Appendix: Marist College SOC and Related Facilities, Equipment, and Resources

NSF-Funded Shared Research Facilities Lab includes

IBM System z114 Model M05, 120 GB Memory, 2 General Purpose and 3 IFL Engines (NSF-Funded) IBM System zEnterprise Blade Extension (zBX) (NSF-Funded)

zBX includes: 2 HX5 System x Blades and 2 PS701 Power Blades, 64 GB each (NSF-Funded) IBM Storwize V7000 Disk Storage with 12.5 TB (NSF-Funded)

IBM PureFlex (3 Power and 3 x86 8-Core Nodes) and IBM PureData for Analytics systems 6 IBM xServer 345 servers, 2 GHz Xeon, 2 GB RAM, 73 GB SCSI

2x IBM J48E Ethernet Switches 2x Brocade 8000 Switches

4x IBM G8264 Switches

4x Plexxi Ethernet Switches

4x IBM System X 3550 M3 Servers

3x Adva FSP 3000, populated with 6 wavelengths each 2x Ciena 6500 packet optical transport platforms

Cisco 2800 Router.

Dedicated and Shared Scalable Computing Facilities

IBM BC12 Mainframe and IBM LinuxOne, z/OS, z/VM and z/Linux on System z, 10 IBM pSeries servers including models up to a p550 8-way P5 processors running AIX/Linux, IBM PureFlex and IBM PureData systems, DASD (Storage over 300 TB of state of the art disk arrays), DS4800, DS8100, DS8300. DS8800, DS8700, V7000, SVC managed SAN (Storage Area Network), ATL (Automated Tape Library), Intel based Linux and Windows Servers, Intel and AIX based servers, Infrastructure for Virtualized Servers on z/VM, AIX, VMWare ESX, and Hyper-V, DB2, Oracle, Microsoft SQL Server, MySQL, Content Manager (v8.x), WebSphere Application Server and Web Services, Apache, Tomcat Application Servers, Library OPAC (Voyager), Survey Tools, Individual workstations (Linux, Windows 10, Mac OS X), Virtual Linux and Windows Servers, Virtual Computing Lab (VCL), IBM SPSS Server, Cognos Business Intelligence Server, Shared Printers, Office Suite (MS Office 2010 and 2013 Professional), Adobe suites, Software

A. E. Hassanien and M. Elhoseny (eds.), *Cybersecurity and Secure Information Systems*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-030-16837-7

Languages/Tools: C++, C#, Visual Basic, JAVA, J2EE, PHP, PERL, XML, Software Applications: Visual Studio, Matlab, Maple, Xcode, and iOS SDK.

Linux Research and Development Lab which contains

Lenovo M92z All-in-One, Quad Core i5 2.9 GHz, 8 GB RAM, 500 GB SATA HDD, DVD RW, Keyboard, Optical Mouse, Ubuntu 12.04 LTS, VMWare Workstation 9.0.2, Windows 10 Professional VM, integrated 23″ widescreen LCD.

PC Lab Facilities contain

Lenovo M92z All-in-One, Quad Core i5 2.9 GHz, 8 GB RAM, 500 GB SATA HDD, DVD RW, Keyboard, Optical Mouse, Windows 10 Professional, integrated 23″ widescreen LCD.

High Speed Network Infrastructure

The three data centers are interconnected by a multi-Gigabit backbone, 10Gb Core with quad SUP VSS enabled and 1 Gb/s to the desktop (all facilities networked on campus), Switches: Cisco network of 6513s, 6509s, 3750Xs, 3560s, and 2950s. Security: Cisco ISE, DMZ, Juniper Intrusion Prevention System, Cisco VPN, Cisco NAC, and Network Proxies, Internet 2 Institution (100 Mb/s), Dual Commodity Internet (1 Gb/s IPv4, IPv6) and Wireless: Cisco Wireless 5508 Modules control over 700 802.11a/g/n Cisco wireless access points (1242, 1500, 3500i and 3600). They have access to high speed international WAN backbone through Internet2 consortium. Networked Think: Centre desktops or ThinkPad laptops for full-time faculty.

Software Defined Networking (SDN) Laboratory Test Bed

This laboratory is a research and research training test bed consisting of three data centers on the Marist campus, interconnected by a 10 Gb/s, 100 km ring of single-mode optical fiber. Each data center houses a combination of compute and storage resources including IBM PureSystems, Power servers, z System enterprise servers, NetApp storage, and v7000 storage. Each center is connected by dense optical wavelength division multiplexing (WDM) equipment, with optical pre- and post-amps as required and demarcation monitoring (Adva XG210 or similar). Networking within the data centers is a configuration of switches and routers from Cisco, Brocade, IBM/Lenovo, Ciena, and Plexxi. IBM Cloud Orchestrator software provides cloud management IT services. As a member of the NyserNet regional network, Marist has access to a high speed MAN/WAN backbone. Marist is creating a dedicated dark fiber connection between this lab and a peering point in NYC which will facilitate global access. SDN network controllers available include Open Daylight from the Linux Foundation, FloodLight, and various vendor proprietary controllers from IBM and Ciena. The lab supports VMWare and KVM virtualization, runs the latest version of OpenStack with FloodLight and Open Daylight cloud middleware, and supports both open source and vendor proprietary cloud orchestration software.

Education and Research Security Operations Center (SOC)

This facility recreates a SOC environment for education and research purposes. Located on the Marist Campus in Hancock Building room 0005, the facility grand opening was held in September 2018. The SOC includes the following:

"smart" classroom with four wall-mounted 72-in. diagonal MondoPad computers, each of which includes build-in web browser, touch screen white board, cloud connected data storage, video conferencing facilities, and ability to cast to/from any computer in the room.

32 desktop computers, partitioned to run Windows or Linux operating systems 32 desktop computers, running Apple iOS operating system.

Ceiling-mounted video projection display with drop-down movie screen.

Software currently installed in the SOC includes the following, under academic license: IBM QRadar, IBM AppScan, IBM i2 Analyze, Cisco Umbrella, Cisco Firepower Threat Defense, Cisco CloudLock, BlackRidge Cloud Dashboard.

In addition the SOC lab is equipped to perform forensic analysis on botnets and malware, including two mobile field kits and one base forensics system with the following specifications: Chipset: Intel® C612 chipset, Two-Intel® Xeon E5-2620v4 2.1GHz, 8-core, 15 MB Cache, Memory: 64 GB DDR4 Registered ECC 2133 MHz, Integrated LAN: Intel® Gigabit LAN Controller, 2 GB DVI and HDMI, 5 External Drive Bays (Tableau T356789iu SATA/SAS/ IDE/USB 3.0/FW/PCIe Forensic Bridge, Forensic Computers Drive Dock (Used in conjunction with Tableau T35689iu), Read Only Media Reader, Trayless SATA Assembly (Read/Write), Triple Burner (BluRay, DVD, CD); Two 500 GB RAID 0, Two 500 GB, Four 2 TB SAS Hard Disk Drives configured in RAID 5 and One 250 GB SATA III SSD for OS, Tableau TD2u forensic duplicator, Bridges (Tableau T35u R/O, T35u R/W, T6u R/O, T8u), Cables (Three SA TA cables, Four Unified SAS cable, Three IDE cables, Three 3M to Molex power cables, Three 3M to SATA power cables, Two USB 3.0 Type A to Type B Power Supplies and Adapters, Tableau TP2 Media Reader, mSATA/M.2 Adapter TDA-TKA5 Adapter Kit.

Course materials in the cybersecurity education program are based on the requirements of the ISC^2 certification and NIST risk management framework. The program covers all topics requires for U.S. Government courseware certification NSTISSI 4011: National Training Standard for Information Systems Security (INFOSEC) Professionals http://en.wikipedia.org/wiki/Committee_on_National_Security_Systems and maps to the requirements from the following organizations:

National Centers of Academic Excellence (CAE)/Cyber Defense Education Program NSA/DHS sponsored program through CISSE http://www.cisse.info/

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework http://csrc.nist.gov/nice/framework/

DHS National Initiative for Cybersecurity Careers and Studies (NICSS) http://niccs.us-cert.gov/

Department of Defense Cybersecurity Workforce Strategy (DCWS) and Workforce Development Framework (CWDF) including DoDD 8570.01 Information Assurance Training, Certification and Workforce Management (emerging) http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed%28final%29.pdf.