CHECKLIST

Top Six Technologies for a Converged Security Operations Center

IT and OT networks are being integrated as digital transformation initiatives sweep across industrial sectors. This shift presents an opportunity to converge security operations across IT and OT in one security operations center (SOC). Synergistic operations across IT and OT are advisable so long as that SOC includes a staffing strategy that accounts for the distinct operational requirements found in OT environments.

The Fortinet 2022 State of Operational Technology Cybersecurity report found that survey respondents who had the best outcomes with the fewest intrusions were 32% more likely to track OT security in their enterprise SOC.[1]

Six Essential Capabilities for Technologies for Converged IT/OT Secure Operations

A converged SOC should leverage these six technologies:

☑ SIEM

Make sure your converged SOC is using security information and event management (SIEM) that is relevant in both IT and OT. For example, choose a SIEM offering that includes the MITRE ATT&CK for ICS tactics, techniques, and procedures dashboard as well as the classic MITRE ATT&CK display relevant in OT.

☑ SOAR

Your security orchestration, automation, and response (SOAR) offering should have runbooks that are relevant to IT as well as OT environments.

☑ Deception or honeypot

If using deception technology, make sure the product can mimic systems found in both IT and OT environments. For example, your deception vendor should support lures and decoys that imitate OT-specific systems and devices such as human-machine interfaces (HMI), supervisory control and data acquisition (SCADA), and programmable logic controllers (PLCs). Of course, it should also be able to imitate classic IT infrastructures such as Microsoft Active Directory servers and Microsoft Exchange servers.

☑ Centralized policy management

A converged SOC should be able to manage firewall policies and switch configurations deployed in IT and OT environments. The management software should be able to be federated to fit well with the on-premises nature of OT environments.

☑ Centralized logging and reporting

The logging and reporting tools in a converged SOC should also be relevant in IT and OT environments. Compliance reports should match well with the needs of OT compliance reporting.

☑ Endpoint detection and response (EDR)

Any EDR offering in a converged SOC must be able to manage infrastructure found both in classic IT as well as OT environments. For example, the EDR product's agent must maintain a commitment to supporting legacy operating systems such as Microsoft Windows XP. It also must be able to run in baseline mode to minimize disruptions while exercising the entire production process. Finally, threat intelligence should be able to reach the endpoint agents in the ICS environments through a hybrid architecture in which the asset owner or OEM can ingest threat intelligence from the security vendor's cloud infrastructure through their data center.

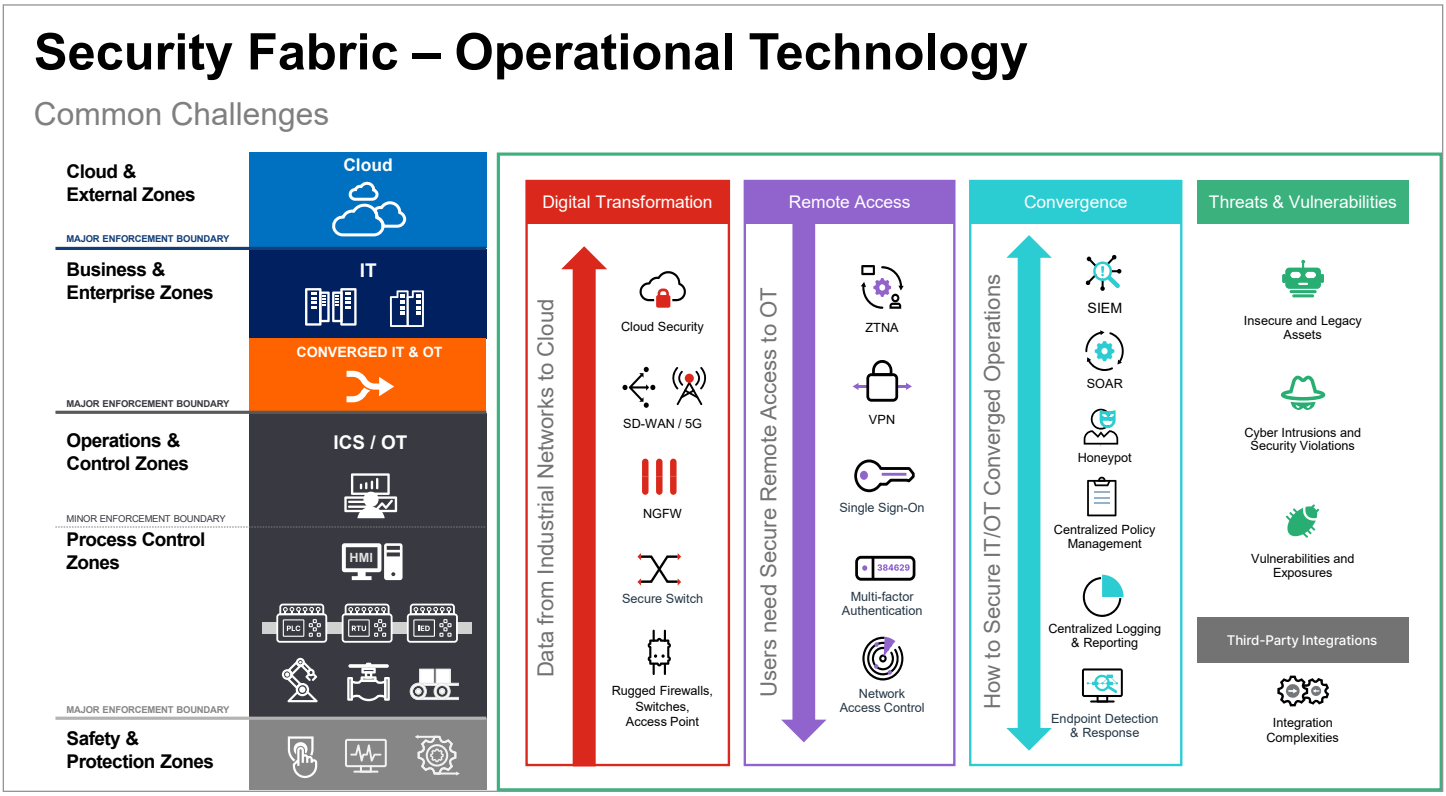

Figure 1: Each of the six technologies in the Convergence column can be applied in a converged SOC.

Conclusion

Any product deployed in a converged SOC must have capabilities relevant and specific to both IT and OT environments. Make sure you look for vendors with the items suggested above to guarantee a good fit and a successful outcome. As a reminder, it's very important to staff your SOC with trained experts who understand the production processes and specialized devices and systems running in the OT environment.

[1] "2022 State of Operational Technology and Cybersecurity Report," Fortinet, June 2022.

FORTINET

www.fortinet.com

November 29, 2022 9:33 AM
1862948-0-0-EN