securonix

WHITEPAPER

Simplify CERT-In Compliance with Securonix Next-Gen SIEM

Table of Contents

Executive summary

The Indian Computer Emergency Response Team, known as "CERT-In" has issued Direction No. 20(3)/2022-CERT-In to provide directions around information security practices, procedures, prevention, response, and reporting cyber incidents for a safe and trusted internet. This whitepaper focuses on the areas of the Direction that can be met by Securonix SIEM solution. These areas include reporting cyber incidents, providing information to CERT-In when ordered/ requested, and enablement of log collection. This paper will not discuss areas of the Direction in which SIEM or threat detection and response technology cannot be applied, including the use of the network time protocol (NTP), maintenance of customer information, or maintenance of Know Your Customers (KYC) information for financial transactions.

Introduction

The Indian Computer Emergency Response Team is the national agency for incident response for cybersecurity. CERT-In was established under section 70B of the Information Technology Act, 2000 (IT Act) and is responsible for establishing guidelines around cyber incidents. The agency outlines emergency measures for handling cybersecurity incidents and coordinating cybersecurity incident response activities.

Specifically, CERT-In holds the responsibility of performing the following functions:

A. Collection, analysis, and dissemination of information regarding cyber incidents.

B. Forecasting and alerting on cybersecurity incidents.

C. Emergency measures for handling cybersecurity incidents.

D. Coordination of cyber incident response activities.

E. Issuing guidelines, advisories, vulnerability notes, and whitepapers relating to information security practices, procedures, prevention, response, and reporting of cyber incidents.

F. Such other functions relating to cybersecurity as may be prescribed.

On April 28th, 2022, CERT-In was granted power via Direction No. 20(3)/2022-CERT-In (referred to as "Direction" in this document) to issue guidance around information security practices, procedures, prevention, response, and reporting of cyber incidents for a safe and trusted internet. CERT-In had identified certain gaps that were hindering its incident analysis.

CERT-In is empowered under Section 70B (6) of the IT Act, to call for information and give directions to service providers, intermediaries, data centers, body corporate, and any other person for carrying out the previously mentioned activities.

Cert-In defines the problem as follows, "Various instances of cyber incidents and cyber security incidents have been and continue to be reported from time to time and in order to coordinate response activities as well as emergency measures with respect to cyber security incidents, the requisite information is either sometimes not found available or readily not available with service providers/data centers/body corporate and the said primary information is essential to carry out the analysis, investigation and coordination as per the process of law."[1]

Direction No. 20(3)/2022-CERT-In was issued to address those identified gaps, facilitate incident response measures more effectively and strengthen the cybersecurity infrastructure of the country.

The Direction outlines several areas in which organizations that operate within India must adhere. These areas include the following:

1. Use of network time protocol (NTP).
2. Reporting of cyber incidents.
3. Providing information to CERT-In when ordered/ requested.
4. Enablement of log collection.
5. Maintenance of customer information for data centers, cloud providers, virtual private servers, and virtual private network providers.
6. Maintenance of Know Your Customer (KYC) information for financial transactions for virtual asset service providers, virtual asset exchange providers, and custodian wallet providers.

This paper will not explore every area of the Direction but focuses on the ones that pertain to how the Securonix solution can provide value. These areas include items B, C, and D above.

Summary of the Direction

Under the Direction, all service providers, intermediaries, data centers, body corporate, and government organizations (hereafter to be referred to as "Organizations" or "The organization" within this document) based in or operating in India are mandated to report all cyber incidents within 6 hours of becoming aware of or being notified of the existence of a cyber incident. Annexure I of the Direction outlines the types of cybersecurity incidents that include:

A. Data breaches.

B. Data leaks.

C. Targeted scanning or probing of critical networks/ systems.

D. Phishing attacks.

E. Compromise of any critical systems or information.

F. Any unauthorized access to IT systems or data.

G. The defacement of a website or unauthorized change to any websites (for example: by inserting malicious code or links to external websites).

Direction No. 20(3)/2022-CERT-In states that, when required by order/direction of CERT-In, the organization is mandated to take action to provide information or any such assistance to CERT-In which may aid in cybersecurity mitigation actions or enhanced cybersecurity situational awareness.

To have the needed information readily available organizations are mandated to enable logs of all their information and communication technology (ICT systems) and maintain them securely for a rolling period of 180 days. The original Direction required that logs be maintained within Indian jurisdiction, however, a subsequent FAQ published by CERT-In amended this statement and pointed out that log data can be stored anywhere if they can be easily provided to CERT-In when requested.

These logs and log data shall be provided to CERT-In along with reporting of any incident or when ordered/ directed by CERT-In.

What this means for organizations operating in India is that they are required to report incidents within 6 hours to the CERT-In. These organizations are also required to provide information derived from their systems logs to CERT-In when they report an incident or are directed by CERT-In to do so. This log data is not only security log information but may also consist of non-security log data that must be maintained for 180 days.

Key SIEM considerations in relation to the CERT-In Direction

SIEM solutions have been the cornerstone of security operations. However, not all SIEM solutions deliver the same level of functionality, leaving it to the organization to ensure that the SIEM they deploy delivers the right capabilities to meet compliance regulations and mandates.

With the introduction of Direction No. 20(3)/2022-CERT-In it is necessary to understand how SIEM technology aligns to meet the requirements of the Direction. The following section will provide guidance to areas to consider when implementing SIEM technology within your security operations to meet the requirements of the Direction. Each section will also outline how Securonix meets the CERT-In Direction requirements as shown in Figure 1.

	Direction	Securonix Support	Whitepaper Section
1	Use of network time protocol (NTP)		
2	Reporting of cyber incidents	▪	Reporting cyber incidents
3	Providing information to CERT-In when ordered/requested	▪	Providing threat details
4	Enablement of log collection	▪	Enable and collect logs for security and non-security systems
5	Maintenance of customer information		
6	Maintenance of Know Your Customer (KYC)		

Figure 1: Securonix SIEM Alignment to Direction No. 20(3)/2022-Cert-In: Areas in which a full features SIEM applies.

The following sections will highlight key capabilities to consider as it aligns with three major areas of the Direction. These capabilities will focus on log collection, reporting, and log maintenance.

Enable and collect logs for security and non-security systems

Direction No. 20(3)/2022 CERT-In, Direction '(iv) Enablement of log collection', requires organizations to enable logs for all their information and communication technology (ICT) systems.

It is critical to be able to collect and make usable data derived from logs within your environment available in real time. A majority of SIEM solutions collect and analyze a rich variety of log data from security systems within your environment including security event logs, user identity data, access privileges, threat intelligence asset metadata, and NetFlow data. To effectively gain the visibility needed to detect threats your organization must also be able to collect and analyze log data from non-security systems such as end devices, the network, and home-grown applications.

The Securonix solution uses out-of-the-box and custom connectors to ingest log event data from a variety of structured and unstructured data sources. These data sources include enterprise applications, endpoint monitoring, perimeter security, and identity systems.

Going Beyond Security Logs

Observing data only from security logs does not provide a comprehensive understanding of sophisticated threats. To effectively understand threats, organizations need to be able to collect logs from endpoint and network devices, properly format them and store them within a central repository. Securonix, through NXLog, allows organizations to collect logs from operating systems, network devices, and IT/IOT sources like ICS/SCADA and store them within the same centralized data store as security logs. This NXLog approach collects the log data, normalizes, and properly stores it to be made available for analytics and reporting.

With the incorporation of the data cloud within the Securonix SIEM solution, we have established the foundation to provide visibility into security and non-security data: Using a single-tiered data architecture. This simplifies how data is searched and analyzed which yields faster search results and a more comprehensive view of incidents.

Combining security and non-security logs into a single platform minimizes the need for multiple log collection systems, one for security logs and one for non-security logs. This approach also minimizes the number of resources needed and time required to manage the log collection and reporting systems. Having this centralized data allows users to view all the information within the same user interface, streamlining analytics, investigation, and hunting workflows. All this combined equates to a substantially lower total cost of ownership (TCO) and prepares you to provide the information needed to CERT-In when requested.

Logs must be maintained securely for a rolling period of 180 days[1]

The CERT-In Direction requires that logs be maintained securely for a rolling period of 180 days.

Organizations must have relevant data readily available using data storage designed to accelerate search results over longer time increments. Recent Thoughtlab research has shown that threats can dwell in an environment for 128 days on average before being discovered. To understand the events leading up to, during, and after a breach; the organization must be able to view data from several months prior to detection.

The Securonix solution leverages an expansive data cloud for log and data storage. This data cloud provides a highly scalable data storage approach that can meet the needs of any size organization with virtually unlimited capacity. This high-capacity data cloud allows Securonix to meet the 180-day mandate of storing logs.

Location of logs

In the original release of the Direction, it was required that all logs be maintained within India's jurisdiction. A subsequent FAQ published by CERT-In states that, "logs may be stored outside India also as long as the obligation to produce logs to CERT-In is adhered to by the entities in a reasonable time."[2] The Securonix solution is a cloud-based SIEM offering flexibility on where data is stored, while also making the data readily available. This approach allows organizations to meet the requirement. As a cloud-native solution Securonix allows you to collect and store data within a single location from any cloud, including AWS, Google and Azure or SaaS applications, as well as collect data from on-premises systems.

[1] No. 20(3)/2022-CERT-In Government of India Ministry of Electronics and Information Technology (MeitY) Indian Computer Emergency Response Team (CERT-In), Dated: 28 April, 2022

[2] Frequently Asked Questions (FAQs) on Cyber Security Direction of 28.04.2022, India Ministry of Electronics and Information Technology (MeitY) Indian Computer Emergency Response Team (CERT-In), Dated: May 2022

Reporting cyber incidents

The CERT-In Direction, '(2) reporting of cyber incidents', requires that you report incidents within 6 hours of becoming aware of or being notified of the existence of cyber incidents.

The first step to meeting this mandate is to detect that a threat exists. As new cyber incidents and threats become more complex and sophisticated, they have become more effective at avoiding detection. This holds true for low and slow threats that are designed to infiltrate your environment gradually so as not to trigger a rule-based alert.

To effectively detect these sophisticated threats organizations must turn to behavior-based user and entity threat detection as well as find ways to understand the relationship across multiple incidents. Behavior analytics delivers the ability to identify when a user or entity deviates from normal behavior or if a user or entity is acting in a way not consistent with its peers.

Sophisticated threats avoid detection through attacks that occur over several stages. These attacks use small activities over multiple attack vectors or stages to avoid detection by rule-based alerts that are triggered when a threshold is violated or if detected they produce alerts that seem to be non-consequential events.

The Securonix SIEM solution detects threats based on behavioral analytics. These behavior-based alerts and analytics allow you to identify when users or entities deviate from normal activities or act in ways far different than their peers.

To identify evolving threats that happen over time, Securonix combines related alerts together across threat chains. Bringing seemingly unrelated threats together allows you to prioritize and identify low and slow attacks that occur over several steps. These individual alerts may not seem significant on their own, but when tied together into a threat chain connected by a single entity (user, IP address, login ID, etc.) they can reveal a severe security event.

Securonix threat chain models are based on industry standard threat modeling, such as the MITRE ATT&CK framework and others.

The threat models combine policies and threat indicators together to detect related behavior across multiple data sources. This approach brings to light potential threats that might otherwise go unnoticed. For example, in a ransomware attack if a threat model recognizes that two out of five behaviors have happened within the threat model, it can predict the attack in progress as well as help you anticipate future actions and suggest remediation steps. This approach allows your organization to preempt an imminent attack and reduce your mean time to detection (MTTD) for faster reporting to CERT-In.

Additionally, Securonix provides new threat content and information via a content-as-a-service model which allows you to keep the solution up to date by incorporating new content created by Securonix security experts as it becomes available. This up-to-date content allows you to identify new and emerging threats.

Providing threat details

The CERT-In Direction, '(3) Providing information to CERT-In when ordered/requested', requires organizations to take action to provide information or any such assistance to CERT-In, which may aid in cybersecurity mitigation actions or enhance cybersecurity situation awareness. To meet this requirement organizations must be able to easily access logs, metadata, and analytics and produce reports in easily viewable formats. These reports must then be delivered to CERT-In.

Securonix provides out-of-the-box reports and custom reports that provide transparency into the activity on your network to identify security issues and meet compliance requirements. Leveraging data derived from log collection, organizations can quickly gather key information pertaining to the threat. The reporting capabilities of the Securonix solution allow you to package the information you found during the detection and investigation in a format that can easily be shared with CERT-In.

Conclusion

In today's modern world cybersecurity is top of mind for organizations and regulatory and government agencies. As these agencies define requirements around cybersecurity, solution vendors have started to rethink how they deliver the services and solutions that organizations depend on. These vendors must also consider new regulations and directives that organizations must adhere to.

Securonix SIEM delivers cutting edge capabilities around how data is collected, stored, and analyzed to not only deliver the threat detection, investigation, and response capabilities needed to keep pace with today's modern sophisticated threats, but to also align with new regulations and requirements.

securonix

About Securonix

The Securonix Security Operations and Analytics Platform automates security operations while our analytics capabilities reduce noise, fine tunes alerts, and identifies threats both inside and outside your enterprise.

The Securonix platform includes Securonix SaaS SIEM, the #1 cloud-based, next-generation, quadrant-leading SIEM solution. Securonix provides fast time to value through its analytics capability, cloud strategy, and integrated SOAR feature set.

Big data driven, Securonix scales from small startups to S&P 100 global enterprises, providing fast security ROI and predictable cost. It automates security operations, allowing your security analysts to focus on threats, not infrastructure.

Contact Securonix

www.securonix.com
info@securonix.com | (310) 641-1000