RANGEFORCE

Certificate of Continuing Education Completion

THIS CERTIFICATE IS AWARDED TO

Thomas Campagna Kunrath

For successfully completing 202 modules, from 09/14/2023 to 09/15/2024, equivalent to 47 hours and 39 minutes of study, provided by the RangeForce Platform

Modules completed are shown in Annexes

09/14/2024

Date

Taavi Must, President of RangeForce

Annex 1

- Microsoft Sentinel: Log Analytics
- QRadar Overview
- QRadar: Basics
- Introduction to Phantom Configuration
- Splunk: Fields and Transforms
- Splunk: Filters and Queries
- Splunk: Basics
- Vulnerability Prevention Guidelines: Mobile
- CVE-2017-6327 Symantec Messaging Gateway RCE: Overview
- CVE-2020-5902 F5 BIG-IP Load Balancer Overview
- CVE-2018-6789 Exim Buffer Overflow
- Microsoft Sentinel: Detection Rules
- Microsoft Sentinel: Threat Management
- Phantom Overview
- Introduction to the SOC
- Introduction to SIEM and SOAR
- Burp Suite: Basics
- Stored XSS
- Reflected XSS
- Microsoft Sentinel: Introduction
- Greenbone Vulnerability Management
- Nmap: NFS Enumeration
- Nmap: SNMP Enumeration
- Nmap: Basics
- Cybersecurity Kill Chain
- Handover Procedures
- Cybersecurity Terminology
- Introduction to Egregor Ransomware
- Introduction to Vulnerability Scanning
- Keys to Useful Threat Intelligence
- Incident Handling
- Managing Incident Response
- Cloud Security - Access Control
- Limiting Access
- Broken Access Control Overview
- Microsoft Identity and Access Management Solutions
- Kerberos Overview
- Implement Secure Authorization
- Identify the Need to Protect IoT Resources
- Manage Risks Related to IoT Device Operating Systems and Firmware
- Map the IoT Attack Surface
- Vulnerability Prevention Guidelines: IoT
- Introduction to Fully Automated Analysis
- Sandbox Evasion Techniques
- Malware Sandboxing
- Introduction to Malware Analysis Stages
- Malware Analysis: VirusTotal
- Malware Analysis: Introduction to Basic Tools
- Introduction to Malware Analysis
- CVE-2020-10189 Zoho ManageEngine RCE Overview
- CVE Overview
- Introduction to Mobile Device Management
- Introduction to Memory Forensics
- Evidence Acquisition and Preservation
- Introduction to File System Forensics
- Introduction to Digital Forensics
- Cryptography Overview
- Anticipating Ransomcloud Attacks
- Linux User Management
- Work Email Handling
- Phishing Urgency
- Chain Mail
- Think Twice - Proper Email Etiquette
- CEO Scam
- Spyware in Attachments
- Malicious Attachments
- Zoom Bombing
- Unknown Networks
- Autofill
- Online PDF Makers
- HTTPS
- Server Protection Overview
- RansomEXX Ransomware TTP
- Hafnium TTP
- Ryuk Ransomware TTP
- Emotet TTP
- Understanding TTPs
- Linux File Permissions and Ownership
- Networking Security Services in Azure
- Azure Security Monitoring
- MITRE ATT&CK Overview
- Phonelocking
- Juice Jacking
- Mobile Listening
- Password Sharing
- Same Passwords
- Password Handling
- Password Managers
- Multi-factor Authentication
- Passphrases
- Passwords
- Phishing Response Actions
- Network Printer
- Free WiFi
- VPN
- Introduction to Cloud Ransomware
- Update Your Software
- Ransomware Attack
- Keylogger
- Spyware
- Ransomware
- Security Topology
- Understanding the Threat Landscape
- Cybersecurity Teams
- Introduction to Cybersecurity Terminology
- Layer 2 Networking
- Linux File Management
- Basic Linux File Editing
- Linux CLI Introduction
- AWS Security Overview
- AWS Security Hub Overview
- Ransomware Kill Chain
- Anticipating Ransomware Attacks
- The Evolution of Ransomware
- YARA Overview
- Traffic Light Protocol Overview
- Ransomware Overview
- Overview of Data Breaches
- Offensive Security Assessments
- Lateral Movement Overview
- IAM Overview
- Burp Suite Overview

Annex 2

- Linux Authentication
- Layer 3 Networking: Routing
- Access Token Manipulation Introduction
- Rundll32 Introduction
- IDS/IPS Overview
- Firewall Overview
- Layer 3 Networking: Overview
- Software Installs
- Home WiFi
- Check Account Number: Fake Invoices
- Popups
- Spreading Viruses
- Removable Media
- Security Awareness
- Company Credit Cards
- Physical Media
- Clean Desk
- Stakeout
- Tailgating 2
- Valuables in Car
- Privacy Screens
- Unattended Computers
- Tailgating
- Microsoft Office Risk
- Dumpster Diving
- USB Key Drops
- Printouts
- Unnecessary Data
- Keeping Data Safe
- Think Twice Before You Post
- Handling Confidential Material
- GDPR
- Data Leaks
- Conference Risk
- Romance Scams
- Sharing Information
- Correct Links
- Doublecheck Before You Trust
- Vishing
- Social Engineering
- Extortion Emails
- Misinformation
- Privilege Escalation: Introduction
- Introduction to Password Cracking Countermeasures
- Password Security In-Depth
- Introduction to Email Based Threats
- Red Team Functions and Tasks
- Blue Team Functions and Tasks
- History of Cybersecurity
- MITRE D3FEND Overview
- NICE Roles for Cybersecurity Workforce Overview
- Introduction to Defense Readiness Index
- Cloud Access Security Broker Introduction
- Containing Lateral Movement in the Cloud
- Cloud Security - Misconfigurations
- Cloud Security - Shared Responsibility
- Hybrid Cloud Overview
- Cloud Security Overview
- Endpoint Protection Overview
- Endpoint Detection and Response
- NIST Cybersecurity Framework Overview
- Introduction to Governance, Risk, and Compliance
- Information Security Governance
- Snyk
- SAST: SonarQube Introduction
- PCAP Forensics: Wireshark
- WireShark Overview
- Introduction to Networking
- Introduction to OSI Networking Model
- Conducting a Risk Assessment
- The Importance of Risk Management
- Introduction to the (AR)² Framework
- Understanding the Cyber Kill Chain
- Introduction to Social Engineering
- Spear Phishing
- Shoulder Surfing
- Phishing
- Module Tutorial
- Learner Onboarding Video
- The Building Blocks of InfoSec