SOCRadar®
Your Eyes Beyond

How SOCRadar helps you to comply with SAMA

Saudi Central Bank's Financial Sector Cyber Threat Intelligence Principles

REQUEST FREE ACCESS

Principle 3: Select and validate relevant sources

As 'Your Eyes Beyond' SOCRadar brings the most relevant threat intelligence sources, cybersecurity news and provides searchable intelligence data as classified and sorted. Users can select and subscribe to any relevant sources such as security bulletins, vendor sites, blogs, credible RSS, Twitter, and Telegram channels.

Principle 6: Process and classify information

SOCRadar automatically processes and correlates intelligence for its customers. The collected intelligence is automatically labeled on the SOCRadar platform. Its smart tagging feature allows users to filter the results based on the country, industry, attack type, and content.

Principle 7: Analyze information

SOCRadar analysts examine the raw data and convert it into intelligence. Before the intelligence is presented to the customer, analysts eliminate false positives. Contextualized intelligence given by SOCRadar helps the CTI team analyze the intelligence easier.

Principle 9: Deliver actionable threat intelligence

SOCRadar analysts turn the findings into actionable intelligence that customers can act upon. Using this timely intelligence context, users can take relevant measures to secure their organization proactively such as patch management, determining incident response and exposure management

Principle 12: Identify a cyber threat landscape

SOCRadar supports organizations to identify cyber threat actors and monitor APT groups. Based on the products and technologies auto-discovered in the organization's external-facing digital assets, aggregated intelligence together with the information on vulnerable assets is presented to the organizations with a risk score.

Principle 15: Define the attack chain

SOCRadar supports SOC teams in getting trends about threat actors' TTPs that match with the MITRE ATT&CK framework. Cyber security teams can derive substantial advantages from this enhanced visibility, as it allows for precise identification and timely response to potential cyber threats.

Principle 18: Collect IOC'S

SOCRadar provides daily threat feeds and indicators of the latest malicious incidents. In addition to SOCRadar's honey pots, the platform provides 150+ open source & commercial IOC feeds. SOCRadar's library of rules containing thousands of YARA & Sigma rules is used by security analysts to quickly identify known malware families and variants as well as to detect new and unknown malware.

Principle 19: Monitor and report vulnerabilities

SOCRadar Vulnerability Intelligence module is a real-time tool for monitoring vulnerabilities that automatically collects data from the NVD database, GitHub repositories, vendor pages and social media. SOCRadar Vulnerability Risk Score (SVRS) calculates the real risk associated with the vulnerabilities.

SAMA & SOCRadar Compatibility

SOCRadar helps organizations to comply with SAMA principles while providing contextualized, false-positives threat intelligence. SOCRadar offers a comprehensive analysis of how it supports your compliance efforts in adhering to each SAMA principle.

CYBER THREAT INTELLIGENCE PRINCIPLES		SOCRADAR COMPATIBILITY
Principle 1: Define roles and responsibilities	Member Organizations should define roles and responsibilities within the organization to produce threat intelligence with their own CTI capability. This includes a dedicated CTI team. CTI team should be supported by skilled resources with **purpose-specific advanced tools.**	SOCRadar provides a thorough CTI solution that enables organizations to identify and mitigate threats across the surface, deep, and dark web. SOCRadar can be utilized to receive purpose-specific intelligence from infrastructure visibility to dark web events. As an extension to your security team, SOCRadar's advanced automation capabilities support the organizations' resources.
Principle 2: Define threat intelligence planning and collection requirements	Requires organizations to define their intelligence objectives. Member organizations should consider different areas of analysis relevant to **their business priorities (e.g., technology, threat actors, etc.).**	Security teams can utilize SOCRadar to understand the threat landscape better. SOCRadar provides them with the required context for adversaries' motivations and plans by categorizing under different areas such as industry, threat actors, and technology to help them define their objectives better.
Principle 3: Select and validate relevant sources	Member Organizations should **select sources** that provide information that is relevant to their business and in line with the threat intelligence requirements defined.	As 'Your Eyes Beyond' SOCRadar brings its users the most relevant threat intelligence, cybersecurity news and provides searchable intelligence data as classified and sorted. Users can select and subscribe to any relevant sources such as security bulletins, vendor sites, blogs, credible RSS, Twitter, and Telegram channels.
Principle 4: Collect data through intelligence sources	Member Organizations should **collect data via various intelligence sources** (e.g. OSINT, TECHINT, SOCMINT, HUMINT and deep web and dark web intelligence).	SOCRadar automatically scraps black markets and dark web forums. Intelligence from hacker chatters, deep web forums, social media, communication channels such as Telegram, ICQ, IRC and ransomware groups' websites are gathered in the platform. SOCRadar takes the burden off the security teams by performing the intelligence collection process automatically.
Principle 5: Define specific standard operating procedures (SOPs)	Member Organizations should **define specific standard operating procedures (SOPs) when conducting specific types of intelligence.**	SOCRadar goes beyond traditional intelligence gathering by conducting thorough Standard Operating Procedures on behalf of organizations.

Principle 6: Process and classify information	Member Organizations should **process and classify collected intelligence** - either manually, automatically, or a combination of the two - from the selected sources and store it securely.	SOCRadar automatically processes and correlates intelligence for its customers. The collected intelligence is automatically labeled on the platform. Its smart tagging feature allows users to filter the results based on the country, industry, attack type, and content.
Principle 7: Analyze information	Member Organizations should apply a variety of quantitative and qualitative analytical techniques to **analyze the importance and implications of the processed information,** and, in turn, produce actionable intelligence.	SOCRadar analysts examine the raw data and convert it into intelligence. Before the intelligence is presented to the customer, it is checked by analysts to eliminate false positives. Contextualized intelligence given by SOCRadar helps the CTI team analyze the intelligence easier.
Principle 8: Share intelligence	The Member Organization's threat intelligence team should **share relevant intelligence with other relevant departments** such as the Security Operations Center (SOC), IT, etc.	SOCRadar platform can be customized to share specific threat intelligence automatically with different teams. Curated intelligence can be shared over security incident and event management (SIEM) tools, team management apps, and ticketing systems. The intelligence can be exported from the platform in different report formats to share with third party organizations.
Principle 9: Deliver actionable threat intelligence	Member Organizations should **take relevant mitigation actions or measures to improve defense infrastructure based on threat intelligence produced** and their knowledge of relevant threats.	SOCRadar analysts turn the findings into actionable intelligence that customers can act upon. SOCRadar users can take relevant measures to secure their organization proactively such as patch management and determining incident response and exposure management.
Principle 10: Continuously improve methods of intelligence	This principle requires member organizations to consider the services of a **dedicated threat intelligence provider, who can offer relevant insights** to complement the organization's existing understanding of threats.	Recognized by Gartner as a Threat Intelligence Representative Vendor, SOCRadar is a unique Extended Cyber Threat Intelligence solution combining external attack surface and digital risk protection with cyber threat intelligence. Prioritized, up-to-date, and relevant cyber threat intelligence empowers its customers to take actions starting from the reconnaissance stage of the cyberattack life cycle.
Principle 11: Integrate CTI	This principle requires Member Organizations to **integrate CTI in situational awareness and red teaming assessments** to validate the organisation's security posture.	SOCRadar's intelligence from dark web forums and hacker channels can be used to raise situational awareness. Vulnerability intelligence generated by SOCRadar can be utilized by red teaming activities to establish a solid security posture.

Strategic Cyber Threat Intelligence		
Principle 12: Identify a cyber threat landscape	This principle requires Member Organizations to **identify the cyber threat landscape relevant to their organization and operations,** with information on **identified vulnerable assets**, threats, risks, threat actors, and observed trends.	SOCRadar supports organizations to identify the threat actors and monitor APT groups. Based on the products and technologies auto-discovered in external-facing digital assets, aggregated intelligence together with the information on vulnerable assets is presented to the organizations with a risk score.
Principle 13: Identify strategic cyber-attack scenarios	This principle requires Member Organizations to **identify the strategic cyber attack scenarios** and perform an assessment of the identified scenarios to prioritize the most likely and impactful scenarios.	SOCRadar empowers CISOs by providing them with attack-surface-centric and industry-specific reports, allowing them to gain valuable insights into the risks faced by their organizations. With tactical intelligence of threat actors and technical intelligence from dark web forums, hacker channels, and IoCs, SOCRadar assists CISOs in creating realistic attack scenarios.
Principle 14: Elaborate Requests for Information (RFIs) and Tailored Threat Assessments	This principle requires Member Organizations to **provide, upon request, detailed information (e.g. cyber threats, trends, events, and malware or tools) related to possible cyber attacks that could target them.** The principle holds the CISO of the Member Organization responsible for validating the quality and relevance of this information.	SOCRadar supports CISOs in improving their investigation through IOC enrichments. CISOs can benefit from SOCRadar's curated intelligence on real-time dark web monitoring, past leaks, phishing domains, and SSL grades related to their organizations. Equipped with this information, CISOs always remain vigilant in understanding the risks posed to their organizations.
Operational Cyber Threat Intelligence		
Principle 15: Define the attack chain	This principle requires Member Organizations to define the **various phases of an attack performed by the threat actors based on industrial standards or frameworks such as MITRE.**	SOCRadar supports Security teams in following trends about threat actors' TTPs that match with the MITRE ATT&CK framework. Security teams can benefit from this visibility for accurate threat detection.
Principle 16: Identify TTP	Member Organizations should **analyze the information collected related to relevant threat actors, tools, or malware to identify relevant Techniques, Tactics, and Procedures (TTPs).** Member Organizations should also rely on Indicators of Compromise (IoCs) for the identification of these TTPs.	SOCRadar keeps track of threat actors with their TTPs based on the **MITRE ATT&CK taxonomy** and matches IOCs with threat actors. Security teams stay up-to-date with recent TTPs and IOCs of threat actors.
Principle 17: Identify malware and tools	Member Organizations should **identify malware and tools during an attack.** Member Organizations can obtain information regarding the different types of malware and tools used by the threat actors using different sources, such as Indicators of Compromises (IoCs), dark web, deep web, OSINT, code repositories, information sharing platforms, etc.	SOCRadar continuously monitors the common forums, source code repositories, and information sharing platforms and provides information about botnets, malware, data dumps, exploits, and hacking as-a-service. Malware's IOCs such as their hash signatures or command and control IPs can be searched through the platform to aggregate the intelligence.

Tactical Cyber Threat Intelligence

Principle 18: Collect IOCs	Member Organizations should **identify, collect, and aggregate IoCs** and implement them in their defence infrastructure.	SOCRadar provides daily threat feeds and indicators of the latest malicious incidents. In addition to SOCRadar's honey pots, the platform provides **150+ open source & commercial IOC feeds.** SOCRadar has a rules library containing thousands of YARA & Sigma rules. SOC analysts easily use these to quickly identify known malware families and variants as well as to detect new and unknown malware.
Principle 19: Monitor and report vulnerabilities	Member Organizations should **constantly monitor announcements of new vulnerabilities discovered,** as well as zero-day vulnerabilities exploited by threat actors. Member Organizations should adopt **a risk-based approach that correlates asset value, the severity of vulnerabilities, and threat actor activity via the use of threat intelligence and analytics to calculate a realistic risk rating.** This rating should be used to prioritize remediation activities.	SOCRadar **Vulnerability Intelligence** module is a real-time tool for monitoring vulnerabilities and their remediation. It automatically collects data from the NVD database, GitHub repositories, vendor pages and social media about vulnerabilities. **SOCRadar Vulnerability Risk Score** (SVRS) calculates the real risk associated with the vulnerabilities. SVRS is a combination of many vulnerability Intelligence elements such as Social Media, News, Code Repositories, Dark/Deep Web, attribution with Threat actors, and malware as opposed to quantitative elements in CVSS calculation.

Integrations

SIEM

- Radar
- Logsign
- ArcSight
- securonix
- DEVO
- Azure Sentinel
- LogRhythm
- McAfee Enterprise Security Manager
- splunk>

SOAR

- XSOAR
- sumo logic

EDR

- CrowdStrike
- wazuh.
- SentinelOne
- CORTEX
- Carbon Black.

Team Management APPS

- slack

Vulnerability Management Products

- RISKSENSE

Firewall

- paloalto NETWORKS
- FORTINET
- Cisco Firepower
- CHECK POINT
- SOPHOS

Work - Service Management & Ticketing

- Jira Software
- ARCHER
- TheHive
- 4me
- Opsgenie

Intelligence Sharing Platform

- MISP Threat Sharing
- SECURE X
- securonix
- ANOMALI

DNS Security

- Cisco Secure Email

Email Security

- Cisco Umbrella

DDoS Protection Products

- ARBOR NETWORKS

CISCO Products

- Cisco
- Secure Network Analytics
- Secure Firewall
- Secure Endpoint
- Secure Web Appliance
- Secure Malware Analytics

Who is SOCRadar®?

Your Eyes Beyond

As an Extended Threat Intelligence (XTI) platform and inventor of the concept, SOCRadar's approach effectively integrates Threat Intelligence, Digital Risk Protection, and External Attack Surface Management (EASM). Adapting proactive security with a hacker mindset, we aim to help security teams to detect blindspots before attackers.

The shortage of cybersecurity experts is a growing problem worldwide. All companies around the world companies must use resources efficiently to provide adequate cyber security with their limited resources. Automated security solutions offer precisely the opportunity that corporations are looking for. With its AI-powered automation technology. **With providing protection against threats for more than 8.400+ companies from 157 countries, SOCRadar has become an extension of security teams from every industry.**

SOCRadar provides extended cyber threat intelligence (XTI) that combines: **"Cyber Threat Intelligence, Digital Risk Protection, and External Attack Surface Management Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

8.400
Number of Users

Darknet and Deep Web Monitoring: SOCRadar's fusion of its unique dark web Recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface web, deep web, and darknet to accurately identify the leakage of your customers' personally identifiable information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resiliency by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS 12 MONTHS FOR FREE

Gartner Peer Insights. Customer First

Gartner Peer Insights™

5/5

Contact Us info@socradar.io +1 (571) 249-4598 651 N Broad St, Suite 205, Middletown, DE 19709