sentor

Part of **Accenture**

Data sheet

# RedSOC

## Continuous scenario-based attacks

# RedSOC

**Most organisations find it challenging to identify and address vulnerabilities as their IT environment continues to grow and evolve. These risks can be identified and mitigated through a combination of qualified scanning activities performed by experienced RedTeam testers that recon and act as a real-life attacker.**

Cyber threats continue to evolve and cloud- and on-premises environments grow through the adoption of new and variable technologies. Continuous development and delivery results in frequent deployment of new applications, code and infrastructure, making a yearly penetration and application test obsolete in just a couple of weeks. This makes it challenging to keep up with attackers that continuously search for new attack surfaces.

Part of the responsibility placed on the IT department is to address vulnerabilities as they occur, but in any given organization of size the workload of handling vulnerabilities could easily consume all the available resources - preventing the IT department from fulfilling its primary purpose, supporting the business. Prioritization of what needs to be addressed and when is a must to keep the balance between security and business value.

## The solution – continuous security testing

The only way of answering the fundamental question - “are we vulnerable to attack?” - is to attack, and analyze the outfall. It is this question that led Sentor to develop the RedSOC service concept - in which we attack you like the real adversaries do.

By gathering threat intelligence, we can analyze the techniques used by real adversaries, allowing us to perform the same attacks, truly answering the question of whether or not this adversary could breach you.

By discussing your business, with you, and understanding your risks and critical assets we can tailor these attacks to focus not on finding *every* issue in *every* system, but on finding the issues that matter to you. The vulnerability that impacts your business is the one that matters.

We combine your risks and your threats to develop attack scenarios which describe the most likely way your business is impacted by cyber attacks. These scenarios are then carried out by our team of 30+ white-hat hackers, ensuring that specialists are available in every step, and the results reported back to you - allowing you to focus on fixing the issues that matter.

## How it works

RedSOC is a managed service, where Sentor’s RedTeam testers act as a real-life attacker, using knowledge discovered using automated scans together with the knowledge of experienced penetration testers to find the easiest way to compromise infrastructure, applications and data. The service runs continuously, and findings are reported to the client as they are discovered and validated.

We will provide you with an in depth understanding of security posture, weakest links and architectural problems that can be exploited. This includes lateral movement, alternative access paths to critical data, possibilities to compromise central assets like Active Directory or critical applications. The scope of the service is based on business risks with defined targets in mind and allows us to build attack scenarios from targeted threat intel.

## Deliverables details

**Threat Intelligence powered by Accenture**
We monitor threats against the protected organization and uses this information both to prioritize and develop scenarios, as well as to highlight new threats in customer reports.

**Vulnerability scanning**
As part of the service, we utilize the tools and techniques used by attackers to maximize effectiveness. This includes vulnerability scanning of target systems to identify easily detected issues which may be used to execute scenarios.

**Scenario based testing**
We maintain a selection of relevant attack scenarios targeting your organization. The scenarios are developed based on threat intelligence detailing how adversaries attack similar organisations, as well as risk information supplied by the customer.

These scenarios are repeatedly executed, progress is recorded, and findings reported. The primary output are tickets, in which important and high-impact issues are detailed, along with recommendations on how to mitigate vulnerabilities.

**Red Team Lead (RTL)**
Each customer has direct access to a Red Team Lead who manages their offensive testing activities. The RTL is also responsible for reporting identified security issues to the customer, as well as handling customer specific demands, questions, and general advice.

**Security Tickets**
Identified issues which are deemed to pose a real threat to the security of the customer are reported as tickets. Tickets contain detailed descriptions of vulnerabilities, including recommendations on how they can be effectively mitigated.

The Red Team Lead is available to discuss mitigation strategies, potential impacts and any other questions that arise around the vulnerability.

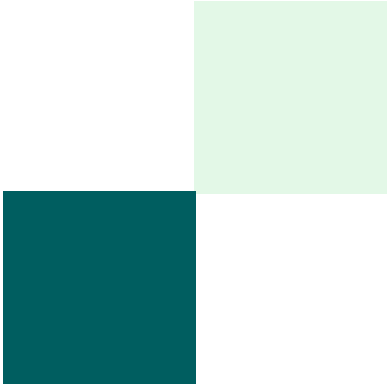
**Monthly reports**
The monthly reports contain information about relevant threats including types of attacks executed, and techniques used, against similar organizations.

The monthly report also contains a summary of the testing that has been performed, as well as any general conclusions based on findings.

**Quarterly meetings and reports**
The quarterly meetings are held in a workshop format where the Red Team Lead and optionally other specialist resources review the testing performed during the reporting period, as well as discuss findings and suggest changes that would be beneficial to the overall security level of your' organization. The customer risk portfolio is reviewed and updated and the key take-aways from the testing period are summarized in a quarterly report.

**Internal testing infrastructure**
While maintaining a realistic approach to security testing provides enormous benefits, there are certain situations where simulation of certain aspects can lead to better results overall. One such key area is the topic of internal network access.

In order to ensure that we can perform as effectively as possible, it is recommended that a Sentor remote access solution is deployed internally. This provides our hackers with internal network access and gives us the ability to deploy as many nodes as is required to get a comprehensive view of the internal networks of multiple sites or geographic locations.



## How to get started

In order to deliver the best service possible, we need to understand your business, motivation, organization and technical environments. This is achieved by an implementation process preceding the start of delivery, outlined below.

- Assignment of Service Delivery Manager and Red Team Lead
- Start of infrastructure deployment
- Threat research
- Risk workshop
- Rules of engagement workshop
- Initial scenario selection
- Start of service delivery

### About our RedSOC services

Sentor's unique RedSOC service is designed to meet the world as it really exists. With an understanding of your business, we combine your threats and risks to develop attack scenarios that describe the most likely ways in which your organisation is vulnerable to cyberattacks.

In a world where perfection doesn't exist, we anticipate what flaws an attacker is likely to find, and we help you create a tailored solution to the problem.

## Key benefits

**Scenario-based attacks**
Continuous scenario-based attacks, carried out using the same methods as real attackers, and constantly adapting to the evolution of both the organisation and the cyber threat.

**Continuous reporting**
Generates a continuous flow of priority-sorted action proposals to continuously raise the lowest level for attackers and mitigate threats.

**Testing your resilience**
Tests how prepared your organisation is to detect and respond to a targeted attack on everything from technology and processes to people.

**Holistic perspective**
Gives you an overview that covers parts of the environment that are never examined through individual system-specific tests.

**Delivered by experts**
Developed and delivered by Sentor's Red team of security experts with extensive experience in security testing of all types of systems, networks and applications.

**Continuous reporting**
Generates a continuous flow of priority-sorted action proposals to continuously raise the lowest level for attackers and mitigate threats.

**Prioritising future investments**
Gives you a better understanding of your organisation's security gaps to ensure that future investments deliver the greatest benefit.

sentor

Part of **Accenture**