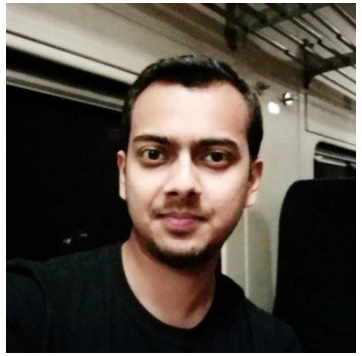
breaking into cybersecurity
as a soc analyst

Global information security society for professionals of Pakistan

who



Syed Ishaq Zafar B.

Security Squad Lead

twitter: twitter.com/k3yb0ardm0nk3y
github: github.com/keyboardmonkey
linkedin: linkedin.com/in/ishaqbukhari

- 7th year into cybersecurity, working in various roles
- helped establish a renowned MSSP business in PK
- been playing a part in bridging the academia-industry gap

Mohammed Waleed Khaliq

Manager SOC @ NourNet

linkedin: linkedin.com/in/m-waleed-khaliq-a774aa17

- 10+ years working in cybersecurity majorly in govt. sector
- mentor and trainer to several security professionals
- SANS lethal forensicator

goals

- promoting Security Operation Center (SOC) Analyst as a career in cybersecurity
    - 🎯 geared towards fresh graduates and young security professionals
- introducing **GISPP** community to academia and cybersec aspirants
- promoting better monitoring habits/techniques for the new/struggling SOC teams & anti-patterns
- suggesting advanced detection/hunting techniques for the established SOC teams
- focusing on providing our review of the popular (and less popular but effective) SOC tools

goals (what is out of scope)

- promoting Security Operation Center (SOC) Analyst as a career in cybersecurity
    - 🎯 geared towards fresh graduates and young security professionals
- introducing GISPP community to academia and cybersec aspirants
- ~~promoting better monitoring habits/techniques for the new/struggling SOC teams & anti-patterns~~
- ~~suggesting advanced detection/hunting techniques for the established SOC teams~~
- ~~providing our review of the popular (and less popular but effective) SOC tools~~

flow

- why get into infosec
- careers in infosec
- security ops center & SIEM
- secops jobs
- career progression
- job market & avg salaries
- further reading

flow

- why get into infosec
- **careers in infosec**
- security ops center & SIEM
- secops jobs
- career progression
- job market & avg salaries
- further reading

  - offensive
  - defensive
  - forensics
  - risk/compliance
  - training & misc.

flow

- why get into infosec
- careers in infosec
- security ops center & SIEM
- **secops jobs**
- career progression
- job market & avg salaries
- further reading

  - soc analyst
  - soc engineer
  - soc manager
  - SIEM specialist
  - MDR analyst
  - threat hunter
  - network sec engr.
  - solutions architect
  - DevSecOps

why should I consider a career in cybersecurity?

www.securitymagazine.com › articles › 92312-of-cyber...

76% of Cybersecurity Leaders Face Skills Shortage | 2020-05 ...

May 6, 2020 — The latest findings of the Stott and May Cyber **Security** in Focus research reveal that leaders are still struggling with the **skills gap** and access to ...

securityboulevard.com › Security Bloggers Network

The Cybersecurity Skills Gap Continues, with SOCs Lacking ...

Jun 18, 2020 — Home » **Security** Bloggers Network » The Cybersecurity **Skills Gap** Continues

insights.dice.com › 2020/08/20 › why-the-cybersecurit...

Why the Cybersecurity Skills Gap Continues to Widen

Aug 20, 2020 — **Security** is more top-of-mind than ever for companies. And

www.csoonline.com › Security

The cybersecurity skills shortage is getting worse | CSO Online

Aug 21, 2020 — For the past four years, ESG and the Information Systems **Security** Association

travel for consultancy

good salary + night-shifts $$

remote work

what are some of the jobs in cybersecurity?

careers in infosec

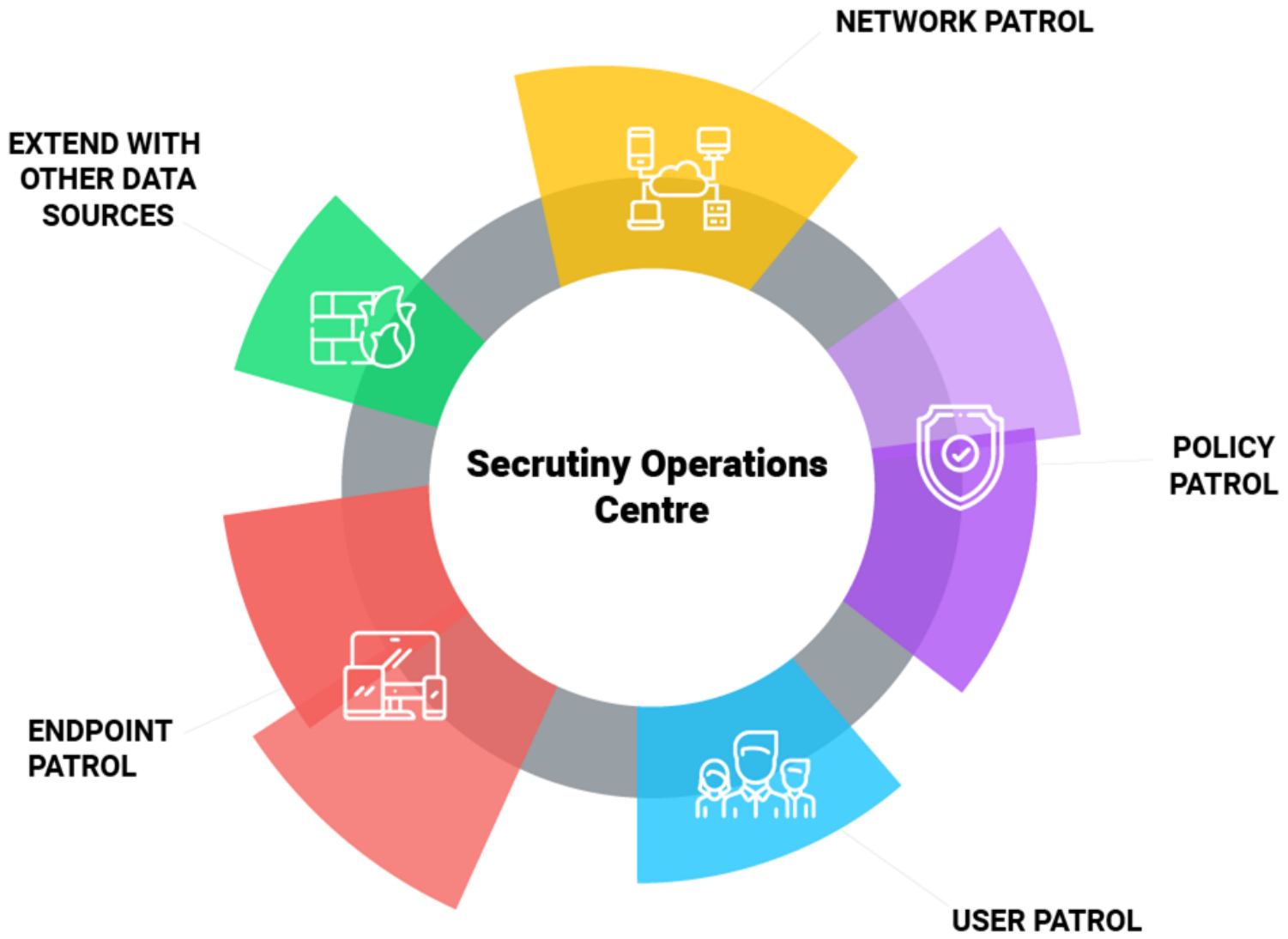
red	blue	purple	green	white
-pentester	-soc analyst	-incident responder	-grc analyst	-solutions architect
-red-teamer	-soc engineer	-incident handler/mgr.	-ISMS implementer	-trainer
-bounty hunter	-soc manager	-threat intel analyst	-compliance auditor	-advisor
-auditor	-SIEM specialist	-malware analyst	-risk analyst	-insurance analyst
-exploit dev	-MDR analyst	-reverse engineer		-cyber litigators
-vuln researcher	-threat hunter			-sec product dev
	-network sec engr.			
	-DevSecOps			

what is a cybersecurity operation center / SOC?


Security Operations Center

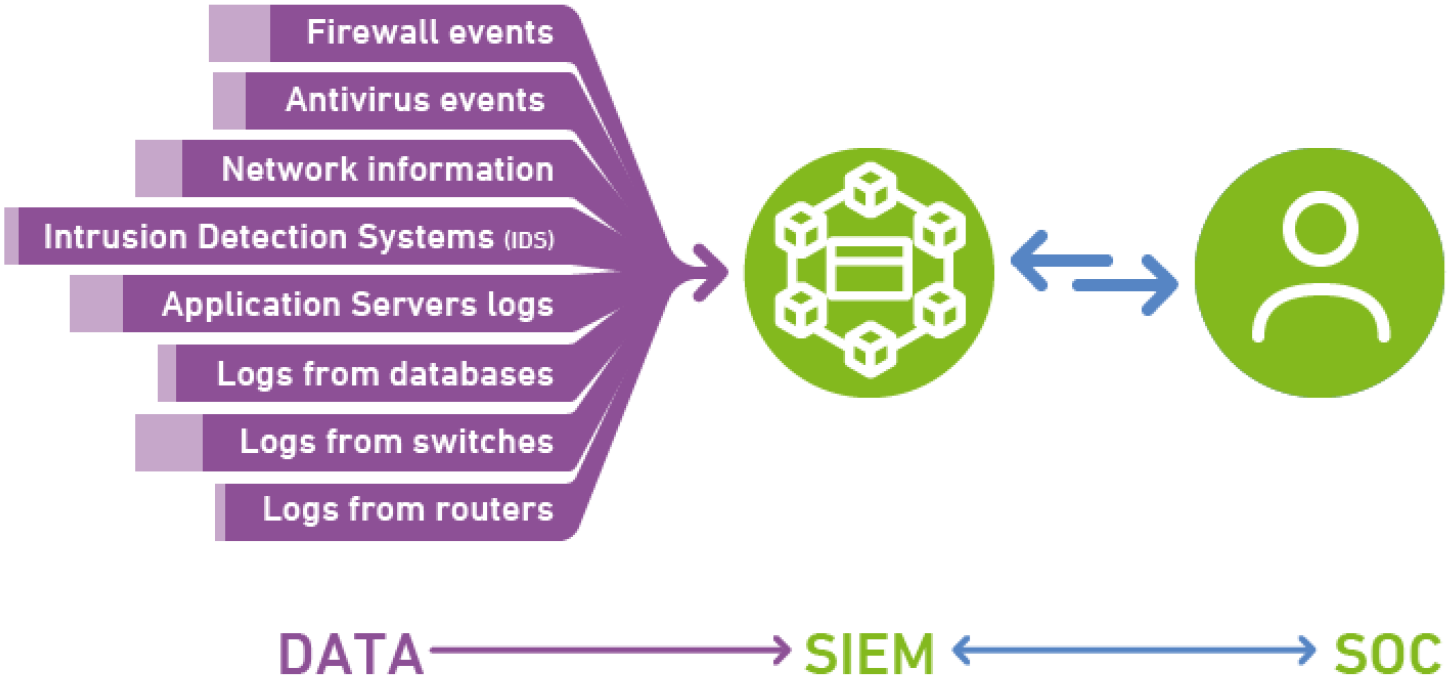
secops center

a combination of **people**, **tools** and **processes**



SIEM (security information and event management)

- single pane of glass for all security events and alerts
- integrates network equipment, security tools, servers and user workstations
- performs log collection & correlation
- integrates with ticketing solutions
- as good as its use-cases
- a dud without a good analysis team



a job in operation center / SOC?

why soc

- lower entry bar, easy to penetrate
- little to no programming language required for most roles
- handsome compensations
- extreme shortage of quality resources world-wide with steady demand

why not

- lower entry bar, easy to penetrate
- little to no programming language required for most roles
- handsome compensations
- extreme shortage of quality resources world-wide with steady demand

this is not an ideal career choice for you if you;

- can't work in 24x7 rotational shifts
- can't work on weekends and public holidays
- can't travel (20-30%) to client-side for various purposes
- don't want to be bothered by work calls/notifications during after-work hours

what are some of the blue-team roles in can get into?

blue-team roles

- soc analyst
- soc engineer
- soc manager
- SIEM specialist
- MDR analyst
- threat hunter
- network sec engr.
- solutions architect
- DevSecOps

soc roles

- **soc analyst**
- soc engineer
- soc manager
- SIEM specialist
- MDR analyst
- threat hunter
- network sec engr.
- solutions architect
- DevSecOps

- performs alert monitoring, triage & analysis
- handles escalations & handover
- performs detection use-case development & testing
- provides remediation advisory & reporting
- performs siem server/sensor healthcheck-ing
- provides incident investigation assistance

typical hiring requirements for this role

- curiosity, critical thinking and ability to analyze w/o bias
- understanding of various systems, logs and SIEM tools
- ability to work in night shifts/weekends/public holidays
- **required exp**: 0-3 years

soc roles

- soc analyst
- **soc engineer**
- soc manager
- SIEM specialist
- MDR analyst
- threat hunter
- network sec engr.
- solutions architect
- DevSecOps

- writes integrations b/w SIEM and other tools
- automates detection, triage & response routines
- integrates threat intel sources/platforms
- develops parsers for disparate data sources

typical hiring requirements for this role

- decent scripting/automation skills in python/go/bash
- hands-on with SDKs/APIs, aws/gcp, elk
- exposure to threat intel platforms/MISP
- **required exp**: 1-3 years

soc roles

- soc analyst
- soc engineer
- **soc manager**
- SIEM specialist
- MDR analyst
- threat hunter
- network sec engr.
- solutions architect
- DevSecOps

- develops SOPs and runbooks
- ensures detection & response SLAs/SLOs
- sets shift roster / on-call schedule
- creates depth in the team
- manages expectations of various stakeholders

typical hiring requirements for this role

- a hands-on background with SOC deployment & analysis
- experience with related infosec domains
- ability to manage competing priorities/pressure handling
- **required exp**: 5-7 years

soc roles

- soc analyst
- soc engineer
- soc manager
- **SIEM specialist**
- MDR analyst
- threat hunter
- network sec engr.
- solutions architect
- DevSecOps

- offers all-round expertise on specific SIEM tool(s)
- troubleshoots any tool issues faced by the sec team
- optimizes the SIEM configurations
- maintains the platform, manages the logger and ingestion pipelines
- setups platform health-checks

typical hiring requirements for this role

- thorough understanding of architecture of the underlying SIEM platform, preferred to hold vendor certs
- hands-on exp with deployment, integration, parsing
- comfortable developing apps/plugins for the given SIEM
- **required exp**: 2-4 years

soc roles

- soc analyst
- soc engineer
- soc manager
- SIEM specialist
- **MDR analyst**
- threat hunter
- network sec engr.
- solutions architect
- DevSecOps

CROWDSTRIKE Carbon Black. kaspersky FIREEYE™

- deploys, tunes and manages EDR (endpoint detection and response) tool
- keeps a tab on latest attack campaigns
- sweeps IOCs/IOAs across the entire fleet
- performs remediation actions directly on the infected system
- acquires & preserves forensic evidence in case of an intrusion

typical hiring requirements for this role

- thorough understanding of all aspects of the underlying EDR/XDR tool, preferred to hold vendor certs
- knowledge of MITRE ATT&CK, latest attack campaigns
- **required exp**: 1-2 years

soc roles

- soc analyst
- soc engineer
- soc manager
- SIEM specialist
- MDR analyst
- **threat hunter**
- network sec engr.
- solutions architect
- DevSecOps

- catches anomalies missed by the SIEM
- relies on OS telemetry and kernel system calls rather than logs
- sweeps IOCs/IOAs across the entire fleet regularly
- undertakes hunt missions with assumed breach mindset
- coordinates purple team exercises

typical hiring requirements for this role

- thorough understanding of MITRE ATT&CK, protocols, latest attack campaigns, APT groups and fileless malware
- **required exp**: 3-5 years

blue-team roles

- soc analyst
- soc engineer
- soc manager
- SIEM specialist
- MDR analyst
- threat hunter
- **network sec engr.**
- solutions architect
- DevSecOps

typical hiring requirements for this role

- thorough understanding of CIS 20 critical controls
- hands-on with heterogeneous network environments
- adequate products knowledge
- **required exp**: 1-3 years

- hardens networking equipment such as firewalls, routers, switches
- setup, maintain syslog & flowlogs collection servers and performs config & log reviews to capture any traffic based anomalies
- often responsible for IAM through radius server & network segregation
- responsible for timely updates and patches from vendors

blue-team roles

- soc analyst
- soc engineer
- soc manager
- SIEM specialist
- MDR analyst
- threat hunter
- network sec engr.
- **solutions architect**
- DevSecOps

typical hiring requirements for this role

- extensive knowledge of vendor products
- proven track record of large-scale solution design
- excellent comms and prez. skills for selling to C-levels
- **required exp**: 7-10 years

- responsible for conceiving, designing and delivering the right combination of security tools for enterprises as per needs
- provides cost estimations for the security needs of a business by taking into account its potential growth projections
- deals with vendors for demos, evaluations, POCs and cost negotiations

blue-team roles

- soc analyst
- soc engineer
- soc manager
- SIEM specialist
- MDR analyst
- threat hunter
- network sec engr.
- solutions architect
- **DevSecOps**

typical hiring requirements for this role

- extensive knowledge of the devops processes & tools
- comfortable writing complex automations & integrations
- hands-on with ci/cd, git, and essential aws/gcp services
- exposure with owasp devsecops maturity model
- **required exp**: 3-5 years

- a fancy name for cloud security
- combination of tools, practices, automation & mindset
- ensuring security is baked into devops, ci/cd, containers and microservices
- IaC for access pro/de-provisioning, infra changes, hardening & governance
- logging & alerting of detection use-cases, secret leakages & misconfigs

how does the career progression path looks like?

typical career progression

ciso

↑

director/head of security

↑

soc/security manager

↑

security lead

↑

sr. security analyst

↑

security analyst

↑

security intern / trainee

staff security engineer

↑

principle threat hunter / threat intel specialist

↑

security lead

↑

sr. security analyst

↑

security analyst

↑

security intern / trainee

solution architect / technology consultant

↑

$vendor-name specialist

↑

sr. security analyst

↑

security analyst

↑

security intern / trainee

okay i’m game, let’s talk numbers!

pakistan

- typical entry level jobs in security start either as an **intern/trainee** with a stipend of **10K-25K**/month
- **jr/security analyst** on standard probation period with a compensation ranging from **30K-70K**/month
- typical salary for a **sr. security analyst** falls between **70K-150K**/month
- **security lead** can range from **150K-250K**/month
- **security managers / HoDs**, depending upon their utility can range from **130K to 500K/month**

- provided the right exposure and training, a security analyst starts to sell like hot cakes after 2 years
- salary package for sec roles on avg. can be depicted as: **Lahore** › **Karachi** › **Islamabad**

key sec firms in PK

company	office locations	expertise
ebryx	lhr, khi, isb, usa, uae	dfir, soc, pentest, cloudsec/devsecops, malware research, training, sec dev & products
trillium	lhr, khi, isb	soc pentest, training, security products, deployments, threat intel
tranchulas	isb, australia, usa	soc, pentest, training, vulnerability research
rewterz	khi	soc, pentest, training, security products, deployments
digit labs	khi	soc, pentest, training, solution deployments, iam
commtel	lhr, khi, isb, peshawar	soc, solution deployments, training
kualitatem	lhr, usa, uk, ksa	pentest
infogistics	lhr, qatar, ksa, oman	pentest, training, compliance
systems ltd.	lhr	soc, compliance

All banks and telcos are mandated by law to have SOC teams and they have a high churn rate.

Complete list: https://github.com/huzaifahere/cyber-security-companies-in-

international (soc roles)

- **gcc**: Dubai, KSA, Qatar, Oman → **8K-20K dirhams**/month with **0% tax** deduction
- **singapore**: jobscentral.com.sg, workable.com → **50K-70K $SG** /year with **10-15% tax** deduction
- **europe**: Germany, Ireland, UK → **40K-70K euros**/year with **30-45% tax** deduction
- **usa/remote**: Upwork, Freelancer, TrustedInternet etc. → **200K PKR - 400K PKR**/month with **0% tax**

how do i prepare for soc analyst roles?

security engineer v/s **tool operator** mindset

a thorough security professional

- networking
  - Network+
  - ICND1 & ICND2
- programming
  - Powershell, Python, Bash
- essential security
  - Security+
  - SANS SEC401
  - EC-Council CEH
  - SANS SEC502
- essence of SOC/NSM (L1/2 role)
  - SANS SEC511: Continuous Monitoring and Security Operations
  - Tao of network security monitoring by Richard Bejtlich
  - The practice of network security monitoring by Richard Bejtlich
  - Applied Network Security Monitoring by Chris Sanders
- advanced DPI & IR for L2/3 roles
  - SANS SEC556: Comprehensive Packet Analysis
  - SANS SEC503: Intrusion Detection In-Depth
  - Practical Packet Analysis by Chris Sanders (Book + Training)
  - Investigation Theory: The Mind of an Analyst by Chris Sanders
  - GIAC GCFE - SANS FOR408/500
  - GIAC GCIH - SANS SEC504 Hacker Techniques, Exploits
- DFIR for L3/SME (subject matter expert) roles
  - GIAC GNFA - FOR572: Advanced Network Forensics and Analysis
  - GIAC GCFA - FOR508: Advanced Incident Response and Threat Hunting
  - SANS SEC550: Active Defense, Offensive Countermeasures, and Cyber Deception
  - SANS FOR578: Cyber Threat Intelligence
- non-tech
  - MS Office/Google Docs
  - OTRS/Atlassian/ManageEngine
  - Report writing: Effective Information Security Writing by Chris Sanders

fast-track SOC analyst

- **SIEM specialist**
- **MDR analyst**

- all major SIEM players offer their training & certifications
- typically divided into admin, deployment, dev and analysis categories
- do market research to decide what vendor(s) you want to train/certify on
- banks in PK typically use IBM QRadar, telcos go with MicroFocus (formerly HPE Arcsight)
- tech companies and fintech are mostly cloud hosted so make sure to choose the right vendor
- *certifications do not guarantee a job but they can surely help your CV stand out from the rest*

how is it like working in a SOC?

Expectations

Reality

certifications

- eLearnSecurity Certified Threat Hunting Professional
- GIAC Continuous Monitoring Certification (GMON)
- SEC455: SIEM Design & Implementation
- SEC555: SIEM with Tactical Analytics
- SEC541: Cloud Security Monitoring and Threat Hunting
- AWS security speciality

labs/ctf

- Pico CTF
- DevSecOps challenges
- Malware-Traffic-Analysis
- Mossé Cyber Security Institute
- cloud security labs

trainings

- ELK for security analysis by Chris Sanders
- ELK training by Elastic.co (Free)
- DPI using wireshark (free)
- Applied Network Defense - Practical Threat Hunting
- SEC586: Blue Team Operations: Defensive PowerShell
- SEC584: Cloud Native Security: Defending Containers & K8s
- FireEye cyber threat hunting training

blogs

- soc analysts illustrated primer by John Strand
- how to be a mentor & mentee by John Strand
- SANS reading room
- awesome blue-teaming resources
- bsides islamabad discord server

Gispp Resources

- Information Security Career Guide
- Career Advice
- Technical Sessions Archive

gispp.org https://www.facebook.com/gispp.org/ https://www.linkedin.com/groups/10314172

https://www.instagram.com/gispp2019/ https://twitter.com/GisppOrg https://bit.ly/2T6RhRa