuat, seperti menambal kerentanan dan autentikasi multi-faktor (MFA).

Ransomware kini menjadi lebih canggih dan sering menggunakan kombinasi vektor serangan, seperti mengirim email phishing ke organisasi bersama dengan serangan brute force, di mana pelaku ancaman menggunakan upaya login ekstensif atau menebak kata sandi untuk mengakses sistem dan jaringan. Ransomware juga dapat menyebar ke sistem dan jaringan organisasi yang terhubung melalui rantai pasokan. Misalnya, sebuah organisasi yang memberikan layanan kepada kliennya melalui jaringan yang saling terhubung dan sistem manajemen klien dapat menjadi sasaran ransomware. Pelaku ancaman kemudian dapat menggunakan jaringan yang saling terhubung atau sistem manajemen klien untuk menginfeksi organisasi lain dalam rantai pasokan dengan ransomware. Organisasi-organisasi ini kemudian akan dikunci dari sistem mereka, sehingga mengganggu operasional mereka.

Setelah pelaku ancaman memiliki kendali penuh atas jaringan, sistem, dan perangkat Anda, mereka akan mengenkripsi data Anda, menghapus file cadangan yang tersedia, dan sering kali mencuri data organisasi Anda. Mereka mungkin mengancam akan membocorkan data ini jika Anda tidak membayar uang tebusan, atau mereka mungkin mengatakan akan mendekripsi data Anda dan memulihkan akses Anda ke data tersebut jika Anda membayar uang tebusan.

1.4 Scope

This document has been designed for the sole use of the first responders such as the Cyber Security Incident Response Team (CSIRT) when responding to a cyber incident. It is not standalone and must be used alongside Cyber Incident Response Plan or Procedure.

1.5 Review Cycle

This document is to be reviewed for continued relevancy by the Cyber Security Incident Response Team (CSIRT) at least once every 12 months; following any major cyber incidents, a change of vendor, or the acquisition of new security services.

1.4 Ruang Lingkup

Dokumen ini dirancang hanya untuk digunakan oleh petugas tanggap insiden seperti Tim Respons Insiden Keamanan Siber (CSIRT) ketika merespons insiden siber. Hal ini tidak berdiri sendiri dan harus digunakan bersamaan dengan Rencana atau Prosedur Respons Insiden Siber.

1.5 Siklus Tinjau Ulang

Dokumen ini akan ditinjau relevansinya oleh Tim Respons Insiden Keamanan Siber (CSIRT) setidaknya sekali setiap 12 bulan; setelah insiden dunia maya besar, pergantian vendor, atau akuisisi layanan keamanan baru.

2. Roles and Responsibilities

2.1 RACI Matrix

	Preparation	Detection	Analysis	Containment&Eradication	Recovery	Post-incident
IT Security Operation Management	R	R				
IT SOC	I	R	C	C		
CSIRT		AR	AR	AR	AR	AR
Cyber Security Risk	R		C		C	
IT Risk Management			C			
Business/System Owner		I	I	I	AR	I
IT Operation (Infrastructure, Application, Support)		R	I	R	R	
Compliance		I	I	I	I	R
Corporate Communication		I	I	I	I	R
Management		I	I	I	A	A

- (R) Responsible

:

Person who is responsible for executing or doing the activity

Orang yang bertanggung jawab melaksanakan atau melakukan kegiatan tersebut
- (A) Accountable

:

Person who owns, approves, and is the final decision maker for the activity

Orang yang memiliki, menyetujui, dan merupakan pengambil keputusan akhir atas kegiatan tersebut
- (C) Consulted

:

Person who can provide further information or feedback for performing the activity

Orang yang dapat memberikan informasi lebih lanjut atau umpan balik untuk melakukan aktivitas
- (I) Informed

:

Person who only needs to be informed the activity's progress or status

Orang yang hanya perlu diberitahu perkembangan atau status kegiatan

2.2. Detail of Responsibilities

This table below describes the Roles and Responsibilities. The R&R below are based on functional structure and should be updated according to organization environment

2.2 Rincian Tanggung Jawab

Tabel di bawah ini menjelaskan Peran dan Tanggung Jawab. Tabel di bawah ini didasarkan pada struktur fungsional dan harus diperbarui sesuai dengan lingkungan organisasi.

Function Fungsi	Responsibilities Tanggung Jawab
Cyber Security Incident Response Team (CSIRT)	<ul style="list-style-type: none">• Team consists Cyber Security Risk, IT, Compliance & Legal, Business Unit, Business Continuity Coordinator and other related unit that provides Bank with services and support surrounding the assessment, management, and prevention of cybersecurity-related emergencies, as well as coordination of incident response efforts.• Complete actions and associated checklists contained in this Incident Response Playbook.• Ensure Incident Response Plan is followed.• Coordinated by Cyber Security Risk unit.• Team terdiri dari Cyber Security Risk, IT, Compliance & Legal, Business Unit, Business Continuity Coordinator dan unit terkait lainnya yang memberikan layanan dan dukungan kepada Bank seputar penilaian, pengelolaan, dan pencegahan keadaan darurat terkait keamanan siber, serta koordinasi upaya respons insiden.• Menyelesaikan tindakan dan daftar periksa terkait yang terdapat dalam Buku Panduan Respons Insiden ini.• Memastikan Incident Response Plan dijalankan• Dikordinasikan oleh unit Cyber Risk
IT Security Operation Management	<ul style="list-style-type: none">• Do coordination with CSIRT Coordinator• Manage and implement configuration for Cyber Security tools and perimeters (Firewall, IPS, Antivirus, Proxy, NAC, MDM, CASB, DLP etc)• Perform assessment to identify security threat by utilizing threat intelligence report• Manage Privilege Access Management (PAM) and User Access Matrix• Melakukan kordinasi dengan CSIRT Coordinator• Mengelola dan implementasi konfigurasi perangkat keamanan siber (Firewall, IPS, Antivirus, Proxy, NAC, MDM, CASB, DLP dll)• Melakaukan penilaian untuk identifikasi ancaman keamanan dengan menggunakan laporan dari threat• Mengelola Privilege Access Management (PAM) dan User Access Matrix

IT SOC	<ul style="list-style-type: none"> • Conduct continuous monitoring and analysis of the Bank's network, infrastructure and system by using Cyber Defense Tools (SIEM) • Ensure the availability of log and escalate malicious activities to CSIRT coordinator • Melakukan pemantauan dan analisa secara berkesinambungan terhadap jaringan, infrastructure dan system Bank dengan menggunakan SIEM • Memastikan ketersediaan log dan eskalasikan kejadian berbahaya ke kordinator CSIRT
IT Field / Regional Service Support	<ul style="list-style-type: none"> • Manage and maintain Antivirus in client desktop / laptop • Troubleshoot problem in client desktop / laptop • Mengelola dan memelihara Antivirus pada client desktop / laptop • Menyelesaikan masalah pada client desktop / laptop
IT Operation (Infrastructure, Application, Support)	<ul style="list-style-type: none"> • Manage and maintain infrastructure such as Server, Router and Switch. • Manage and maintain Antivirus in client desktop / laptop • Troubleshoot problem in client desktop / laptop • Manage and maintain operational of IT application • Mengelola dan memelihara infrastructure seperti Server, Router dan Switch. • Mengelola dan memelihara Antivirus in client desktop / laptop • Menyelesaikan masalah pada client desktop / laptop • Mengelola dan memelihara operasional aplikasi IT
Cyber Security Risk	<ul style="list-style-type: none"> • Develop and implement Cyber Security awareness and training program • Prepare and develop incident report and notification to Regulator • Act as CSIRT coordinator or lead in the security incident response process • Membuat dan implelementasi kesadaran terhadap keamanan siber dan program latihan • Menyiapkan dan membuat laporan insiden dan pemberitahuan ke Regulator • Bertindak sebagai coordinator CSIRT atau memimpin proses respons insiden keamanan
IT Risk Management	<ul style="list-style-type: none"> • Perform coordination with Cyber Security Risk Management to analyze and identify incident impact. • Melakukan koordinasi dengan Cyber Security Risk Management dalam melakukan analisa dan identifikasi dampak insiden yang terjadi.

Compliance	<ul style="list-style-type: none"> • Internal messaging for stakeholders, business owners and end-users • External messaging for Regulator (OJK and BI) • Internal komunikasi Dengan pemangku kepentingan, pemilik bisnis, dan pengguna akhir • Komunikasi eksternal dengan Regulator (OJK dan BI)
Corporate Communication	<ul style="list-style-type: none"> • External messaging for Customer, including press conference • Pesan eksternal untuk Pelanggan, termasuk konferensi pers
Business / System Owner	<ul style="list-style-type: none"> • Specialist system related technical advice. • Service impact assessments. • Spesialis sistem perihal saran teknis • Penilaian dampak layanan
Management	<ul style="list-style-type: none"> • Representative from management who will take responsibility to take strategic decision • Perwakilan dari manajemen yang akan bertanggung jawab mengambil keputusan strategis
External Service Providers (i.e. SOC, ISP, Cloud service provider, PaaS, SaaS etc.)	<ul style="list-style-type: none"> • Coordination of incident remediation action for external services as required. • Communication managed through internal relationship owners (e.g. Service Delivery Team) • Specialist resource related technical advice. • Advice and assistance as requested by CSIRT. Advice and assistance as requested by CSIRT. • Koordinasi tindakan remediasi insiden untuk layanan eksternal sesuai kebutuhan • Komunikasi melalui pemilik hubungan internal (Service Delivery Team) • Spesialis sumber daya perihal saran teknis • Memberikan anjuran dan bantuan sesuai permintaan dari CSIRT

3. Ransomware Incident Response Phase

This Ransomware playbook moves logically through each incident response step from initiation to event closure using the overarching organization Cyber Security Incident Response phases. Although playbook activities might be followed in sequence as each one builds upon the other, it does not always happen like that. Some activities might happen at the same time or even repeatedly along the duration of the incident. The phases are explained briefly in the table below. Some of the activities within those phases might happen in parallel to respond to the incident more effectively.

3. Fase Ransomware Incident Response

Playbook Ransomware ini bergerak secara logis melalui setiap langkah respons insiden mulai dari inisiasi hingga penutupan kejadian menggunakan fase Respons Insiden Keamanan Siber organisasi yang menyeluruh. Meskipun aktivitas playbook mungkin diikuti secara berurutan karena masing-masing aktivitas saling melengkapi, namun tidak selalu terjadi seperti itu. Beberapa aktivitas mungkin terjadi pada waktu yang sama atau bahkan berulang kali sepanjang durasi kejadian. Fase-fase ini dijelaskan secara singkat pada tabel di bawah ini. Beberapa aktivitas dalam fase tersebut mungkin dilakukan secara paralel untuk merespons insiden tersebut dengan lebih efektif.



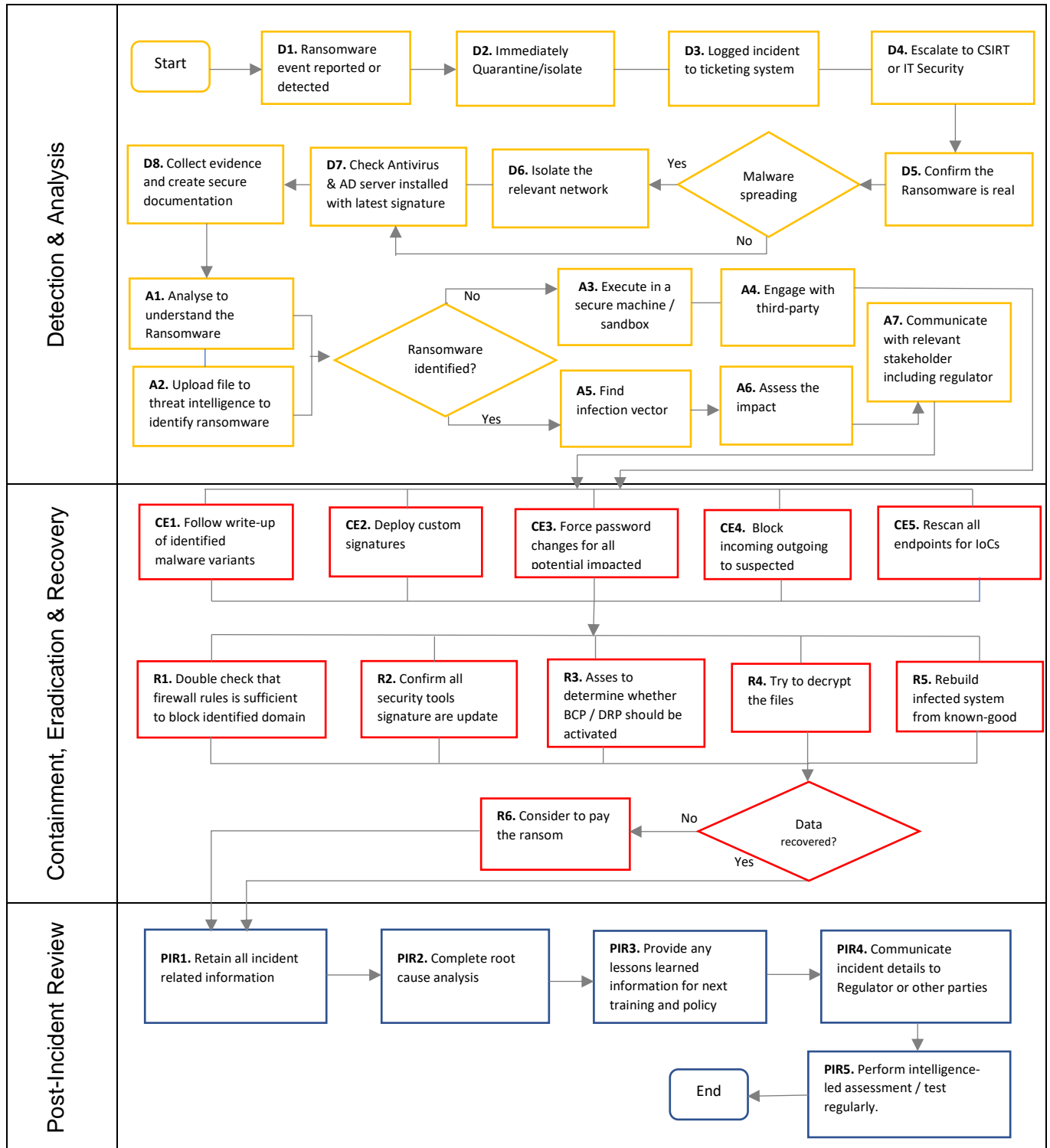
Phase Fase	Description Deskripsi
Preparation	<p>The preparation phase is handled before an actual incident happens. It includes establishing the people, process, and technology to effectively respond to information security incidents.</p> <p>In order to prepare organization readiness to encounter Ransomware incident, there are suggested activities to be performed:</p> <ol style="list-style-type: none">1. Define and implement security preventive control (ie: access rule, active scanning, deploy new signature).2. Conduct security awareness training to refresh current cyber security threat to all employees.3. Perform simulation testing / table top exercise and review testing result. <p>Tahap persiapan ditangani sebelum kejadian sebenarnya terjadi. Hal ini mencakup pembentukan sumber daya manusia, proses, dan teknologi untuk merespons insiden keamanan informasi secara efektif.</p> <p>Untuk mempersiapkan kesiapan organisasi menghadapi insiden Ransomware, ada beberapa kegiatan yang disarankan untuk dilakukan:</p> <ol style="list-style-type: none">1. Mendefinisikan dan menerapkan kontrol preventif keamanan (yaitu: aturan akses, pemindaian aktif, penerapan tanda tangan baru).

	<p>2. Menyelenggarakan pelatihan kesadaran keamanan untuk mengingatkan kembali ancaman keamanan siber yang ada saat ini kepada seluruh karyawan.</p> <p>3. Melakukan pengujian simulasi/latihan table top dan meninjau hasil pengujian</p>
Detection & Analysis	<p>This phase details how cyber security incidents are identified, scoped, categorized, and prioritized, as well as how stakeholders are notified depending on the incident priority. Further, investigation of the incident is conducted at this phase.</p> <p>Fase ini merinci bagaimana insiden keamanan siber diidentifikasi, diberi cakupan, dikategorikan, dan diprioritaskan, serta bagaimana pemangku kepentingan diberi tahu berdasarkan prioritas insiden tersebut. Selanjutnya, penyelidikan atas insiden tersebut dilakukan pada tahap ini.</p>
Containment, Eradication & Recovery	<p>This phase details the steps to limit the damage and stop the incident including but not limited to disconnecting system from the network, disconnecting network connections of BTPN to and/or from (subsidiaries and/or SMBC groups and/or third parties) etc., identify and remediate the root cause of the incident, and recover to normal operational status.</p> <p>Fase ini merinci langkah-langkah untuk membatasi kerusakan dan menghentikan insiden termasuk namun tidak terbatas kepada memutuskan sambungan sistem dari jaringan, memutuskan koneksi jaringan BTPN ke dan/atau dari (anak Perusahaan dan/atau grup SMBC dan/atau pihak ketiga) dll, mengidentifikasi dan memulihkan akar penyebab insiden, dan memulihkan status operasional normal.</p>
Post Incident Activity	<p>This phase details post incident steps, including further notification to affected customers and/or regulators, and conducting post incident reviews to identify lessons learned.</p> <p>Fase ini merinci langkah-langkah pasca insiden, termasuk pemberitahuan lebih lanjut kepada pelanggan dan/atau regulator yang terkena dampak, dan melakukan tinjauan pasca insiden untuk mengidentifikasi pembelajaran.</p>

The detail of ransomware flowchart is described in the next page.

Detail diagram alur ransomware dijelaskan di halaman berikutnya.

3.1 Ransomware Flowchart



3.2 Technology Matrix

The table below lists organization technologies that can be used in each phase of the Incident Response process when dealing with Ransomware incidents.

3.2 Technology Matrix

Tabel di bawah mencantumkan teknologi organisasi yang dapat digunakan dalam setiap fase proses Respons Insiden ketika menangani insiden Ransomware.

Category	Technology	Detection	Analysis	Containment	Eradication	Recovery
Asset Management	ServiceNow					
Monitoring System	Splunk					
	Solarwind					
Threat Intelligence	Cyfirma					
Endpoint Protection	Sophos					
	Symantec					
Identity and Access Management	Active Directory					
	Beyond Trust					
Firewall	Checkpoint Firewall					
	PaloAlto Firewall					
	Tipping Point					
Proxy	Mcafee Proxy					
IPS	Fortigate IPS					
Anti-DDOS	Cloudflare					
Web App Firewall						
Email Security	Cisco Ironport					
Patch Management	Bigfix					
Data Security	Forcepoint					
Vulnerability Scanner	Tenable					
Backup / Restore	AWS EC2 Snapshot					
	Backup Solution					
	OneDrive					

4. Ransomware Playbook Detail

4.1 Detection and Analysis

Detection & Analysis phase includes two distinct sub-sections:

- **Detection** – An event has occurred and has been reported.
- **Analysis** – Analyze activity logs, relevant reports, and documentation to identify the actions taken by the attacker and determine the scope of the incident

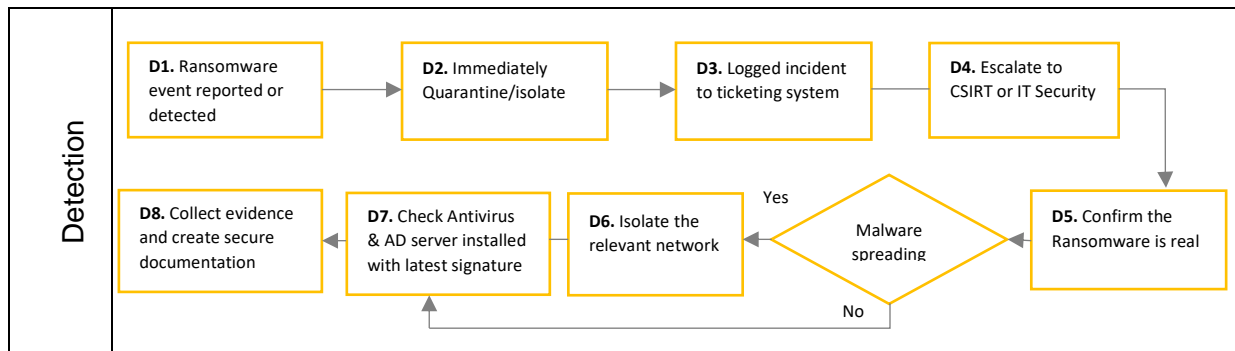
4. Detail Playbook Ransomware

4.1 Detection and Analysis

Fase Detection & Analysis mencakup dua sub-bagian berbeda:

- **Detection** – Suatu peristiwa telah terjadi dan telah dilaporkan.
- **Analysis** – Analisis log aktivitas, laporan yang relevan, dan dokumentasi untuk mengidentifikasi tindakan yang diambil oleh penyerang dan menentukan cakupan insiden.

4.1.1 Detection



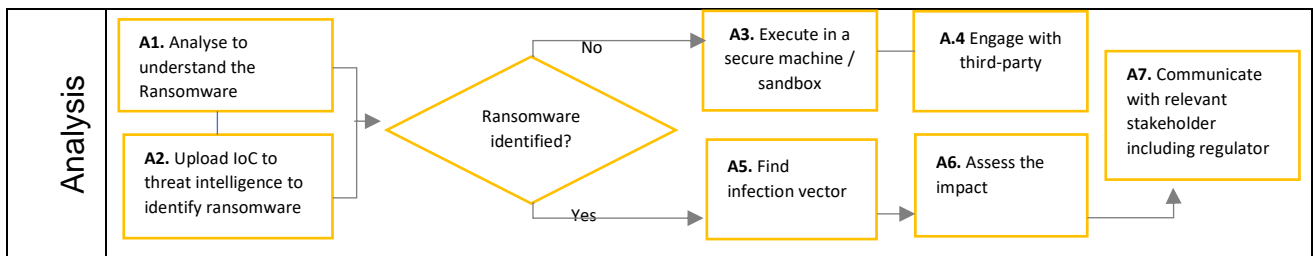
ID	Description	Resources	Responsible	Who am I might need to contact?
D1	<p>A Ransomware incident has been reported. The incident report or notification might be come from:</p> <ul style="list-style-type: none"> • User (Employee) • IT Operation • Business / System Owner • IT Helpdesk / Service desk <p>Insiden Ransomware telah dilaporkan. Laporan atau pemberitahuan kejadian dapat berasal dari:</p> <ul style="list-style-type: none"> • User (Pegawai) • IT Operation • Business / System Owner • IT Helpdesk / Service desk 	<p>Tools that can be used:</p> <ul style="list-style-type: none"> • Media communication channel (Microsoft Teams, Slack, etc) <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> • Kanal media komunikasi (Microsoft Teams, Slack, etc) 	<p>User who first discovered the ransomware incident</p> <p>User yang menemukan atau melaporkan ransomware</p>	<p>You might need to contact:</p> <ul style="list-style-type: none"> • IT Security Operation Management <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> • IT Security Operation Management

ID	Description	Resources	Responsible	Who am I might need to contact?
D2	<p>Immediately quarantine/isolate affected endpoint or machine. Decision to be made based on initial information available.</p> <ul style="list-style-type: none"> Remove network and data cables, USBs, and dongles. Disable affected user accounts. Contain/Quarantine affected files and systems. Disable wireless connections such as Wi-Fi and Bluetooth. <p>Segera karantina/isolasi titik akhir atau mesin yang terkena dampak. Keputusan harus diambil berdasarkan informasi awal yang tersedia.</p> <ul style="list-style-type: none"> Lepas kabel jaringan dan data, USB dan dongle Nonaktifkan akun pengguna yang terdampak Karantina file dan sistem yang terdampak <p>Nonaktifkan koneksi nirkabel seperti Wi-Fi dan Bluetooth</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Active Directory Endpoint Protection <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> Active Directory Endpoint Protection 	<ul style="list-style-type: none"> IT Security Operation Management IT Field/Regional Service Support <ul style="list-style-type: none"> IT Security Operation Management IT Field/Regional Service Support 	<p>You might need to contact:</p> <ul style="list-style-type: none"> User who report the incident <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> User yang melaporkan insiden
D3	<p>Log the incident into organization ticketing system that includes at least date and time of report and a brief incident description.</p> <p>Record all information available, including:</p> <ul style="list-style-type: none"> Pictures of the screen of the affected system(s) using smartphone showing things like ransom messages, encrypted files, system error messages, etc. Get more clarifications from user impacted <p>Catat insiden tersebut ke dalam sistem tiket organisasi yang mencakup setidaknya tanggal dan waktu laporan serta deskripsi singkat insiden.</p> <p>Catat semua informasi yang tersedia, termasuk:</p> <ul style="list-style-type: none"> Gambar layar system yang terkena dampak menggunakan smartphone yang menampilkan hal-hal seperti pesan tebusan, file terenkripsi, pesan kesalahan sistem dan lainnya. Dapatkan lebih banyak klarifikasi dari pengguna yang terkena dampak 	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Ticketing System <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> Ticketing System 	<ul style="list-style-type: none"> IT Security Operation Management IT Field/Regional Service Support <ul style="list-style-type: none"> IT Security Operation Management 	<p>You might need to contact:</p> <ul style="list-style-type: none"> User who reports the incident <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> User yang melaporkan insiden
D4	<p>Escalate to CSIRT.</p> <p>Establish bridge details and coordinate meetings, depending on severity of incident.</p> <p>Ekskalasikan ke CSIRT.</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Ms Team Email <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> MS Teams Email 	<p>IT Security Operation Management</p> <p>IT Security Operation Management</p>	<p>N/A</p> <p>N/A</p>

ID	Description	Resources	Responsible	Who am I might need to contact?
	Tetapkan detail dan koordinasikan pertemuan, tergantung pada tingkat keparahan insiden.			
D5	<p>Confirm the Ransomware incident is real and active.</p> <ul style="list-style-type: none"> Check if file extensions have been modified, for instance, .lock or .crypt. Check if files are really affected. Check for clues like the name of the Ransomware and search on the Internet. Check security logs: Endpoint protection console alerting and unknown/unexpected network traffic. Determine which devices have been affected <p>Konfirmasi bahwa insiden Ransomware itu nyata dan aktif.</p> <ul style="list-style-type: none"> Cek bila ekstensi file sudah dimodifikasi, contohnya, .lock atau .crypt. Cek apakah file benar-benar terdampak Check for clues like the name of the Ransomware and search on the Internet. Periksa petunjuk seperti nama Ransomware dan cari di internet Periksa log keamanan: konsol endpoint protection memberikan peringatan tidak diketahui/tidak terduga lalu lintas jaringan Tentukan perangkat yang telah terdampak 	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Endpoint Protection Monitoring system <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> Endpoint Protection Monitoring system 	<ul style="list-style-type: none"> CSIRT IT Field/Regional Service Support <ul style="list-style-type: none"> CSIRT IT Field/Regional Service Support 	<p>You might need to contact:</p> <ul style="list-style-type: none"> Affected users Business/System Owners <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> User terdampak Business/System Owners
D6	<p>If the infection is spreading, isolate the relevant network segment(s) either physically or logically through implementing network access controls such as firewall rules or through access rule in switch or blocking ports.</p> <p>Jika infeksi menyebar, isolasi segmen jaringan yang relevan baik secara fisik atau logis melalui penerapan kontrol akses jaringan seperti aturan firewall atau melalui aturan akses di port switch atau pemblokiran.</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Switch Firewall <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> Switch Firewall 	<ul style="list-style-type: none"> CSIRT IT Infrastructure Operation <ul style="list-style-type: none"> CSIRT IT Infrastructure Operation 	<p>You might need to contact:</p> <ul style="list-style-type: none"> Business/System Owners Affected User External Service Providers <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> Business/System Owners User terdampak Penyedia Jasa Eksternal
D7	Check to ensure Antivirus and Active Directory server has been installed with latest / updated Antivirus signature	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Endpoint Protection 	CSIRT	<p>You might need to contact:</p> <ul style="list-style-type: none"> IT Infrastructure Operation

ID	Description	Resources	Responsible	Who am I might need to contact?
	Periksa untuk memastikan server Antivirus dan Active Directory telah diinstal dengan signature Antivirus terbaru/terupdate.	Alat yang bisa digunakan: <ul style="list-style-type: none"> Endpoint Protection 	CSIRT	Anda mungkin perlu menghubungi: IT Infrastructure Operation
D8	<p>Collect and preserve evidence for forensics purpose. Define and create a secure location to store all information, documentation and evidence related to the incident. Ensure that only authorised people will have access to the location.</p> <p>Mengumpulkan dan menyimpan bukti untuk tujuan forensik. Menetapkan dan membuat lokasi yang aman untuk menyimpan semua informasi, dokumentasi dan bukti-bukti yang berkaitan dengan kejadian tersebut. Pastikan hanya orang yang berwenang yang dapat mengakses lokasi tersebut.</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> OneDrive Sharepoint <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> OneDrive Sharepoint 	<p>CSIRT</p> <p>CSIRT</p>	<p>You might need to contact:</p> <ul style="list-style-type: none"> Business/System Owners Affected User External Service Providers <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> Business/System Owners User terdampak Penyedia Jasa Eksternals

4.1.2 Analysis



The results of the analysis will be used to support the containment, eradication, and recovery process.

Hasil analisis akan digunakan untuk mendukung proses pembendungan, pemberantasan, dan pemulihan.

ID	Description	Resources	Responsible	Who am I might need to contact?
A1	<p>Analyze to understand the Ransomware. Look for Indicators of Compromise (IoC), review alerts and available information to ensure you know the ransomware family and variant.</p> <p>Check:</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Endpoint Protection 	CSIRT	<p>You might need to contact:</p> <ul style="list-style-type: none"> Affected users Business/System Owners SOC Team

ID	Description	Resources	Responsible	Who am I might need to contact?
	<ul style="list-style-type: none"> Graphical user interfaces (GUIs) for the malware itself. Text or html files, sometimes opened automatically after encryption. Image files, often as wallpaper on infected systems. Contact emails in encrypted file extensions. Pop-ups after trying to open an encrypted file. <p>Analisis untuk memahami Ransomware. Cari Indicators of Compromise (IoC), tinjau alert dan informasi yang tersedia untuk memastikan Anda mengetahui family dan varian ransomware.</p> <p>Check:</p> <ul style="list-style-type: none"> Graphical user interfaces (GUIs) dari malware tersebut File text atau html, terkadang otomatis terbuka setelah enkripsi File gambar, sering kali sebagai wallpaper pada sistem yang terinfeksi. Kontak emails pada file terenkripsi. Pop-ups setelah mencoba membuka file yang terenkripsi. 	<p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> Endpoint Protection 	CSIRT	<ul style="list-style-type: none"> IT Infrastructure Operation <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> User terdampak Business/System Owners SOC Team IT Infrastructure Operation
A2	<p>Upload IoCs to automated categorization services like Crypto Sheriff, ID Ransomware, or VirusTotal to identify Ransomware variant.</p> <p>Look up for Ransomware write-up for the specific Ransomware variants identified. This will be useful during containment and eradication steps.</p> <p>Unggah IoC ke layanan kategorisasi otomatis seperti Crypto Sheriff, ID Ransomware, atau VirusTotal untuk mengidentifikasi varian Ransomware.</p> <p>Cari artikel Ransomware untuk varian Ransomware spesifik yang teridentifikasi. Hal ini akan berguna dalam langkah pembendungan dan penghapusan.</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Virus Total Crypto Sheriff - https://www.nomoreransom.org/crypto-sheriff.php ID Ransomware - https://id-ransomware.malwarehunterteam.com/ Threat Intelligence (Cyfirma) <p>Note: This above are example</p> <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> Virus Total Crypto Sheriff - https://www.nomoreransom.org/crypto-sheriff.php ID Ransomware - https://id-ransomware.malwarehunterteam.com/ Threat Intelligence (Cyfirma) 	CSIRT	<p>You might need to contact:</p> <ul style="list-style-type: none"> SOC Team IT Infrastructure Operation Legal <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> SOC Team IT Infrastructure Operation Legal

ID	Description	Resources	Responsible	Who am I might need to contact?
		Catatan: List diatas merupakan contoh		
A3	<p>If Ransomware type cannot be identified, execute it in a secure environment or sandbox, segregated from the corporate network, to determine its behavior and get a list of Indicators of Compromise (IoC).</p> <p>Jika jenis Ransomware tidak dapat diidentifikasi, jalankan di system yang aman atau sandbox, terpisah dari jaringan perusahaan, untuk menentukan perilakunya dan mendapatkan daftar Indikator Kompromi (IoC).</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Cloud and Virtual environment Endpoint Protection Sandbox <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> Cloud and Virtual environment Endpoint Protection Sandbox 	<p>CSIRT</p> <p>CSIRT</p>	<p>You might need to contact:</p> <ul style="list-style-type: none"> IT Infrastructure Operation Incident Response and Forensic Partner <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> IT Infrastructure Operation Incident Response dan Forensic Partner
A4	<p>Engage with third-party, for example McAfee, Microsoft and etc, to determine behavior of Ransomware.</p> <p>Mengajak third-party, contohnya McAfee, Microsoft dan lainnya untuk menentukan sifat dari ransomware.</p>	<p>N/A</p> <p>N/A</p>	<p>CSIRT</p> <p>CSIRT</p>	<p>You might need to contact:</p> <ul style="list-style-type: none"> External Service Provider <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> Penyedia Jasa Eksternal
A5	<p>Find the infection vector. Review available information sources to determine source of compromise (which generally will be removable media, web, or e-mail).</p> <p>Temukan vektor infeksi. Tinjau sumber informasi yang tersedia untuk menentukan sumber penyusupan (yang umumnya berupa media yang dapat dipindahkan, web, atau email).</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Monitoring system Endpoint Protection Firewalls, IPS and Proxy Email security <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> Monitoring system Endpoint Protection Firewalls, IPS and Proxy Email security 	<p>CSIRT</p> <p>CSIRT</p>	<p>N/A</p> <p>N/A</p>
A6	<p>Assess the impact to prioritize, escalate and motivate resources. The principal risk type to be assessed must follow organization matrix.</p> <ul style="list-style-type: none"> Is there any financial loss? 	<p>Useful documentation:</p> <ul style="list-style-type: none"> Risk Management Framework or Policy 	<ul style="list-style-type: none"> IT Risk Management Cyber Security Risk 	<p>You might need to contact:</p> <ul style="list-style-type: none"> Business/System Owners

ID	Description	Resources	Responsible	Who am I might need to contact?
	<ul style="list-style-type: none"> Is there any impact to Operational & Technology? Is there any reputational impact? Is there any impact to Regulatory Compliance? <p>Kaji dampaknya untuk memprioritaskan, meningkatkan, dan memotivasi sumber daya. Jenis risiko utama yang akan dinilai harus mengikuti matriks organisasi.</p> <ul style="list-style-type: none"> Apakah ada kerugian finansial? Apakah ada dampak pada operasional dan teknologi? Apakah ada dampak reputasi? Apakah ada dampak kepatuhan pada regulator? 	<p>Dokumen yang dapat digunakan:</p> <ul style="list-style-type: none"> Risk Management Framework or Policy 	<ul style="list-style-type: none"> IT Risk Management Cyber Security Risk 	<p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> Business/System Owners
A7	<p>Communicate with relevant stakeholders, including Regulator.</p> <p>Prepare and submit Incident Cyber notification to OJK. Please refer to Appendix 5.1</p> <p>Komunikasikan dengan stakeholder termasuk Regulator.</p> <p>Menyiapkan dan menyampaikan pemberitahuan Insiden Siber kepada OJK. Silakan lihat Lampiran 5.1</p>	<p>Useful documentation:</p> <ul style="list-style-type: none"> SEOJK 29 / 2022 <p>Dokumen yang dapat digunakan:</p> <ul style="list-style-type: none"> SEOJK 29 / 2022 	<ul style="list-style-type: none"> Cyber Security Risk Cyber Security Risk 	<p>You might need to contact:</p> <ul style="list-style-type: none"> Compliance Incident Management Team (IMT Head) <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> Compliance Incident Management Team (IMT Head)

4.2 Containment, Eradication and Recovery

Containment, Eradication & Recovery phase includes two distinct sub-sections:

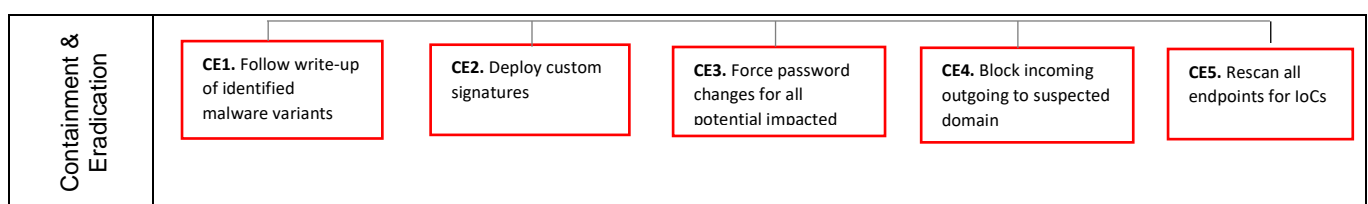
- **Containment & Eradication**– The effects of an active Ransomware event are successfully contained and purged
- **Recovery** – Checking that the eradication process was effective and that systems are fully restored to normal operational function.

4.2 Containment, Eradication and Recovery

Fase Containment, Eradication & Recovery memiliki dua sub-bagian:

- **Containment & Eradication**– Efek dari peristiwa Ransomware yang aktif berhasil diatasi dan dibersihkan
- **Recovery** – Memeriksa apakah proses pemberantasan sudah efektif dan sistem sudah pulih sepenuhnya ke fungsi operasional normal.

4.2.1 Containment and Eradication

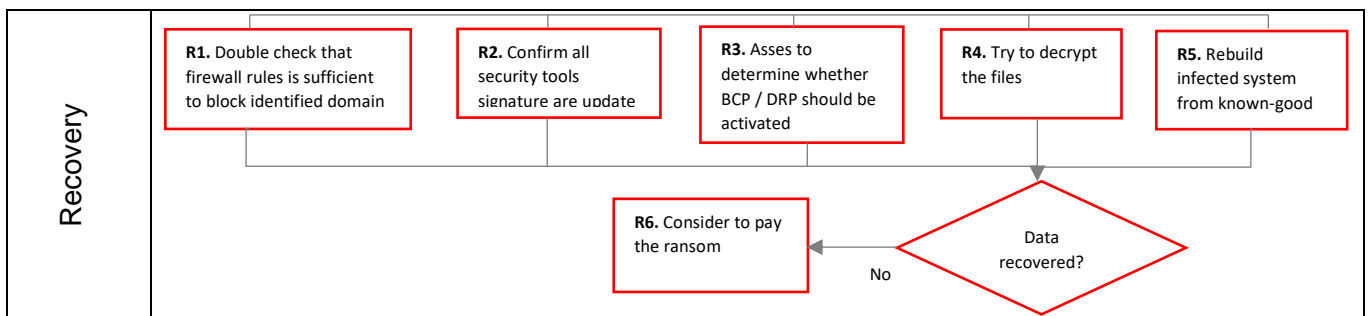


ID	Description	Resources	Responsible	Who am I might need to contact?
CE1	<p>Follow write-up of identified malware variants, if available. These will provide you known successful steps to respond to known Ransomware variants.</p> <p>Ikuti petunjuk dari ransomware yang teridentifikasi, jika ada. Ini akan memberi Anda langkah-langkah sukses yang diketahui untuk merespons varian Ransomware yang diketahui.</p>	<p>N/A</p> <p>N/A</p>	<p>CSIRT</p> <p>CSIRT</p>	<p>N/A</p> <p>N/A</p>
CE2	<p>Deploy custom signatures and block executables.</p> <ul style="list-style-type: none"> Deploy custom signatures that will block all identified IoCs to endpoint protection and network security tool. Block identified executables using endpoint protection and application controls to prevent execution on other devices. 	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Endpoint Protection Firewall IPS Proxy Email security 	CSIRT	<p>You might need to contact:</p> <ul style="list-style-type: none"> External Service Providers

ID	Description	Resources	Responsible	Who am I might need to contact?
	<p>Terapkan signature khusus dan blokir file yang dapat dieksekusi.</p> <ul style="list-style-type: none"> • Terapkan signature khusus yang akan memblokir semua IoC yang teridentifikasi ke alat perlindungan endpoint dan keamanan jaringan. • Blokir file executable yang teridentifikasi menggunakan perlindungan endpoint dan kontrol aplikasi untuk mencegah eksekusi pada perangkat lain. 	<p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> • Endpoint Protection • Firewall • IPS • Proxy • Email security 	CSIRT	<p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> • Penyedia Jasa Eksternal
CE3	<p>Force a password change on all potentially compromised user accounts.</p> <p>Rubah password untuk semua akun yang berpotensi terdampak.</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> • Active Directory <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> • Active Directory 	<p>CSIRT</p> <p>CSIRT</p>	<p>You might need to contact:</p> <ul style="list-style-type: none"> • IT Infrastructure Operation (for account server) • System Administration Management (for user account) <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> • IT Infrastructure Operation (untuk akun server) • System Administration Management (untuk akun user)
CE4	<p>Block both incoming and outgoing traffic to identified fraudulent addresses and domains.</p> <p>Blokir koneksi keluar masuk ke domain yang dicurigai.</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> • Firewall • IPS • Proxy <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> • Firewall • IPS • Proxy 	<p>CSIRT</p> <p>CSIRT</p>	<p>N/A</p> <p>N/A</p>
CE5	<p>Rescan all endpoints for IoCs and lateral movement.</p> <p>If new findings arise, revisit Analysis steps of this playbook and refer to the actions.</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> • Endpoint Protection • Monitoring system • Vulnerability Scanner 	CSIRT	N/A

ID	Description	Resources	Responsible	Who am I might need to contact?
	<p>Pindai ulang semua endpoint untuk IoCs</p> <p>Jika ada temuan baru, tinjau kembali langkah-langkah Analisis dalam playbook ini dan lihat tindakannya.</p>	<p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> Endpoint Protection Monitoring system Vulnerability Scanner 	CSIRT	N/A

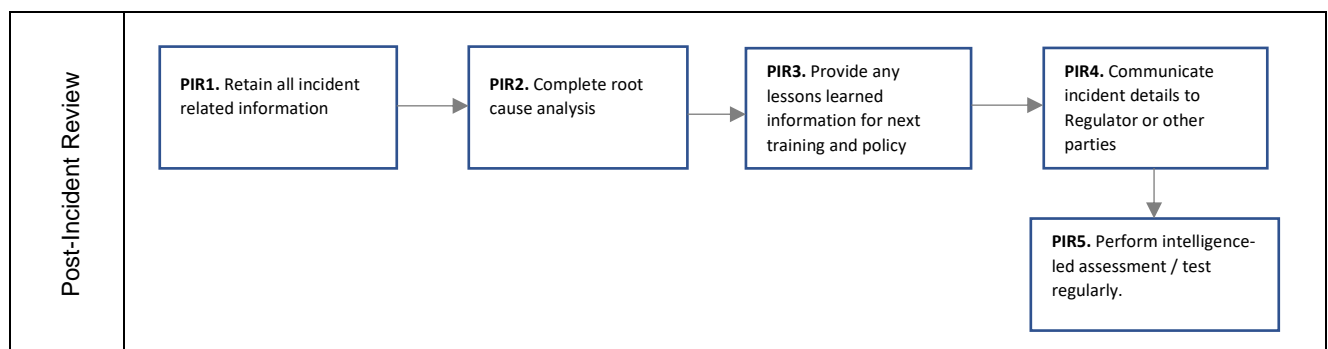
4.2.2 Recovery



ID	Description	Resources	Responsible	Who am I might need to contact?
R1	<p>Double check that firewall rules/network access controls are sufficient to block both incoming and outgoing traffic to identified fraudulent addresses.</p> <p>From an isolated and safe controlled environment, attempt to contact the hosts of the fraudulent content to ensure it is blocked or removed.</p> <p>Periksa kembali apakah aturan firewall/kontrol akses jaringan cukup untuk memblokir lalu lintas masuk dan keluar ke alamat palsu yang teridentifikasi.</p> <p>Dari sistem yang terkendali dan terisolasi serta aman, cobalah menghubungi host konten palsu untuk memastikan konten tersebut diblokir atau dihapus.</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Firewall IPS Proxy <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> Firewall IPS Proxy 	<p>CSIRT</p> <p>CSIRT</p>	<p>N/A</p> <p>N/A</p>
R2	<p>Confirm all security technologies have the latest signatures deployed to detect malware variant. If required, deploy custom signatures or definitions.</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Monitoring system Endpoint protection Email security Firewalls IPS Proxy 	CSIRT	N/A

ID	Description	Resources	Responsible	Who am I might need to contact?
R5	<p>Rebuild infected systems from known-good media. If decrypting does not work and known-clean backup is available, securely wipe the compromised system(s), and reinstall the operating system, service packs and patch levels to the most up to date available.</p> <p>Reinstalling new operating system must follow standard configuration and policy of organization.</p> <p>Bangun kembali sistem yang terinfeksi dari known-good media. Jika dekripsi tidak berhasil dan cadangan yang diketahui bersih tersedia, hapus sistem yang disusupi dengan aman, dan instal ulang sistem operasi, paket layanan, dan tingkat patch ke tingkat paling mutakhir yang tersedia.</p> <p>Menginstal ulang sistem operasi baru harus mengikuti konfigurasi standar dan kebijakan organisasi.</p>	<p>Tools that can be used:</p> <ul style="list-style-type: none"> Virtual environment Backup System Vulnerability Scanner <p>Alat yang bisa digunakan:</p> <ul style="list-style-type: none"> Virtual environment Backup System Vulnerability Scanner 	<ul style="list-style-type: none"> CSIRT IT Infrastructure Operation IT Regional / Field Service Support CSIRT IT Infrastructure Operation IT Regional / Field Service Support 	<p>You might need to contact:</p> <ul style="list-style-type: none"> Business Owner <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> Business Owner
R6	<p>For irrecoverable critical assets/data you might consider paying the ransom.</p> <ul style="list-style-type: none"> Consider the Company policies. Understand financial, legal, and regulatory implications based on risk assessment in Analysis phase <p>Untuk aset/data penting yang tidak dapat dipulihkan, Anda mungkin mempertimbangkan untuk membayar uang tebusan.</p> <ul style="list-style-type: none"> Pertimbangkan kebijakan perusahaan Memahami implikasi finansial, hukum dan peraturan berdasarkan penilaian risiko pada tahapan analisis 	<p>N/A</p> <p>N/A</p>	<ul style="list-style-type: none"> CSIRT (as coordinator) Business Owner Management CSIRT (sebagai kordinator) Business Owner Management 	<p>You might need to contact:</p> <ul style="list-style-type: none"> Legal Compliance <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> Legal Compliance

4.3 Post Incident Review



ID	Description	Resources	Responsible	Who am I might need to contact?
PIR1	<p>Retain all incident related information, including incident response log sheet, evidence handling sheets, information gathering sheets and evidence in a secure location for future reference.</p> <p>Simpan semua informasi terkait insiden, termasuk lembar catatan respons insiden, lembar penanganan bukti, lembar pengumpulan informasi, dan bukti di lokasi yang aman untuk referensi di masa mendatang.</p>	<p>N/A</p> <p>N/A</p>	<p>CSIRT</p> <p>CSIRT</p>	<p>You might need to contact:</p> <ul style="list-style-type: none"> Affected users Business/System Owners IT Risk Management <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> User terdampak Business/System Owners IT Risk Management
PIR2	<p>Complete root cause analysis.</p> <p>Selesaikan analisis akar masalah.</p>	<p>N/A</p> <p>N/A</p>	<p>CSIRT</p> <p>CSIRT</p>	<p>N/A</p> <p>N/A</p>
PIR3	<p>Provide any 'lessons learned' information to allow updating of security education and training materials. For example:</p> <ul style="list-style-type: none"> Malware infection identification indicators. Describe current/prevalent Malware attacks. Warn against clicking on links, opening attachments, or connecting unknown devices. Develop case studies and consequences. <p>Buat informasi 'lesson-learned' untuk memungkinkan pembaruan materi edukasi dan pelatihan keamanan. Misalnya:</p> <ul style="list-style-type: none"> Identifikasi indikator infeksi malware. Menjelaskan serangan malware saat ini Peringatkan agar tidak mengklik tautan, membuka lampiran, atau menghubungkan perangkat yang tidak dikenal. Mengembangkan studi kasus dan konsekuensinya. 	<p>N/A</p> <p>N/A</p>	<p>CSIRT</p> <p>CSIRT</p>	<p>You might need to contact:</p> <ul style="list-style-type: none"> Service Desk Human Resource Affected users Business/System Owners <p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> Service Desk Human Resource User terdampak Business/System Owners
PIR4	<p>Communicate incident details outside the organization if considered appropriate (BSSN, Financial Regulator, Customers (PII), etc)</p> <p>Please refer to Appendix 5.2 to submit report of cyber incident to OJK, by the latest 10 working days from the incident date.</p>	<p>N/A</p>	<p>CSIRT</p>	<p>You might need to contact:</p> <ul style="list-style-type: none"> Corporate Communication Compliance Legal Business Owners

ID	Description	Resources	Responsible	Who am I might need to contact?
	<p>Mengkomunikasikan rincian kejadian ke luar organisasi jika dianggap perlu (BSSN, Regulator Keuangan, Pelanggan (PII), dll).</p> <p>Silakan merujuk pada Lampiran 5.2 untuk menyampaikan laporan kejadian siber kepada OJK, selambat-lambatnya 10 hari kerja sejak tanggal kejadian.</p>	N/A	CSIRT	<p>Anda mungkin perlu menghubungi:</p> <ul style="list-style-type: none"> • Corporate Communication • Compliance • Legal • Business Owners
PIR5	<p>Perform intelligence-led assessment / test regularly.</p> <p>Perform specific scenario Ransomware Attack testing based on organization specific condition, process, scenario, and risk appetite.</p> <p>Lakukan intelligence-led assessment / test secara teratur.</p> <p>Lakukan pengujian Serangan Ransomware skenario tertentu berdasarkan kondisi spesifik organisasi, proses, skenario, dan selera risiko.</p>	<p>N/A</p> <p>N/A</p>	<p>CSIRT</p> <p>CSIRT</p>	<p>You might need to contact:</p> <p>External Service Provider</p> <p>Anda mungkin perlu menghubungi:</p> <p>Penyedia Jasa Eksternal</p>

5. Appendix

5. Lampiran

5.1 Initial notification of Cyber Incident

5.1 Notifikasi Awal Insiden Siber

NOTIFIKASI AWAL INSIDEN SIBER

A. INFORMASI BANK

1. Nama Bank :
2. Alamat Kantor Pusat Bank :
3. Nomor Telepon :
4. Nama Narahubung :
5. Nomor Telepon Narahubung :
6. Otoritas/Lembaga Penerima :¹⁾

B. INFORMASI UMUM INSIDEN SIBER

1. Tanggal dan Waktu Terjadinya Insiden Siber: ²⁾
.... / / (dd/mm/yyyy), ... : (hh:mm)
2. Tanggal dan Waktu Insiden Siber Diketahui:
.... / / (dd/mm/yyyy), ... : (hh:mm)
3. Jenis Insiden Siber.....³⁾
4. Titik Serangan.....⁴⁾
5. Respons Awal Bank Pasca Insiden Siber
:.....⁵⁾
6. Penilaian Awal atas Dampak Insiden Siber bagi Bank
:⁶⁾

Keterangan:

- 1) Diisi dengan nama otoritas dan/atau lembaga selain Otoritas Jasa Keuangan yang jugamenerima pelaporan notifikasi awal ini (jika ada).
- 2) Diisi dalam hal Bank telah mengidentifikasi tanggal dan waktu terjadinya insiden siber.
- 3) Memuat informasi mengenai jenis insiden siber. Contoh: *malware, hacking, ransomware, webdefacement, denial of services (DoS)/distributed denial of services (DDoS)*.
- 4) Memuat informasi mengenai nama sistem atau jaringan yang diserang atau mengalami gangguan.
- 5) Memuat informasi mengenai tindakan awal penanganan yang telah dilakukan oleh Bank setelah diketahui terjadinya insiden siber.
- 6) Diisi dalam hal dampak insiden siber telah diidentifikasi (insiden siber dapat berdampak kepada antara lain produk Bank, pihak ketiga, keuangan Bank, dan reputasi Bank).

5.2 Report of Cyber Incident

5.2 Laporan Insiden Siber

LAPORAN INSIDEN SIBER

A. INFORMASI PELAPOR

1. Nama Bank :
2. Alamat Kantor Pusat Bank :
3. Nomor Telepon :
4. Nama Narahubung :
5. Nomor Telepon Narahubung :
6. Tanggal Penyampaian Notifikasi Awal :
.... / / (dd/mm/yyyy)
7. Otoritas/Lembaga Penerima 1)

B. INFORMASI UMUM INSIDEN SIBER²⁾

1. Tanggal dan Waktu Terjadinya Insiden
Siber: ³⁾
.... / / (dd/mm/yyyy), ... : (hh:mm)
2. Tanggal dan Waktu Insiden Siber Diketahui:
.... / / (dd/mm/yyyy), ... : (hh:mm)
3. Jenis Insiden Siber 4)
4. Titik Serangan 5)
5. Respons Awal Bank Pasca Insiden Siber 6)

C. PENILAIAN ATAS DAMPAK INSIDEN SIBER BAGI BANK⁷⁾

1. Penilaian Dampak Insiden Siber terhadap
Ketersediaan dan Operasional Layanan Bank⁸⁾
.....
.....
2. Penilaian Dampak Insiden Siber terhadap Finansial Bank⁹⁾
.....
.....
3. Penilaian Dampak Insiden Siber terhadap Reputasi Bank¹⁰⁾
.....
.....
4. Penilaian Dampak Insiden Siber terhadap Aspek
Hukum dan Kepatuhan Bank¹¹⁾
.....
.....
5. Penilaian Dampak Insiden Siber terhadap Pihak Ketiga¹²⁾
.....
.....

-
6. Penilaian Dampak Lainnya dari Insiden Siber yang Dapat Diidentifikasi oleh Bank
-
-

D. INFORMASI KRONOLOGIS INSIDEN

1. Durasi terjadinya insiden siber.
2. Langkah eskalasi insiden siber yang dilakukan.
3. Langkah penanggulangan insiden siber yang dilakukan.
4. Langkah pemulihan insiden siber yang dilakukan.
5. Keterlibatan pihak ketiga dalam penanggulangan dan pemulihan insiden siber.
6. Pihak yang menerima informasi terkait insiden siber (pemangku kepentingan, contoh: otoritas, mitra layanan, dan nasabah).
7. Informasi pendukung yang digunakan untuk mengidentifikasi serangan siber, jika diketahui. (contoh: alamat IP yang mencurigakan, lalu lintas jaringan yang tidak biasa, tingkat kegagalan autentikasi yang tinggi, dan permintaan *file* secara berulang kali)

E. ANALISIS PENYEBAB TERJADINYA INSIDEN

1. Sumber Serangan:
 - a. Pihak 13)
 - b. Negara Asal..... 14)
 - c. Motif Serangan..... 15)
2. Faktor penyebab insiden..... 16)

F. ANALISIS FINAL

1. Kesimpulan.
2. Langkah Perbaikan.¹⁷⁾
3. Target Waktu Penyelesaian Insiden Siber : / /
(dd/mm/yy) ¹⁸⁾

Keterangan:

- 1) Diisi dengan nama otoritas dan/atau lembaga selain Otoritas Jasa Keuangan yang juga menerima laporan ini (jika ada).
- 2) Berisi informasi yang sesuai dengan informasi yang telah disampaikan pada notifikasi awal, namun dapat ditambahkan atau disesuaikan dengan informasi tambahan jika ada.
- 3) Diisi dalam hal Bank telah mengidentifikasi tanggal dan waktu terjadinya insiden siber.
- 4) Memuat informasi mengenai jenis insiden siber. Contoh: *malware, hacking, ransomware, webdefacement, denial of services (DoS)/distributed denial of services (DDoS)*.
- 5) Memuat informasi mengenai nama sistem atau jaringan yang diserang atau mengalami gangguan.
- 6) Memuat informasi mengenai tindakan awal penanganan yang telah

- dilakukan oleh Bank setelah diketahui terjadinya insiden siber.
- 7) Pada bagian ini informasi yang diberikan berupa penjelasan tambahan dari penilaian awal yang sudah dilakukan oleh Bank saat pelaporan notifikasi awal insiden siber.
 - 8) Diisi dalam hal terdapat dampak terhadap bisnis Bank, termasuk dalam kaitannya dengan ketersediaan dan operasional layanan Bank. Informasi paling sedikit memuat:
 - a. jenis layanan dan/atau nama produk yang terdampak (contoh: layanan *treasury*, *trade finance*, *cash management*, dan layanan perbankan digital); dan
 - b. penjelasan mengenai dampak yang terjadi (jika layanan dan/atau produk yang terdampak lebih dari 1 (satu), maka penjelasan diberikan untuk seluruh layanan dan produk yang terdampak).
 - 9) Diisi dalam hal terdapat dampak finansial dari insiden siber. Informasi paling sedikit memuat:
 - a. hal yang terdampak (contoh: nilai atau volume transaksi, penarikan dana, dan likuiditas Bank); dan
 - b. penjelasan mengenai dampak yang terjadi (jika insiden memberikan dampak bagi lebih dari 1 (satu) hal maka penjelasan diberikan untuk seluruh hal yang terdampak).
 - 10) Diisi dalam hal terdapat dampak terhadap reputasi Bank dari insiden siber (contoh: insiden dipublikasikan oleh media).
 - 11) Diisi dalam hal terdapat dampak terhadap aspek hukum dan kepatuhan (contoh: pelanggaran ketentuan peraturan perundang-undangan dan adanya tuntutan hukum dari pihak terkait).
 - 12) Diisi dalam hal terdapat dampak terhadap pihak ketiga dari Bank. Informasi paling sedikit memuat:
 - a. kategori pihak ketiga (contoh: nasabah, pihak penyedia jasa, dan mitra kerja sama layanan); dan
 - b. penjelasan mengenai dampak yang terjadi (jika insiden memberikan dampak bagi lebih dari 1 (satu) kategori mitra maka penjelasan diberikan untuk seluruh mitra terdampak).
 - 13) Memuat informasi mengenai pihak yang melakukan serangan atau menjadi sumber serangan, antara lain: pihak intern, pihak ekstern atau pihak ketiga (jika diketahui).
 - 14) Memuat informasi mengenai negara asal dari sumber serangan (jika diketahui).
 - 15) Memuat informasi mengenai motif atau tujuan atas serangan yang dilakukan oleh pelaku (jika diketahui).
 - 16) Memuat penjelasan lengkap dari faktor yang menyebabkan terjadinya insiden siber di Bank.
 - 17) Memuat informasi mengenai langkah yang dilakukan Bank untuk mencegah insiden serupa terjadi di masa depan.
 - 18) Diisi dalam hal insiden belum sepenuhnya diselesaikan pada saat menyampaikan laporan kepada Otoritas Jasa Keuangan
 - 19) Memuat informasi mengenai langkah yang dilakukan Bank untuk mencegah insiden serupa terjadi di masa depan.
 - 20) Diisi dalam hal insiden belum sepenuhnya diselesaikan pada saat menyampaikan laporan kepada Otoritas Jasa Keuangan.