

## MEMORANDUM

To: Network Operations Management

From: Team 03

Date: October 18, 2025

Subject: Security Team Organization

Our security team works across multiple technical disciplines and professional responsibility. **Eight full-time staff** comprise the security team.

To best organize business needs and strengthened team efficacy, each team member has a **primary responsibility and a secondary responsibility**.

Team members spend most of their time developing skills and tools to aid their primary responsibility although they also work diligently to ensure that they are foundationally proficient in their secondary role. Team members practice consistently to develop these skills and maintain their effectiveness. In the case that an individual is unable to fulfill their primary responsibility, the secondary lead will step in and assume given role.

The team is also **cross-trained in all responsibilities** at a shallow level in order to best understand the cohesion of the business.

With the current configuration of our security team and their associated responsibility, we **adequately and comprehensively cover all essential aspects associated with the security of our organization**.

The following table identifies the primary and secondary responsibilities assigned to our team members, although not identifying them personally. The table also specifies the key skills that are associated with the roles undertaken by our security team.

Primary	Secondary	Primary Key Skills & Knowledge
Team Lead	Incident Investigation	<i>Skills:</i> Leadership, Business Prioritization, Professional Communication, each concept required for the team <i>Tools:</i> Each tool required for the team
Windows Administration	Linux Administration	<i>Skills:</i> Operating Systems, Incident

		Investigation, Networking <i>Tools:</i> Active Directory, Domain Name Services, Windows Operating Systems, PowerShell, Windows Servers
Firewalls	Team Lead	<i>Skills:</i> Networking, Subnetting <i>Tools:</i> Palo Alto Firewalls, Cisco Firewalls, pfSense
Network Engineering	Firewalls	<i>Skills:</i> Networking, Subnetting <i>Tools:</i> ESXI, Cacti, Proxmox
Vulnerability Management	Network Engineering	<i>Skills:</i> Threat Intelligence, Adversary Emulation, Vulnerability Management <i>Tools:</i> OpenVAS, Nmap, Wireshark
Linux Administration	Threat Intelligence	<i>Skills:</i> Operating Systems, Incident Investigation, Networking, Mail <i>Tools:</i> Linux Operating Systems,
Organizational Communications	Windows Administration	<i>Skills:</i> Risk Management, Industry Standards, Business Communication, Professional Communications, Customer Success <i>Tools:</i> Microsoft Office, Libre Office
Incident Investigation	Organizational Communications	<i>Skills:</i> Security Information and Event Monitoring (SIEM), Incident Response, Operating Systems, Networking <i>Tools:</i> Splunk

Please let us know if there are any other actions we can perform at this time.

Best regards,

Team 03