MSP
Barracuda
Your journey, secured.

A comprehensive guide to Security Operations Center (SOC) maturity levels

SOLUTION BRIEF

MSP Barracuda
Your journey, secured.

Importance of a SOC in today's cybersecurity landscape

Organizations across the globe are faced with a constant barrage of cybersecurity threats. A robust defense against these threats is more important than ever, and this is where SOCs play a critical role. In the realm of cybersecurity, SOCs are the front line of defense, where dedicated teams work tirelessly to protect and secure an organization's digital assets. However, it's important to stress that not all SOCs are created equally. The SOC maturity model outlines five distinct levels, each representing an increasing degree of sophistication and effectiveness in addressing cybersecurity threats. For customers seeking SOC services, understanding the differences between various SOC maturity levels can be the key to ensuring digital assets are well-protected.

This article is designed to help provide a breakdown of the five SOC maturity levels, and what an ideal, mature SOC should look like.

SOC maturity levels

	LEVEL 1 Basic	LEVEL 2 Intermediate	LEVEL 3 Advanced	LEVEL 4 Optimized	LEVEL 5 Innovative
People	Blue Team Analysts, business hours coverage	Blue Team, 24x7 Coverage	24x7 SOC team with specialized roles (Blue, Green)	24x7 SOC team with advanced roles (Purple, Red)	24x7 Global SOC Blue, Green, Purple, Red, White Teams with regional presence (AMER, EMEA, APAC)
Skills	Network Security, Operating Systems knowledge, Email analysis	IDS and IPS knowledge. SOC tools such as SIEM	Cloud Computing, Endpoint security, audit and threat analysis, adversary attack tactics and techniques	Deep experience with live attacks ranging from various ATPs. Advanced SOC tools such as SOAR	Comprehensive skill set, covering all aspects of defensive and offensive security tools along with development and AI/ML expertise. R&D into new security advancements & optimizations
Certifications	Security+, Network+	CIEH, CySA+	AWS Cloud Practitioner, Azure Fundamentals	GIAC, AWS Solutions Architect, AWS Developer	CISSP, AWS, Azure, CISA, CSAP, ISO 27001, AWS Security, GCIH, CIEH, GIAC, and CySA+, Security+, Network+
Process	Simple incident escalation and out of the box rules	Runbooks/playbooks, threat hunting, basic emerging threats coverage	Security risk classification, manual allow and blocklist capabilities, custom SIEM rules	Advanced threat hunting, attack and defend exercises, log correlation across multiple data sources	Advanced runbook mapping, attack and defend exercises, incident response guidance and threat hunting. Automated allow and blocklist capabilities. Faster zero-day coverage
Technology	Basic SIEM	Advanced SIEM, Open-source threat intelligence	EDR resources, malware sandbox	SOAR, 300+ signature-based detections mapped to MITRE ATT&CK, cloud lab	State of the art SIEM, SOAR, TIP with 10B+ IOCs, 800+ ML-based detections, MITRE ATTACK framework mapping, attack labs, automated threat defense

MSP Barracuda
Your journey, secured.

What determines SOC maturity?

MATURITY LEVEL	RESPONSIBILITIES
Basic	A basic SOC operates during business hours of any given region. It is staffed by level 1 and 2 cybersecurity analysts who have foundational skills in network security and operating systems. They may hold certifications such as Security+ and Network+, but their processes and technology are relatively simple. The SOC may use a basic security information and event management (SIEM) system and simple incident escalation procedures, with out-of-the-box rules to detect and respond to threats.
Intermediate	An intermediate SOC has 24/7 coverage equipped with level 1 cybersecurity analysts with knowledge of Intrusion Detection Systems (IDS) and, Intrusion Prevention Systems (IPS). The SOC is powered by tools like SIEM. With certifications such as Certified Ethical Hacker (CEH) and Cybersecurity Analyst (CySA+), they are also beginning to develop threat hunting capabilities and the ability to respond to emerging threats. Technology-wise, they use mid-level SIEM and open-source threat intelligence.
Advanced	An advanced SOC operates 24/7 and introduces specialized Team(s) to provide coverage for various attack surfaces. The teams have skills in cloud computing, endpoint security, audit, and threat analysis, and are familiar with various adversary attack tactics and techniques. Key certifications at this level include AWS Cloud Practitioner and Azure Fundamentals. The advanced SOC uses intermediate endpoint tools and malware sandboxing, and they manually maintain allow and block lists for better control over network traffic.
Optimized	At the optimized level, the SOC operates 24/7 and has a team structure that not only covers the various attack surfaces but incorporates level 2 team(s) with members who hold advanced certifications such as GIAC, AWS Solutions Architect, and AWS Developer. Their skills now include deep experience with live attacks from various Advanced Persistent Threats (APTs) and advanced SOC tools such as Security Orchestration, Automation, and Response (SOAR). Additionally, they possess knowledge of Bash and scripting, which allows for a more efficient and automated response to incidents. Their processes have evolved to include advanced threat hunting, attack and defense exercises, and the ability to correlate logs across multiple data sources. This level of maturity empowers the SOC to detect and respond to complex threats swiftly and effectively. In terms of technology, an optimized SOC leverages SOAR, signature-based detections mapped that may map to industry framework to ensure gaps can easily be found. The combination of advanced skills, processes, and technology makes the optimized SOC well-equipped to handle sophisticated cyber threats.
Innovative	The innovative level of SOC operates 24/7 and the teams boast a comprehensive skill set, covering all aspects of defensive and offensive security tools, along with development and AI/ML expertise. They also add programming skills, such as Python, a widely used programming language used in cybersecurity for tasks such as automating incident response, data analysis, Machine learning/AI and threat modeling. Their certifications range from Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA) to GIAC and CySA+. An innovative SOC should include advanced processes, including automated runbook mapping, advanced attack and defense exercises, and rapid zero-day threat coverage. The technology at this level is state-of-the-art and may integrate with a multitude of systems such as SIEM, SOAR, Threat Intelligence Platform (TIP), and machine learning-based detections.

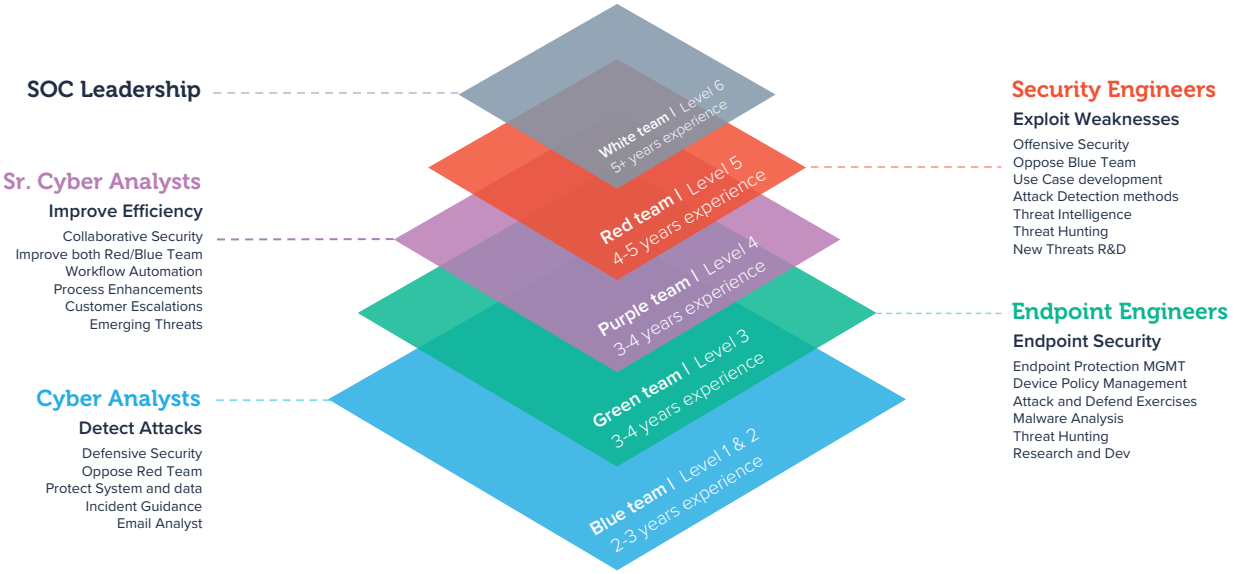
MSP Barracuda
Your journey, secured.

The innovative Barracuda global SOC

Barracuda's SOC offers 24/7 operation, utilizing a "follow-the-sun" model with specialized teams including Blue, Green, Purple, Red, and White, distributed across American, Europe, Middle East, and Africa, and Asia Pacific. Leveraging Barracuda XDR, an open XDR, that integrates with best-in-class SIEM, SOAR, TIP with over 11 billion Indicators of Compromise (IOCs), and 800+ machine learning-based detections, Barracuda SOC can efficiently and effectively detect and respond to incidents.

The Barracuda SOC is structured with a clear hierarchy of roles and responsibilities, ensuring that every aspect of security operations is managed by experienced professionals with specialized skills. This unique structure fosters collaboration and enhances efficiency, enabling Barracuda SOC to provide top-tier cybersecurity service.

At the heart of the Barracuda SOC structure are specialized teams, each with a distinct focus. These teams include Blue, Green, Purple, Red, and White Teams, all working in tandem to ensure a holistic, robust, and responsive cybersecurity posture.



CERTIFICATIONS

MSP Barracuda
Your journey, secured.

Barracuda's SOC teams

Blue Team - comprised of cyber security analysts where their primary responsibility is to detect attacks and protect systems and data. The team provides incident guidance and conducts email analysis, playing a vital role in defensive security.

Green Team - made up of Endpoint Engineers, focuses on endpoint security. They manage endpoint protection and device policy, conduct malware analysis, and engage in attack and defense exercises.

Purple Team - serves as a bridge between the Blue and Red Teams, working to improve efficiency and collaboration. They handle workflow automation, process enhancements, customer escalations, and address emerging threats.

Red Team - mission is to exploit weaknesses, opposing the Blue Team. Their responsibilities include developing use cases, devising attack detection methods, and conducting threat intelligence and hunting.

White Team - which represents the SOC Leadership, oversees daily global SOC operations, updates SOC policies, improves SOC capabilities, and evaluates SOC team performance. They also ensure continuous training programs, fostering an environment of constant growth and development.

The combined experience of these teams in the cybersecurity field exceeds 20 years, reflecting a deep well of expertise and a long-standing commitment to excellence in security. This wealth of experience, combined with their cutting-edge technology and mature processes, positions Barracuda global SOC as a leader in the SOCaaS space.

Barracuda global SOC's organizational structure, combined with the vast expertise of its teams, is a testament to their unwavering commitment to excellence and their leadership in the cybersecurity industry.

TEAM / LEVEL	GOAL	ROLE	EXPERIENCE	RESPONSIBILITIES
Blue team: Level 1-2	Detect Attacks	Cyber Security Analysts	2-3 Years	These defensive security specialists oppose the Red Team and protect systems and data. Their duties include providing incident guidance and conducting email analysis.
Green team: Level 3	Endpoint Security	Endpoint Engineers	3-4 Years	The Green Team is responsible for endpoint protection management and device policy management. They engage in attack and defense exercises, malware analysis, threat hunting, and research and development.
Purple team: Level 4	Improve Efficiency	Sr. Cyber Security Analyst	3-4 Years	The Purple Team works to improve the efficiency of both the Red and Blue Teams. Their tasks include workflow automation, process enhancements, incident response guidance, handling customer escalations, and addressing emerging threats.
Red team: Level 5	Exploit Weaknesses	Sr. Cyber Security Analyst	4-5 Years	The Red Team's goal is to exploit weaknesses, opposing the Blue Team. They develop use cases, devise attack detection methods, conduct threat intelligence and hunting, incident response guidance and research and develop new threats.
White team: Level 6	Boost SOC efficiency and Quality	SOC Leadership	5+ Years	The White Team, composed of SOC leadership, manages daily global SOC operations, updates SOC policies, improves SOC capabilities, ensures the proper functioning of SOC tools, evaluates SOC team performance, and ensures continuous training programs.

Blue Team Level 1-2

Goal: Detect Attacks
Role: Cyber Security Analysts
Experience: 2-3 Years
Responsibilities: These defensive security specialists oppose the Red Team and protect systems and data. Their duties include providing incident guidance and conducting email analysis.

Green Team Level 3

Goal: Endpoint Security
Role: Endpoint Engineers
Experience: 3-4 Years
Responsibilities: The Green Team is responsible for endpoint protection management and device policy management. They engage in attack and defense exercises, malware analysis, threat hunting, and research and development.

Purple Team Level 4

Goal: Improve Efficiency
Role: Sr Cyber Security Analyst
Experience: 3-4 Years
Responsibilities: The Purple Team works to improve the efficiency of both the Red and Blue Teams. Their tasks include workflow automation, process enhancements, incident response guidance, handling customer escalations, and addressing emerging threats.

Red Team Level 5

Goal: Exploit Weaknesses
Role: Sr Cyber Security Analyst
Experience: 4-5 Years
Responsibilities: The Red Team's goal is to exploit weaknesses, opposing the Blue Team. They develop use cases, devise attack detection methods, conduct threat intelligence and hunting, incident response guidance and research and develop new threats.

White Team Level 6

Goal: Boost SOC efficiency and Quality
Role: SOC Leadership
Experience: 5+ Years
Responsibilities: The White Team, composed of SOC leadership, manages daily global SOC operations, updates SOC policies, improves SOC capabilities, ensures the proper functioning of SOC tools, evaluates SOC team performance, and ensures continuous training programs.

Conclusion

The SOC maturity model provides a clear illustration that not all SOCs are created equal. The pinnacle of excellence, the innovative level 5 SOC, embodies an unprecedented combination of comprehensive skill sets, diverse team structures, advanced processes, and state-of-the-art technology. This is where Barracuda SOC sets the benchmark for cybersecurity service provision.

Barracuda SOC's innovative SOC is not just about the impressive list of certifications its teams hold, or even the advanced technology they employ. What truly sets them apart is their dynamic, agile approach to cybersecurity. They're continually researching and developing new security advancements and optimizations, ensuring they stay ahead of the ever-evolving threat landscape.

For instance, their automated runbook mapping and incident response guidance streamline the process of dealing with threats, enabling faster response times and more efficient mitigation. Meanwhile, their automated allow and block list capabilities and faster zero-day coverage ensure they're ready to tackle new threats as soon as they emerge.

The innovative SOC's technology stack is equally impressive. Their SIEM, SOAR, and TIP systems handle an enormous volume of threat indicators, and they employ machine learning to detect threats more accurately and efficiently. Moreover, they have integrated the MITRE ATT&CK framework, ensuring they can effectively combat the diverse range of tactics and techniques used by adversaries.

In a world where cybersecurity threats are growing in both number and sophistication, the value of a high-maturity SOC cannot be overstated. As such, Barracuda global SOC's commitment to achieving and maintaining level 5 maturity is a testament to their dedication to providing the highest possible level of cybersecurity service.

As we look to the future of cybersecurity, we can expect the demand for high-maturity SOCs to grow. Organizations are increasingly recognizing the importance of strong cybersecurity defenses, and high-maturity SOCs like Barracuda global SOC are ideally positioned to meet this demand. By combining their sophisticated Open XDR Platform with their innovative SOC services, Barracuda global SOC is leading the way in cybersecurity service provision.