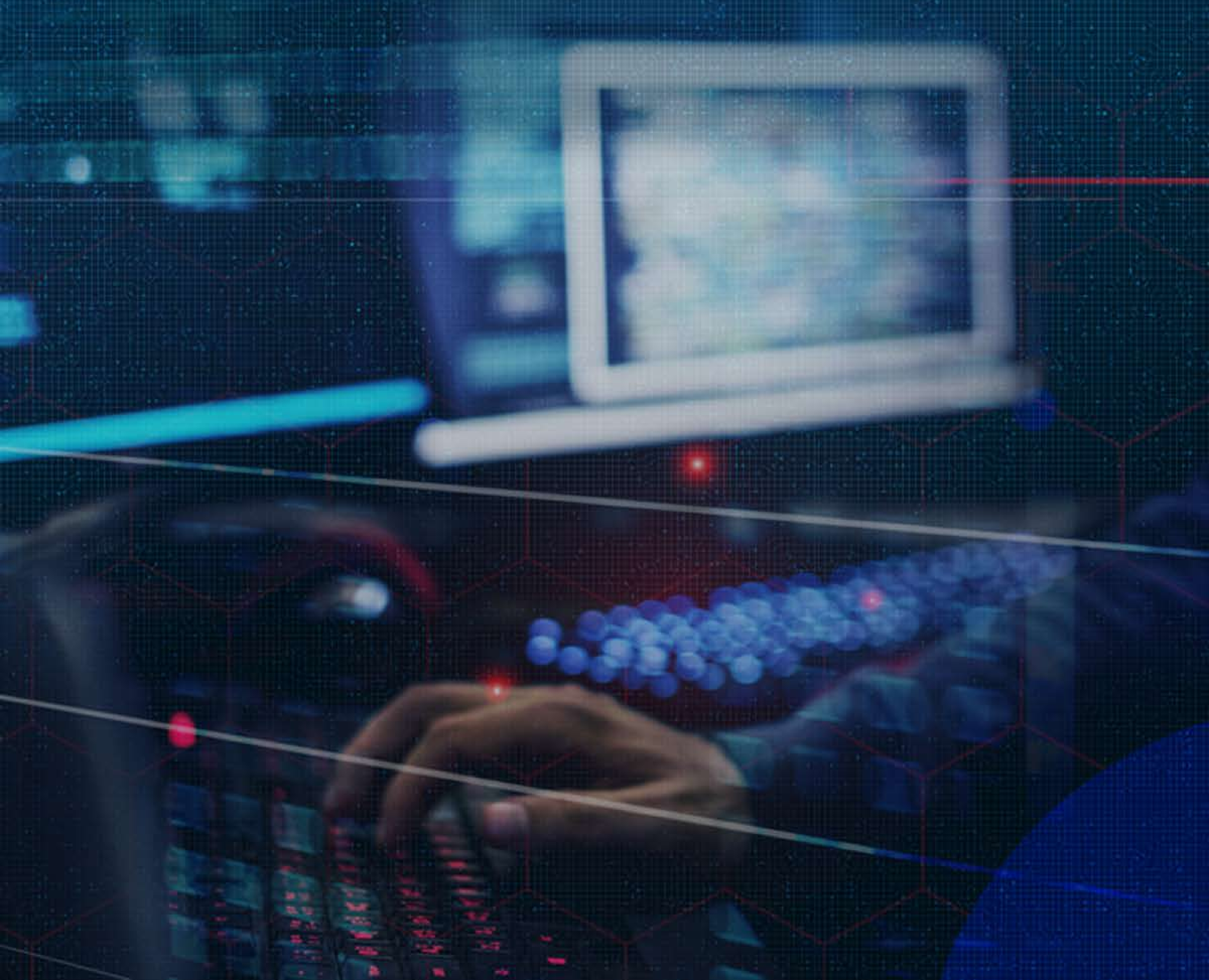
TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Remote SOC

A Challenge for **Security Professionals**



As the COVID-19 outbreak has strained the global workforce to stay home, most of the organizations have established work from home policies to maintain business continuity and productivity. This immediate shift has raised challenges for the security operations team to stay connected and overcome the possible risks in this critical time. Since personal devices and networks are more prone to cyber-attacks, the global pandemic is giving C-Level executives as well as SOC managers sleepless nights.

CERT-In, in its latest advisory, notified that there has been a substantial rise in the number of cyberattacks on personal computers, routers and networks as most of the security professionals are working from home.

When it comes to the security operations center (SOC), it is important to discover how to achieve effective remote SOC operations. The only key to the success of this transformation (from on-site to remote) is “security”. Whether the teams are working on-premises or remotely, the basics of maintaining an effective SOC will remain the same.

Secured Devices

An on-site SOC is contained in an environment with advanced cyber as well as physical security measures because of the nature of the information resides in it. Since it is not possible to deliver the same set of security procedures to the team’s residence, remote SOC becomes a bit challenging. Therefore, each analyst’s device (including the home router) must be configured carefully and given secured access (preferably via VPN) to SOC resources.

Most security researchers believe that multifactor authentication must be implemented while requesting access to such critical resources. They also suggest that blacklisted IPs should be removed and monitoring tools must be retrained for new user behaviors.

Proper Communication

Communication and Collaboration are one of the most crucial parts of successful SOC operations. They become even more important when everyone operates remotely. The information must be shared regularly through collaboration tools used for group chats, conference calls, or videoconferencing. It is also vital to ensure that the information is shared over a secured platform, preferably, an internal platform as business-critical information cannot be shared over a public messaging platform. This will help in preventing the exploitation of intellectual property in case it gets compromised.

It is also important to ensure that your entire network is secured with a VPN as it encrypts the traffic and makes it difficult for the intruder to read.

A good communication plan could be:

- Ensure that appropriate notifications are set up and reaching to the relevant teams
- Ensure that the contact information of each team member is updated (including both work and personal phone numbers and email addresses)
- Provide a contact matrix for information on who to contact on different issues that could arise

Update IR (Incident Response) Plan

As it is uncertain, how long WFH will continue, it becomes important to focus on response planning, adversarial threat modeling, and vulnerability/patch/remediation management. The senior executives and managers need to reassess the cybersecurity incident response strategies, particularly while triaging events and collecting artifacts.

How TASL Driving SOC Services Amidst Global Pandemic

We know that security is not the only thing that needs to be focussed while talking remote security operations center. Confidentiality, Integrity and Availability also need to be addressed at the same time. In the midst of this COVID-19 situation, we believe that every security analyst needs to be available and perform respective duties to keep SOC operational.

Our “Martial” – Next Gen SOC provides next-level assurance of protection and security in a world where cyber-attacks can now affect almost every aspect of our lives both personally and professionally. It embraces security controls like multi-factor authentication, strong encryption over data transmission, and real-time collaboration solutions that enables SOC professionals working remotely to support businesses to continue function and maintain productivity in this critical time.

We are dedicated to seamlessly improve your organization's security posture and make you future-ready against all advanced and complex threats, regardless of the circumstances.

Trust in us with confidence!!

PROTECTING LIKE A **GUARDIAN**

TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

For a custom build SOC solution

Connect with us at

contactcs@tataadvancedsystems.com