

## Selecting some features and grouping them :

### Data Collection And Integration

Penetration  
Testing &  
Vulnerability  
Assessments

Security  
Information  
and Event  
Management  
(SIEM) Logs

Intrusion  
Detection  
System  
(IDS) Alerts

Firewall &  
Endpoint  
Security  
Logs

### Cyber Threats & Evolution

Definition  
of Cyber  
Threats

Types  
of Cyber  
Threats

Impact on  
Organizations  
& Individuals

### Threat Detection Techniques

Real-Time  
Threat  
Detection

Challenges  
and  
Limitations  
of IDS

Signature-  
Based vs.  
Anomaly-  
Based  
Detection

Intrusion  
Detection  
Systems  
(IDS) & How  
IDS Works

### Future Trends & Challenges in Cybersecurity

Predictions  
for Future  
Cyber  
Threats

Impact of  
Emerging  
Technologies  
on Security

### Post-Incident Activities & Cybersecurity Hardening

Patch  
Management  
&  
Configuration  
Management

Timeliness  
& Accuracy  
of  
Reporting

### Incident Response Planning & Execution

Key  
Components  
of an IRP

Roles &  
Responsibilities  
in Incident  
Response