**MEMORANDUM**

To: Management

From: Team

Subject: Team Roles

Date:

The security team works across multiple technical disciplines and professional responsibilities. Eight full-time staff comprise the security team.

To best organize business needs and strengthen 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 In the case that an individual is unable to fulfill their primary responsibility, the secondary lead will step in and assume responsibilities. The team is also cross-trained in all responsibilities at a shallow level in order to best understand the cohesion of the business.

|  |  |  |  |
| --- | --- | --- | --- |
| **Individual** | **Primary** | **Secondary** | **Primary Key Skills & Knowledge** |
|  | Team Lead | Incident Investigation | *Skills:* Leadership, Business Prioritization, Professional Communication, each concept required for the team *Tools:* Each tool required for the team |
|  | Windows Administration | Linux Administration | *Skills:* Operating Systems, Incident Investigation, Networking *Tools:* Active Directory, Domain Name Services, Windows Operating Systems, PowerShell, Windows Servers |
|  | Firewalls | Team Lead | *Skills:* Networking, Subnetting *Tools:* Palo Alto Firewalls, Cisco Firewalls, pfSense |
|  | Network Engineering | Firewalls | *Skills:* Networking, Subnetting *Tools:* ESXI, Cacti, ProxMoc |
|  | Vulnerability Management | Network Engineering | *Skills:* Threat Intelligence, Adversary Emulation, Vulnerability Management *Tools:* OpenVAS, Nmap, Wireshark |
|  | Linux Administration | Threat Intelligence | *Skills:* Operating Systems, Incident Investigation, Networking, Mail *Tools:* Linux Operating Systems, |
|  | Organizational Communications | Windows Administration | *Skills:* Risk Management, Industry Standards, Business Communication, Professional Communications, Customer Success *Tools:* Microsoft Office, Libre Office |
|  | Incident Investigation | Organizational Communications | *Skills:* Security Information and Event Monitoring (SIEM), Incident Response, Operating Systems, Networking *Tools:* Splunk |

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

Thank you,

Team 01