Cybersecurity and Technology Operations Paradigm-Reference Architecture

Architect's on both sides have to consider how to operationalize their architectures and how that impact's both cybersecurity and technology operations (SOC, NOC, Fusion Centers).

- Cybersecurity Solution Architect
- Network Cybersecurity Architect
- Information Cybersecurity Architect
- Application Cybersecurity Architect
- Enterprise Cybersecurity Architect
- Enterprise Architect
- Business Architect
- Network Architect
- Software Architect
- Database Architect
- Information Architect
- System Architect
- Cloud Architect
- Solution Architect

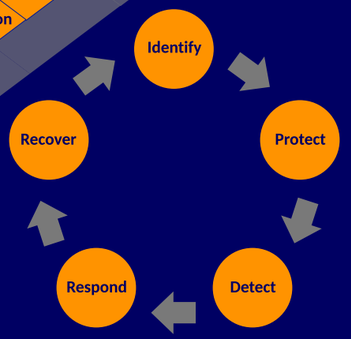
Cybersecurity Mechanisms/Service Catalog (not an exhaustive list)

HIDS/HIPS	CASB	Firewall Risk Mionitoring
EDR	AI	Forward Proxy/Web Content Filitering
NDR	WAF	Malware Behavior Analysis
XDR	MDM	XML Gateway/API Gateway
PIM/PAM	FIM	User Behavior Analysis
SIEM	DBF	Deception Technologies
DAM/DAS	Directory Services	Certificate Management
DLP	Whole Disk Encryption	TLS Decryption
FSM/FAM	GRC Platform	NIDS/NIPS
Unsupervised ML	HSM/TPM	DDoS Mitigation
Supervised ML	IDEA/IAM	Federated Services/SSO

Incident Response, Disaster Recovery, and Business Continuity is a Team Effort.

It's not just cybersecurity personnel. It's all ops functions that help keep the lights on 24x7.

If there isn't enough personnel. How will alerts and incidents be actioned?
Do you know how many FTEs operations need?
1k alerts per Analyst?
Is an MssP/MSP the right direction?



ICT Mechanisms/Service Catalog (not an exhaustive list)

SaaS	Mail Servers	Middleware Servers
PaaS	Web Servers	Application Servers
IaaS	File Servers	Source Code Repositories
SDN/IBN	RDMS Servers	Web Services Proxies
Cloud Storage	NoSQL Servers	Application Load Balancer
NAS/DAS/SAN	Data Lake	Data Warehouse
Firewalls	Big Data Analytics	ESB/Middleware
Routers	Web Services	Microservices
Switches	Certificate Authority	Certificate Management
Load Balancer	HSM/TPM	Directory Services
WAN Scaler	IoT	Service Desk
VPN Gateways	ICS/SCADA	KMS
WAPs	Sensor Networks	CMS

Operationalizing cybersecurity mechanisms and the cybersecurity services catalog implies:

- The need for Runbooks
- The need for Standard Operating Procedures
- The need for Playbooks
- The need to wrap it all in relevant Business Processes
- Will these cybersecurity mechanisms be operationally sustainable over time?

These concepts are not mutually exclusive between IT and cybersecurity. People need to know what they are doing, why they need to do it, and when it needs to be completed by.

The devil is in the details. Not providing for operationalization requirements will create chaos and confusion for operational personnel.

Operationalizing ICT mechanisms and the ICT services catalog implies:

- The need for Runbooks
- The need for Standard Operating Procedures
- The need for Playbooks
- The need to wrap it all in relevant Business Processes
- Will these ICT mechanisms be operationally sustainable over time?