aws marketplace

SOCRadar Extended Threat Intelligence

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

SOCRadar Extended Threat Intelligence

SOCRadar Extended Threat Intelligence Recap

SOCRadar Extended Threat Intelligence enables users to identify and mitigate cybersecurity risks through comprehensive threat visibility and real-time monitoring.

Organizations utilize SOCRadar Extended Threat Intelligence for early detection and proactive defense against potential cyber attacks. With its robust features, users gain enhanced security posture and informed strategic decision-making. Detailed analytics and actionable insights contribute to improved threat response and management, making it a valuable tool in the cybersecurity landscape.

What are the key features of SOCRadar Extended Threat Intelligence?

- Comprehensive Threat Detection: Identifies a wide range of cyber threats across different vectors.
- Real-Time Alerts: Provides instant notifications to address threats promptly.
- Detailed Threat Analysis: Offers in-depth examination of threats to understand their impact.
- Seamless Integration: Integrates smoothly with existing security infrastructure.
- Actionable Insights: Delivers practical recommendations for threat mitigation.
- Intuitive Dashboard: Simplifies monitoring and management with a user-friendly interface.
- Threat Hunting Capabilities: Enables continuous search for potential threats.
- Timely Threat Identification: Ensures prompt and accurate identification of security risks.

What are the benefits or ROI that users should look for in reviews?

- Enhanced Security Posture: Strengthens overall defenses against cyber threats.
- Proactive Defense: Allows for early threat detection and timely response.
- Informed Decision-Making: Supports strategic planning with detailed intelligence.
- Improved Threat Response: Enhances ability to react quickly and effectively to incidents.
- Streamlined Operations: Integrates with current systems for efficient threat management.
- Comprehensive Visibility: Provides a broad view of potential threats for better protection.

SOCRadar Extended Threat Intelligence finds application across multiple industries such as finance, healthcare, and retail, where cybersecurity is critical. In finance, it helps secure sensitive financial data. Healthcare organizations use it to protect patient information. In retail, it safeguards against data breaches and fraud, ensuring safe consumer transactions.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "According to me, SOCRadar Extended Threat Intelligence is a very good product with competitive pricing."

yozkul

Cyber Security Engineer at Cevizsoft Teknoloji AŞ

- "The most complete solution of all, which goes across everything and the entire spectrum, is SOCRadar Extended Threat Intelligence."

Pedro Ladeiro

Senior Cyber Security Expert at a computer software company with 201-500 employees

- "Thanks to SOCRadar, we have saved more than $500,000 for our customers by protecting them from cyber attacks."

Verified user

Senior Threat Researcher at a tech vendor with 5,001-10,000 employees

"We proactively blocked the IOCs provided by SOCRadar Extended Threat Intelligence before breaches occurred in other banks and financial industries."

Ganesh Pagidipalli

Senior Security Analyst at Doyen

"SOCRadar Extended Threat Intelligence has positively impacted my organization by reducing the risk score."

Sgolla Golla

Security Threat Analyst 2 at a consultancy with 501-1,000 employees

"SOCRadar Extended Threat Intelligence is a very proactive security providing product in the market, and it helps identify potential threats related to our organization that we currently found."

Pranjul Tiwari

Security Administrator at Yotta Data Center

"SOCRadar Extended Threat Intelligence has positively impacted my organization because it provides tools that alert us if there is credential leakage or vulnerabilities on our public-facing assets, and I can also read news about the dark web."

Verified user

Product Engineer at a tech services company with 11-50 employees

What users had to say about valuable features:

"The best features SOCRadar Extended Threat Intelligence offers are its Threat Intelligence capabilities, which I believe are great, along with many integration supports for third-party tools like EDR, SIEM, and firewall, making it useful to enrich our security tools. SOCRadar Extended Threat Intelligence also has sandboxing tools that are useful for checking if a file attachment is clean or malicious, and if it is malicious, I can see the behavior of the file to take appropriate action, such as blocking the sender. Additionally, the attack surface feature is very good because SOCRadar Extended Threat Intelligence provides risk ratings for our company, allowing us to fix vulnerabilities and address open ports.

"The sandboxing tool has helped my team when we have suspicious files, such as email attachments or files downloaded from the internet that we do not know if the source is trusted. We use the sandboxing tools to test the files to check if they are malicious.."

Verified user

Product Engineer at a tech services company with 11-50 employees

Read full review

"The best features SOCRadar Extended Threat Intelligence offers are the threat intelligence feature, which I find very effective, as it allows me to scan for data breach exposures in the dark web, and the Attack Surface Management feature, which helps us know what a potential attack surface is. I also use the Vulnerability Intelligence feature.

"The dark web intelligence feature has helped me in threat hunting, allowing me to research my domain and digital assets, such as IP addresses and cloud buckets involved in potential leaks or data breaches. The Attack Surface Management feature gives us a comprehensive view of our digital footprint and vulnerability monitoring systems.

"SOCRadar Extended Threat Intelligence has impacted my organization positively by enabling us to monitor and see exactly what our external threat exposures are, a capability we lacked before using SOCRadar Extended Threat Intelligence.."

Ismaila Jawara
Cyber Security Specialist at Gambia Revenue Authority

Read full review

"The best features offered by SOCRadar Extended Threat Intelligence include the centralized platform, having all the reports at hand, all the functionalities related to CTI-type tools, which are indeed useful for investigations and threat hunting, and the tool is very easy to use.

"SOCRadar Extended Threat Intelligence makes my work or my team's work more efficient by reducing the time it takes to do a search based on a specific domain for some client to whom we provide the service, allowing us to search for all the information related to that domain and different types of indicators or valuable information.

"SOCRadar Extended Threat Intelligence positively impacts my organization significantly by providing reports and high-level executive reporting that gives interesting visibility to top management or personnel with decision-making capacity, without requiring major additional effort to obtain this information.."

Verified user

Cibersecurity Pre Sales Enginer at a tech vendor with 11-50 employees

Read full review

"The best features of SOCRadar Extended Threat Intelligence include the intuitive alert processing that significantly aids in understanding severity, credibility, and relevance of offenses generated by their custom rule engine, showcasing how companies invest in this type of security within SIEM solutions. The X-Force engine is crucial for real-time threat scoring of each vulnerability, despite the ever-evolving threat landscape.

Alert processing is integrated with Jira, enabling efficient ticketing and prioritization of security incidents which provide a graphical aspect that allows filtering to funnel priorities, understanding issues at their core such as detecting suspicious network traffic or anomalous behavior

SOCRadar Extended Threat Intelligence has positively impacted my organization by enhancing user experience through right-click options for further analysis. Future improvements may concern simplifying the tool, which is currently already well-structured.."

Federico Presti
Cyber Security Analyst at a university with 1,001-5,000 employees

Read full review

"The best features SOCRadar Extended Threat Intelligence offers include VIP monitoring, which I personally prefer, Digital Risk Protection, Brand Risk Protection, and malware intelligence. Since I am always active in the cyber threat landscape, I proactively monitor geopolitical intelligence that I find very interesting because remaining on the bleeding edge requires understanding the geopolitical landscape. SOCRadar providing geopolitical threat intelligence information is extremely useful, and these modules provide a good level of information.

"SOCRadar Extended Threat Intelligence has positively impacted my organization in many ways. For instance, we successfully thwarted a cyber attack against our customer. Internally, it brings considerable motivation toward learning a cyber threat intelligence platform, which itself is a very substantial concept. We learn more about cyber threats and various concepts that I believe we cannot learn independently or would take considerable time. Rather than using a threat intelligence platform that is not SOCRadar Extended Threat Intelligence, I believe you will be able to learn such concepts without difficulties and invest your time into more useful and helpful products to develop your core skills.

"Thanks to SOCRadar, we have saved more than $500,000 for our customers by protecting them from cyber attacks. SOCRadar has also saved more than 900 hours of our analysts' time, reducing the Mean Time to Detect, Mean Time to Response, and automating serious tasks within our platform. It has serious capabilities, and we appreciate that.."

Verified user

Senior Threat Researcher at a tech vendor with 5,001-10,000 employees

Read full review

"The features of SOCRadar Extended Threat Intelligence that stand out the most for me are Vulnerability Intelligence, Dark Web Monitoring, Threat Actor Intelligence, IOC Intelligence, and Attack Surface Management because they help us proactively identify and mitigate risk before they become security incidents. Vulnerability Intelligence helps us to track newly disclosed CVEs, understand their severity, determine whether they are being actively exploited or not, and prioritize the patching. Dark Web Monitoring allows us to detect leaked employee credentials, stolen data, ransomware leak posts, and company mentions on underground forums, enabling early response. Threat Actor Intelligence provides insights into attacker groups, their tactics, techniques, and procedures, and recent campaigns, which helps us to understand potential threats targeting our clients. IOC Intelligence enables us to enrich malicious IPs, then domains, URLs, and file hashes and correlate them with known campaigns during investigations. Finally, Attack Surface Management helps us to identify internet-facing assets, exposed services, and misconfigurations so organizations can reduce their attack surface before attackers exploit them. These features are valuable because they allow us to move from a reactive approach to a proactive security posture. Instead of waiting for an alert, we can identify emerging threats, assess them, and assess which clients are affected, issue security advisories, and implement mitigation measures before an incident occurs.

"SOCRadar Extended Threat Intelligence has a significant impact on our organization because my organization is providing security as a service to a lot of financial clients, primarily the banking sector. It is really important to us to provide security in both proactive and reactive ways. While working in the SOC particularly, you are entirely based on the reactive approach, where something will trigger, an alert will be there in the SIEM, and then your team will respond. But proactively, the SOC is not that helpful. For the proactive approach, we implemented SOCRadar Extended Threat Intelligence in our organization and started giving dark web monitoring as a service to a lot of our clients. As I mentioned before, many of our clients are based in the banking sector. It is really important to us that we also provide a proactive approach to security and in that way, SOCRadar Extended Threat Intelligence helped us to provide them proactive security. Basically, we monitor if any employee credentials are leaked in the

darknet or dark webs and if any confidential data is leaked over the dark web and also monitor if the company name is discussed in the dark web forums and if any confidential data is leaked. In all of that, SOCRadar Extended Threat Intelligence has played a vital role for us. Hence, we continue using SOCRadar Extended Threat Intelligence as our DWM tool.

“SOCRadar Extended Threat Intelligence has been a stable platform. During my day-to-day work, it has been consistently available for monitoring vulnerabilities, threat actors, ransomware campaigns, and dark web intelligence. I have not experienced any major stability issues that significantly impacted our operations. The platform delivers timely threat intelligence updates and performs reliably for daily analyst activities. Like any cloud-based platform, there may occasionally be scheduled maintenance or brief service interruptions, but I have not seen these have a significant impact on our workflow..”

Verified user

Associate Threat Hunter And Threat Intelligence Analyst at a tech services company with 11-50 employees

Read full review

Other Solutions Considered

"I previously studied and practiced with Splunk, and later had the chance to understand SOCRadar Extended Threat Intelligence better, which prompted my switch.."

Federico Presti
Cyber Security Analyst at a university with 1,001-5,000 employees

Read full review

"We did not evaluate other options before choosing SOCRadar Extended Threat Intelligence; we just appreciated SOCRadar Extended Threat Intelligence's features.."

Tanuja Parab
Dark L2 Web Analyst at a tech services company with 11-50 employees

Read full review

"I cannot remember whether I evaluated other options before choosing SOCRadar Extended Threat Intelligence. It was a very long time, maybe six or seven years ago.."

yozkul
Cyber Security Engineer at Cevizsoft Teknoloji AŞ

Read full review

"As I mentioned earlier, we were not providing dark web monitoring service. This is the first time we are providing the dark web monitoring service to our clients. SOCRadar Extended Threat Intelligence is our first solution for this service.."

Verified user

Associate Threat Hunter And Threat Intelligence Analyst at a tech services company with 11-50 employees

Read full review

"We previously used OpenCTI but understood its limitations, particularly as our organization grew. We could not rely on OpenCTI due to the constant need to scale up infrastructure and manage platform availability and security, which consumed more time than focusing on threat intelligence. Therefore, we switched to SOCRadar, trusting it more than relying solely on public data.."

Verified user

Senior Threat Researcher at a tech vendor with 5,001-10,000 employees

Read full review

"I was not directly involved in the product selection process, so I did not personally evaluate or compare multiple threat platforms before SOCRadar Extended Threat Intelligence was adopted. However, as far as I know, per the information I received from the upper management, we did consider multiple platforms such as Recorded Future, CrowdStrike Falcon Intelligence, Microsoft Defender Threat Intelligence, and Mandiant Threat Intelligence. SOCRadar Extended Threat Intelligence stood out because it offered a combination of threat intelligence, Digital Risk Protection, ASM, and dark web monitoring in one platform, along with an intuitive interface and actionable intelligence that suited our operational requirements.."

Verified user

Associate Threat Hunter And Threat Intelligence Analyst at a tech services company with 11-50 employees

Read full review

ROI

Real user quotes about their ROI:

"I do not have the exact figure for return on investment with the platform, but there is a significant reduction in the effort of conducting threat hunting and threat investigations manually.."

Verified user
Cibersecurity Pre Sales Enginer at a tech vendor with 11-50 employees

Read full review

"The primary driver of SOCRadar's ROI is the prevention of major security incidents—such as data breaches, ransomware, and third-party supply chain compromises.You can automate many processes, reduce the number of people involved, and get more accurate results.."

yozkul
Cyber Security Engineer at Cevizsoft Teknoloji AŞ

Read full review

"I have seen a return on investment because I can prevent data breaches, which would be more costly than the price of SOCRadar Extended Threat Intelligence. It also enhances my security tools when using the IOCs from SOCRadar Extended Threat Intelligence, saving both time and money.."

Verified user
Product Engineer at a tech services company with 11-50 employees

Read full review

"I have seen a return on investment since we previously deployed more than six to seven employees to gather intelligence and maintain vigilance on the dark web, but now we use only one or two analysts per shift. The amount of money saved is invaluable, although I cannot provide specific metrics as I do not have that data. Time saved exceeds 900 hours since we started utilizing SOCRadar.."

Verified user
Senior Threat Researcher at a tech vendor with 5,001-10,000 employees

Read full review

"I have seen a return on investment; for example, with user creations, many people create numerous accounts, but not everyone uses SOCRadar Extended Threat Intelligence. We focused on one or two main accounts and made use of the webhook feature to get alerts on Teams for critical updates. This way, our costs regarding users have diminished, and we can monitor significant events.."

Tanuja Parab
Dark L2 Web Analyst at a tech services company with 11-50 employees

Read full review

"Regarding return on investment, SOCRadar Extended Threat Intelligence has really helped us in a positive way. Earlier, our whole team was doing reactive monitoring work, basically in the SOC. After setting up SOCRadar Extended Threat Intelligence as a dark web service, half of the team is working entirely into the dark web operations. This has improved the client's security posture a lot compared to when they were only taking the SOC service. Through SOCRadar Extended Threat Intelligence, we are enabled and we got a chance to provide proactive security to the clients. In that case, SOCRadar Extended Threat Intelligence has really helped us and really helped organizations to make planned decisions about their security posture.."

Verified user
Associate Threat Hunter And Threat Intelligence Analyst at a tech services company with 11-50 employees

Read full review

Use Case

“Investigating indicators of compromise, searching for threat actor reports and threat activity, and performing threat hunting activities are the main use cases I have for SOCRadar Extended Threat Intelligence in my day-to-day work.

“I primarily use SOCRadar Extended Threat Intelligence for detecting an alert during monitoring or something that has been reported on the network, in searching for malicious indicators of some type, including IP addresses or some URLs.

“Another interesting case with SOCRadar Extended Threat Intelligence is searching for credential compromises on the Dark Web, which is something that was commonly used and continues to be used..”

Verified user

Cibersecurity Pre Sales Enginer at a tech vendor with 11-50 employees

Read full review

"The main use case for SOCRadar Extended Threat Intelligence involves analyzing security tickets, specifically with ticketing requests from the company that bought their services as a SIEM as a service, responding to Jira tickets from clients experiencing several issues regarding their security network monitoring tools such as Palo Alto and endpoint detection and response tools such as XDR.

One specific example of how my colleagues used SOCRadar Extended Threat Intelligence involved deep diving into CVE 2021-44228, named the Log4Shell vulnerability, which is commonly used for backdoor execution on web application Java vulnerabilities. Despite being an old vulnerability, it still runs on the system of a very important vendor in Italy, showcasing how threat actors continue using these methods to exploit systems. ."

Federico Presti
Cyber Security Analyst at a university with 1,001-5,000 employees

Read full review

"My main use case for SOCRadar Extended Threat Intelligence is for cyber threat intelligence activities related to our work, as we use it to search for potential threats to our digital infrastructure.

"A specific example of how I use SOCRadar Extended Threat Intelligence for searching potential threats to my digital infrastructure is a recent incident involving a third-party data breach, where one of our staff's email addresses was involved. Through SOCRadar Extended Threat Intelligence, we were able to investigate and discovered that a staff email had been involved in a data breach. Due to that information, the platform proved to be very effective as we followed our incident response procedures, notified the staff to change her password, and investigated further.

"Another way I have used SOCRadar Extended Threat Intelligence is that the platform automatically scans for potential digital targets based on certain preset values we configured in the system, giving us insight into the external threat exposure of our infrastructure. This helps us understand what we are putting out there and how the world sees that as a threat to our systems and how we can protect it.."

Ismaila Jawara
Cyber Security Specialist at Gambia Revenue Authority

Read full review

"My main use case for SOCRadar Extended Threat Intelligence is Digital Risk Protection, brand risk monitoring, threat intelligence, supply chain attacks, supply chain monitoring, VIP monitoring, identity intelligence, and geopolitical intelligence.

"I can provide a specific example of how I have used SOCRadar Extended Threat Intelligence for one of those use cases. We obtained information regarding a particular threat actor for our customer, and that threat actor was targeting other brands and companies in that particular sector. We notified our customer that this threat actor might pose a risk to them, we recommended they safeguard their defenses, and we started monitoring for that customer. The effort was successful, and we successfully thwarted that cyber threat attack against our customer, saving a significant amount of money that would have been lost as a victim.

"I have additional information about my main use case and how I use SOCRadar Extended Threat Intelligence. SOCRadar provides high fidelity, suspicious, and malicious IOCs that we can straightaway input into our security tools and directly block, which is valuable. Instead of scouring the internet or social media platforms for malicious IOCs for weeks or months, which consumes considerable time, I have used SOCRadar Threat Hunting platform. In conducting proactive threat hunts, I use the information about threat actors and their TTPs provided by SOCRadar to perform proactive threat hunts on my customers' environments. We use the information provided by SOCRadar to develop detection mechanisms, which is extremely useful and has proven to be a great success story for our organization.."

Verified user

Senior Threat Researcher at a tech vendor with 5,001-10,000 employees

Read full review

“My main use case for SOCRadar Extended Threat Intelligence is to monitor the attack surface and then to monitor credential leakage and Digital Risk Protection like impersonation domain and impersonation web, and data breach. I also use SOCRadar Extended Threat Intelligence to integrate IOCs to SIEM, to firewall, and to EDR.

“One specific example of how I use SOCRadar Extended Threat Intelligence for credential leakage or digital protection is when I receive an alert about password leakage, and from there I can see whose password is leaked and sold on the dark web, and then I can tell the user and ask them to change the password.

“I can add that another example is about SOCRadar Extended Threat Intelligence having Attack Surface Management where I can monitor vulnerabilities on our public-facing assets, and SOCRadar Extended Threat Intelligence will scan our assets regularly and report to us if there are vulnerabilities. I can check the vulnerabilities and then fix and patch them as recommended by SOCRadar Extended Threat Intelligence.

“Regarding SOCRadar Extended Threat Intelligence's AI capabilities, I believe it has good governance and security since SOCRadar Extended Threat Intelligence has an NDA in place, meaning I trust them to handle our sensitive data.

“I have utilized SOCRadar Extended Threat Intelligence's unique dark web sources, which include IOCs such as malicious IPs and domains, and I can integrate these sources into our security tools like SIEM and firewall to identify potential threats early and block them.

“I have utilized the managed takedown services provided by SOCRadar Extended Threat Intelligence when there are impersonation cases involving domains, websites, or social media accounts, allowing us to take down malicious accounts or sites..”

Verified user

Product Engineer at a tech services company with 11-50 employees

Read full review

“In my current role, I am using SOCRadar Extended Threat Intelligence as a threat intelligence platform to monitor emerging cyber threats and assess their impact on our clients. Every day, I review newly disclosed CVEs, ransomware campaigns, threat actor activities, phishing campaigns, exploited vulnerabilities, and malware trends. I identify whether any of these threats are relevant to our clients by checking the affected technologies, software versions, or exposed assets. If a critical vulnerability or active exploitation is observed, I prepare an advisory containing the CVSS score, affected products, exploitation status, business impact, and recommended mitigation steps. I also enrich indicators such as malicious IPs, domain URLs, and file hashes before sharing them with the SOC team for detection and monitoring. SOCRadar Extended Threat Intelligence is also useful for tracking ransomware groups, threat actor profiles, attack trends, and industry-specific threats, allowing us to proactively inform clients before they become victims.

“My primary usage of SOCRadar Extended Threat Intelligence includes threat intelligence to monitor the latest cyber threats, malware campaigns, ransomware attacks, and threat actors, then tracking attacker TTPs using the MITRE ATT&CK framework, then identifying IOCs such as malicious IPs, domain URLs, and file hashes. For example, SOCRadar Extended Threat Intelligence really helps us when a new ransomware group starts targeting the financial sector. Through SOCRadar Extended Threat Intelligence, we can provide intelligence about the group's behavior, IOCs, and then mitigate the issue effectively. The other use case is related to vulnerabilities. We are using SOCRadar Extended Threat Intelligence to track newly disclosed CVEs, then check whether these vulnerabilities are being actively exploited or not in the environment and whether they are affecting the sector of our clients or not. This is very helpful in that case. The third case associated with SOCRadar Extended Threat Intelligence is attack surface management. It helps us to discover internet-facing assets such as websites, servers, IP addresses, and subdomains, then to identify exposed services, misconfigurations, or forgotten assets that attackers could exploit. For example, we have worked on multiple such cases where SOCRadar Extended Threat Intelligence helped us to identify an exposed RDP service on a public IP that should not be accessible from the internet. This helped us to provide effective security posture and improve the security posture of the client successfully. The last use

case is Digital Risk Protection. We are using SOCRadar Extended Threat Intelligence to monitor for brand protection or brand impersonation, then detecting phishing websites using the company name or logo, identifying fake mobile applications or fraudulent domains that are targeting our clients or organization.

“One example where SOCRadar Extended Threat Intelligence was really very helpful was during the Fortinet SSL VPN vulnerability, which is also known as FortiBleed or FortiOS critical vulnerability. When the advisory was published, SOCRadar Extended Threat Intelligence generated intelligence about the vulnerability, including the affected FortiOS versions, the CVSS score, exploitation status, technical details, and mitigation recommendations. My first step was to review the advisory and understand the impact. I then identified which of our clients were using Fortinet firewalls and checked whether their FortiOS versions were vulnerable or not. Since the vulnerability was being actively exploited, we classified it as high priority. Then I prepared a client advisory that included a summary of the vulnerability, affected FortiOS versions, whether public exploits were available or not, the business impact, and the vendor mitigation and patching recommendations. Along with that, we informed the SOC team to closely monitor FortiGate VPN logs for indicators of compromise, such as unusual SSL VPN logins, then unexpected administrator account creation. Through this, we helped the clients, and we also ensured the clients were advised to patch immediately and review the logs for any signs of compromise..”

Verified user

Associate Threat Hunter And Threat Intelligence Analyst at a tech services company with 11-50 employees

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

"My experience with pricing, setup cost, and licensing is very good; I can quickly check how many tokens are required for domain utilization and make budget adjustments. It is wonderful and allows for easy minor changes.."

Tanuja Parab Read full review

Dark L2 Web Analyst at a tech services company with 11-50 employees

"The initial setup takes time; you need to create a good inventory and prioritize items according to their importance. If your preparation is correct and sufficient, the setup will be quick.."

yozkul Read full review

Cyber Security Engineer at Cevizsoft Teknoloji AŞ

"Since implementing SOCRadar Extended Threat Intelligence, one of the key outcomes we have noticed is faster threat identification and improved response time, as the platform provides early visibility into potential risks such as credential risks and exposed assets. We have seen an improvement in threat detection speed and investigation efficiency, which helps us identify potential risks much faster compared to when we were not using this tool.."

Pranjul Tiwari

Security Administrator at Yotta Data Center

Read full review

"SOCRadar Extended Threat Intelligence was easy to deploy because it is a SaaS-based tool that does not require much integration with our other tools. It does not require any personally identifiable information from our company, so the deployment was straightforward. We have completed a few integrations, and these were also simple. The tool does not have direct integration, but it offers open-source integrations such as STIX format and TAXII, which were helpful.."

Mohammed Tajammul Ubaidullah

Principal Cybersecurity Engineer at a tech vendor with 1,001-5,000 employees

Read full review

"The initial setup is fairly easy. SOCRadar Extended Threat Intelligence does the whole work for us, and if we need to add an integration to our CM tools or anything else, it is super easy. They have a quite complete API tool. They have integrations for Palo Alto and other tools, or even for Sentinel, Rapid7, and others. They are really good at this. They have multiple integrations, and the implementation is fairly easy.."

Pedro Ladeiro

Senior Cyber Security Expert at a computer software company with 201-500 employees

Read full review

Customer Service and Support

"The customer support for SOCRadar Extended Threat Intelligence is pretty good. You will get a response within one business day. For example, if there is a takedown request, you will definitely get a faster response.."

Verified user
Soc Analyst 11 at a tech services company with 11-50 employees

Read full review

"The customer support is good, as SOCRadar Extended Threat Intelligence provides 24/7 global support that responds quickly and effectively when I encounter problems.

"I would rate the customer support a 9 due to its quality.."

Verified user
Product Engineer at a tech services company with 11-50 employees

Read full review

"Customer support is absolutely brilliant.

"I give customer support a rating of ten because of the quality of investigation, feedback, and the amount of threat intelligence support and takedown requests handled professionally.."

Verified user
Senior Threat Researcher at a tech vendor with 5,001-10,000 employees

Read full review

"Customer support for SOCRadar Extended Threat Intelligence is very good. There are some levels: level one, level two, or level three. When you open a ticket, they generally answer immediately.

One time I had a problem and I opened a support ticket for SOCRadar Extended Threat Intelligence. The customer support responded to me in one hour because there was a problem with the SOCRadar GUI. They resolved it in a very quick time.."

yozkul
Cyber Security Engineer at Cevizsoft Teknoloji AŞ

Read full review

"Regarding customer support for SOCRadar Extended Threat Intelligence, it is really active. We have attended multiple meetings with the SOCRadar Extended Threat Intelligence original team, and they were really supportive when we were facing some issues with the integrations of SOCRadar Extended Threat Intelligence feeds in our SIEM tool. At that time, we had a meeting with the support staff. The technical team really helped us in that situation, and we were successfully able to integrate SOCRadar Extended Threat Intelligence with our SIEM tool. I think it is a very good aspect of SOCRadar Extended Threat Intelligence that their customer support is really active over time when we needed them. I rate them highly.."

Verified user

Associate Threat Hunter And Threat Intelligence Analyst at a tech services company with 11-50 employees

Read full review

"I haven't utilized much customer support, but whenever I had doubts about the UI—such as needing to mention my organization with typosquatting or requesting more analysis based on triggered rules—I made a ticket, and I received analysis within a day.

The pre-sales team and my manager coordinated directly with customer support, with a designated SPOC for us.

I rate the technical support from SOCRadar Extended Threat Intelligence as nine.

Customer support is crucial. SOCRadar provides IOC-related insights that correlate with recent campaigns and geopolitical tensions, enabling us to understand whether the information suits the financial services or retail sectors.."

Ganesh Pagidipalli

Senior Security Analyst at Doyen

Read full review

Other Advice

"I would rate SOCRadar Extended Threat Intelligence an 8.5 out of 10. I advise others looking into using SOCRadar Extended Threat Intelligence to try the product, as it is very effective and a great product that I believe would be very helpful.."

Ismaila Jawara
Cyber Security Specialist at Gambia Revenue Authority

Read full review

"I would advise other people who are considering using SOCRadar Extended Threat Intelligence to focus on the versatility of the tool, on its entire scope and all the coverage it has in the different types of intelligence it handles, from the executive point of view to the operational one, and to adapt it to their internal processes based on that. I would rate this product a 9 out of 10.."

Verified user
Cibersecurity Pre Sales Enginer at a tech vendor with 11-50 employees

Read full review

"My advice for others considering SOCRadar Extended Threat Intelligence is to buy the correct amount of licenses since SOCRadar Extended Threat Intelligence is strict regarding licensing. If you purchase credits that cover fewer assets than you have, you will not cover all your assets, which could jeopardize your company's security.

"The freemium tier offered by SOCRadar Extended Threat Intelligence is beneficial

for exploring its features as you can try it for free before considering purchasing credits for your company.

“I believe SOCRadar Extended Threat Intelligence is already good and does not require additional improvements that we have not mentioned. My overall review rating for SOCRadar Extended Threat Intelligence is 8.5 out of 10..”

Verified user
Product Engineer at a tech services company with 11-50 employees

Read full review

"My advice for others would be positive about SOCRadar Extended Threat Intelligence because as a fresher, I used SOCRadar Extended Threat Intelligence as my first tool in the threat intelligence and dark web monitoring part. It is really easy to use and easy to understand. The features are very good for everyone to understand how dark web monitoring works, how analysts see, and what they are doing regarding the alerts that are generated by SOCRadar Extended Threat Intelligence. It is really easy to understand. The dashboard is very easy to navigate. The options are very familiar, and it really helps anyone to understand what is actually going on the platform. Compared to the other solutions, I would prefer SOCRadar Extended Threat Intelligence as a fresher.

"Overall, my final thought about SOCRadar Extended Threat Intelligence is that I had a positive experience with it. It has helped us to move from a reactive to a more proactive security approach by providing timely intelligence of vulnerabilities, threat actors, and other activities of the attackers. I particularly value having threat intelligence and dark web monitoring integrated into a single platform, which streamlines investigations and improves analyst efficiency. While there is always room for improvement, particularly around deeper automation or SIEM or SOAR integrations, I believe SOCRadar Extended Threat Intelligence is a mature and reliable platform that delivers actionable intelligence and helps organizations strengthen their overall security posture. I would rate SOCRadar Extended Threat Intelligence a nine out of ten.."

Verified user
Associate Threat Hunter And Threat Intelligence Analyst at a tech services company with 11-50 employees

Read full review

"In my experience, I supported my colleagues in the Ethical Hacking course while using SOCRadar Extended Threat Intelligence, and I had this brief yet fully comprehensive experience in approximately two months.

Considering how supply chain attacks are solved and their devastating impact, I

believe that cybersecurity in the coming years will focus on these critical vulnerabilities, highlighted by CVE 2024-3094, which features a backdoor in the XZ library. The SolarWinds attack provides an effective example, as it exploited the Orion vulnerability, showing that supply chain security is crucial for a company to understand SLA and inquire about software and updating procedures, as it plays a role in the security of the entire infrastructure.

SOCRadar Extended Threat Intelligence's governance and security through its AI capabilities are impressive, as they aid greatly in CVE understanding and allow for network comprehension of threats, proving to be a formidable tool for open-source intelligence.

The outputs generated by SOCRadar Extended Threat Intelligence are robust and intuitive in terms of AI capabilities.

It is significant for my organization that SOCRadar Extended Threat Intelligence validates its IOC data with input from over 35,000 global users, as this ensures a constantly evolving database that keeps pace with growing threats, contributing to SOCRadar Extended Threat Intelligence's excellent reputation.

The remediation process is carried out manually, where analysts thoroughly examine files that might potentially compromise the client's system, as it is primarily the analyst's responsibility to understand each issue better.

I recommend this solution for organizations aiming to strenghten threat intelligence and improve incident response efficiency.

I have no additional thoughts about SOCRadar Extended Threat Intelligence, except to suggest it as an effective tool for any company looking to enhance their work. I assigned a rating of eight to this product based on my overall experience. ."

Federico Presti
Cyber Security Analyst at a university with 1,001-5,000 employees

Read full review

“SOCRadar Extended Threat Intelligence earns a rating of ten on a scale of one to ten.

“I rate it a ten because of the quality of information that is always delivered when needed, and the support from SOCRadar's internal security team is absolutely brilliant. The high-fidelity information that I rely on as a cyber threat intelligence analyst is what I seek. Ultimately, you want correct information that you can work on and a platform that supports you with overall visibility and extended capabilities. When everything falls into place, that is what makes a platform deserve a score of ten.

“Regarding SOCRadar Extended Threat Intelligence's AI capabilities, I believe its accuracy and reliability of output are quite accurate and reliable because most of our customers are satisfied with the services that we provide as a managed security service provider. They have never complained regarding the reporting or metrics we provide or the cyber threats that we address to keep them safe. SOCRadar's AI is absolutely brilliant in terms of creating reports, which is flexible because ultimately you need some form of automation feature that helps you write lengthy reports instead of investing human hours. I would rely on SOCRadar Extended Threat Intelligence's AI capabilities to handle that task and provide automation instead.

“Regarding the freemium tiers and flexible pricing offered by SOCRadar, I believe the freemium pricing is invaluable for new companies or startups. At the starting point, when your infrastructure is small and limited, you do not have many users or an external surface to manage. The freemium tier helps you start by providing the hints and information you need to stay updated in the platform. SOCRadar can prove to be an invaluable product for new companies. However, flexible pricing and premium tiers are necessary for organizations that mature and need to reach a certain level where they should pursue enterprise pricing or professional pricing because their external surface expands and they cannot afford to miss costly cyber threats. Regarding its impact on my IT budget planning, SOCRadar does not pose any problems since some cyber threat intelligence platforms are overwhelmingly costly, and you may not always have a budget for your ideal threat intelligence platform.

“I have utilized SOCRadar's unique dark web sources, and they significantly impact identifying potential threats early. Our analysts work on dark web sources, and there was a client whose name was leaked in one of the dark web forums. We proactively validated that particular data, which turned out to be a false positive created as a scareware technique by threat actors to extort money or frighten clients. Without SOCRadar, I do not believe we would have discovered the truth and might have faced a real cyber attack, costing us considerably more. SOCRadar has been instrumental in dark web related information and investigations.

“We are not currently using SOCRadar's AI-driven solution with the 44 orchestrated tools. However, we are using AI to automate report scheduling.

“I have utilized the managed takedown services provided by SOCRadar, and it is absolutely amazing. Ultimately, we do not have to deal with the takedown and manage all the associated hassle; SOCRadar handles everything, allowing us to remain stress-free, which is what matters.

“SOCRadar validating its IOC data with input from 35,000 or more global users is very significant for my organization. There are many IOCs from over 35,000 global users providing their input with context. It is essential to have high fidelity IOCs, avoiding falsely flagged IOCs that could put our customers in danger. For my organization and customers, SOCRadar has done a fantastic job in providing high fidelity IOCs because all IOCs I have encountered from SOCRadar are highly suspicious and malicious.

“I have utilized the Attack Surface Threat Assessment (ASTA) feature, and I have used it more times than I can count. I discovered more than 1,000 publicly exposed and vulnerable assets that our IT team did not maintain, which were shadow IT devices. Thanks to SOCRadar, we were able to integrate it with our internal security tools and conduct vulnerability assessments, safeguarding those publicly exposed assets.

“My advice to organizations looking into using SOCRadar Extended Threat Intelligence is that if you are starting your search for a threat intelligence platform, you can confidently trust and choose SOCRadar. It is an emerging leader in the field of cyber threat intelligence with massive capabilities for growth in the future, providing high fidelity IOCs that you always seek to block on your

perimeter devices. It is very cost-effective compared to other threat intelligence platforms, which is a significant advantage since not every organization has a budget for a dedicated threat intelligence platform. Furthermore, its ever-growing capabilities that include threat intelligence, geopolitical events, vulnerability intelligence, identity intelligence, brand risk protection, Digital Risk Protection, malware intelligence, and proactive threat hunting are fantastic. Overall, it is a great product. I give SOCRadar Extended Threat Intelligence an overall review rating of ten.."

Verified user
Senior Threat Researcher at a tech vendor with 5,001-10,000 employees

Read full review

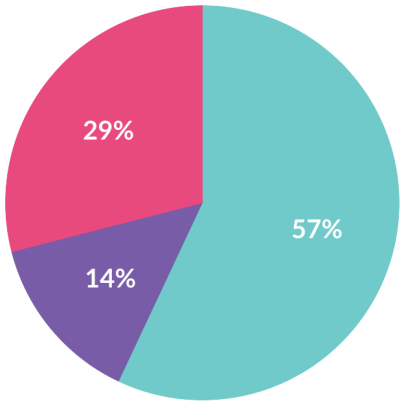
Top Industries

by visitors reading reviews

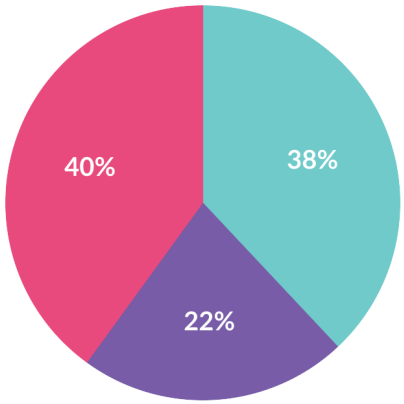
Financial Services Firm	14%
Outsourcing Company	12%
Comms Service Provider	10%
Manufacturing Company	8%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944