How to set up your SOC for success

Considering setting up or reconfiguring your security operations center (SOC) for optimal efficiency?

A well-designed SOC is critical for safeguarding your organization against emerging physical and cybersecurity threats. Here, we break down key considerations into seven crucial categories: configuration, collaboration, context, clarity, coordination, compliance, and cybersecurity.

Configuration: Extend reach and flexibility

- **Optimize the hub layout**: Arrange the SOC strategically, creating collaborative workspaces and optimizing monitor visibility.
- **Avoid having windows**: The room should have no windows and limited access to ensure security and minimize distractions.
- **Consider your IT infrastructure**: What type of IT infrastructure do you have? On-premises, cloud-based, or hybrid? How does it impact your SOC's efficiency?

Collaboration: Enhance teamwork inside and outside your SOC

- **Install video walls**: Implement video walls to display real-time feeds and enhance overall visibility.
- **Invest in communications tools**: Use SIP-based communication management tools such as Sipelia™ to easily transmit information and communicate with others.
- **Set up a dedicated email address**: Improve communications by establishing a specific email address to handle all requests.
- **Dispatch and assign tasks**: Consider implementing collaborative decision management systems like Mission Control™ for efficient task assignment.

Context: Get a unified view

- **Leverage advanced mapping features**: Utilize mapping tools in your SOC to easily visualize and understand events across facilities.
- **Connect IIoT devices**: Enhance contextual awareness by connecting IIoT devices and aggregating data into a single unified platform.
- **Add browser windows to dashboards**: Integrate news feeds and social media updates for external event awareness.

Clarity: Digitize information to get actionable insights

- **Create rules**: Establish user-friendly rules that eliminate false alarms and reduce operator overhead.
- **Automate tasks**: Create automated workflows operators can follow during critical times to ensure notifications are handled according to security procedures for compliance.
- **Filter through data**: Implement automation tools to filter through data, allowing operators to quickly address potential threats.

Coordination: Escalate and respond to events efficiently

- **Set up dynamic operating procedures**: Introduce dynamic operating procedures with Mission Control for tailored responses to different incident phases.
- **Consider workstation-based escalation rights**: Assign workstation-based escalation rights for quicker and more efficient reactions during emergencies.

Compliance: Comply with regulations

- **Assign user privileges**: Fine-tune user privileges to ensure regulatory compliance.
- **Set up reporting**: Facilitate forensic investigations by putting in place comprehensive incident reports.

Cybersecurity: Stay ahead of cyber threats

- **Automate maintenance updates**: Set up automated tasks to receive notifications with device maintenance updates and system health statuses to remain cybersecure.
- **Maintain an audit trail**: Choose software that facilitates exporting in native format and file sharing while maintaining a robust audit trail.

Optimize your security operations center with the help of a collaborative decision management system

Learn more about Mission Control

Genetec Inc.
genetec.com
info@genetec.com
@genetec

UPDATED: FEB-08-24