# vCISO Suite - Installation Guide (Bare-Metal Edition)

## System Requirements

OS: Ubuntu 22.04 LTS (preferred)

CPU: 4-core (Intel i5/Ryzen 5)

RAM: 16 GB

Storage: 100 GB SSD

Network: Ethernet preferred

## 1. Clone the Repository

```
git clone https://github.com/yourusername/vciso-suite.git
cd vciso-suite
```

## 2. Install Dependencies

```
sudo apt update && sudo apt upgrade -y
sudo apt install docker.io docker-compose curl unzip git ufw fail2ban -y
sudo usermod -aG docker $USER
```

## 3. Configure the Firewall

```
sudo ufw allow OpenSSH
sudo ufw allow 5601,5044,9200,8080,8081,8082,8200,9000,9001,8443,3780/tcp
sudo ufw enable
```

## 4. Launch the Suite

```
docker-compose up -d
```

(Wait a few minutes for all containers to initialize.)

### 5. Access the Tools

Kibana (SIEM): http://localhost:5601

Nexpose (Vuln Scanning): http://localhost:3780

Wazuh (EDR): Port 1514/1515

TheHive (IR): http://localhost:9000

Cortex (Response): http://localhost:9001

MISP (Threat Intel): https://localhost:8443

Bitwarden (Passwords): http://localhost:8081

Keycloak (IAM): http://localhost:8080

Nextcloud (File Sharing): http://localhost:8082

Duplicati (Backups): http://localhost:8200

BookStack (Docs/GRC): http://localhost:6875

### Optional: Windows Endpoint Logging

Use the provided PowerShell script `install-sysmon.ps1` to install Sysmon and Winlogbeat. Update $ELK_IP in the script to your server IP.

### Optional Enhancements (Already Included)

- ElastAlert2: Email/Slack alerting for ELK
- Cortex: Automates response actions from TheHive
- BookStack: Includes GRC templates and OWASP WSTG docs

### Stopping the Suite

```
docker-compose down
```

## Updating the Suite

```
git pull
docker-compose pull
docker-compose up -d
```

## Backup Critical Data

Use Duplicati or back up volumes:

- elasticsearch-data
- bookstack-data
- bookstack-db-data
- cortex-data
- duplicati-data
- nextcloud-data

## Support & Docs

BookStack contains internal docs, policies, and templates.

Refer to README in repo for roadmap and tool documentation.