National Cyber Security Operations Center (N-CSOC)

Stakeholders' Conference

Benefits to the Stakeholders

'A Collaborative and Win-Win Strategy'

Lal Dias
Chief Executive Officer
Sri Lanka CERT|CC

Cyber attacks are no longer a matter of “if” …..
but a matter of “when.”

We also have to understand that;

- Attacks can never be fully prevented
- Organizations should advance their detection capabilities so they can respond appropriately

What is a Cyber Security Operations Center (CSOC)?

SRI LANKA CERT|CC

Sri Lanka Computer Emergency Readiness Team | Coordination Centre

A valuable resource for security incident detection ….

- It is a facility that houses an information security team that is responsible for monitoring and analysing an organization's security posture on an ongoing basis
- The SOC team's goal is to detect, analyse, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes
- SOCs are typically staffed with security analysts and engineers as well as managers who oversee security operations
- SOC staff works closely with incident response teams of participating organisations to ensure security issues are addressed quickly upon discovery
- SOCs monitor and analyse activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for suspicious activity that could be indicative of a security incident or compromise
- In summary … a SOC is responsible for ensuring that potential security incidents are correctly identified, analysed, defended, investigated, and reported

How does a CSOC Work?

- A SOC does not engage in developing security strategy, design security architecture, or implement protective measures
- Instead a SOC focusses on ongoing, operational component of enterprise information security
- Additional capabilities of some SOCs can include advanced forensic analysis, and malware reverse engineering to analyse incidents
- Typical SOC infrastructure includes firewalls, IPS/IDS, breach detection solutions, probes, and a security information and event management (SIEM) system
- Technology should be in place to collect data via data flows, telemetry, packet capture, syslog, and other methods so that data activity can be correlated and analysed by SOC staff
- The SOC also monitors networks and endpoints for vulnerabilities in order to protect sensitive data and comply with industry or government regulations

Benefits of Having a Cyber Security Operations Center

- The key benefit of having a SOC is the improvement of security incident detection through continuous monitoring and analysis of data activity
- By analysing this activity across an organization's networks, endpoints, servers, and databases around the clock, a SOC team is well placed to ensure timely detection and response of security incidents
- The 24/7 monitoring provided by a SOC gives organizations an advantage to defend against incidents and intrusions, regardless of source, time of day, or attack type
- The gap between attackers' time to compromise and an organisations' time to detection is very small
- A SOC helps organizations close this gap and stay on top of the threats facing their environments

Benefits of Having a Cyber Security Operations Center

- A SOC continuously manages known and existing threats while working to identify emerging risks
- SOC keeps up with the latest available threat intelligence and leverages this information to improve internal detection and defence mechanisms
- SOC uses logs from participating organizations and correlates it with information from a number of external sources that deliver insight into threats and vulnerabilities
- External cyber intelligence includes news feeds, signature updates, incident reports, and vulnerability alerts from various sources
- This helps the SOC to keep up with evolving cyber threats
- SOC constantly feed this threat intelligence into SOC monitoring tools to keep up to date with threats, and the SOC has processes in place to discriminate between real threats and non-threats

Q & A ?