CAPITOL TECHNOLOGY UNIVERSITY

1927

Integrating security operations experience into a four year undergraduate cyber security program

Capitol is a NSA and DHS National Center of Academic Excellence in Cyber Defence Education

CAPITOL TECHNOLOGY UNIVERSITY
1927

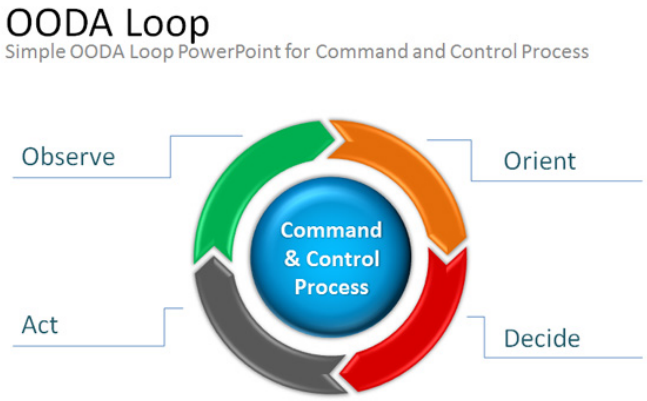
Concept of Operations

Capitol will integrate a security operations experience into its Bachelor of Science in Cyber and Information Security Program. This unique operational experience will better prepare our graduates to protect and defend networks by integrating the required tools and technologies into a CONOPS. Students will be trained and mentored by both vendors, faculty and alumni knowledgeable of SOC operating tools and techniques. Students will receive industry recognized certifications where appropriate and focused experiences with those tools.

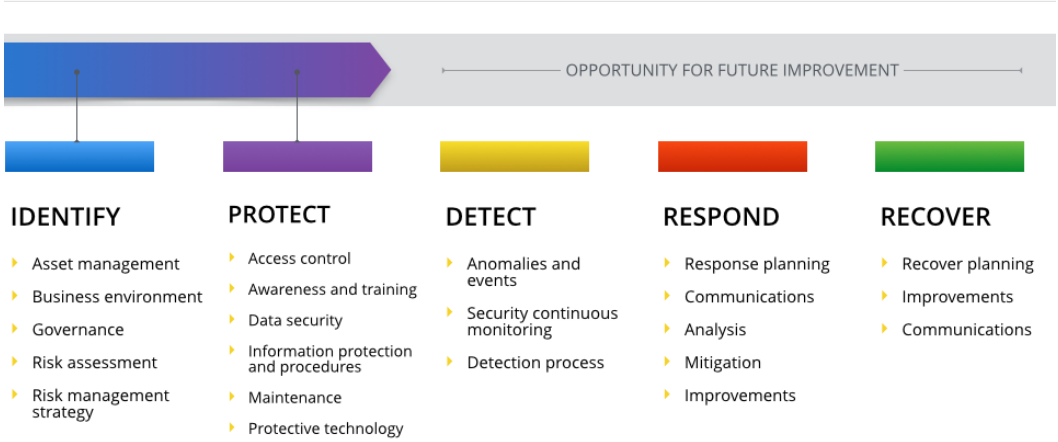
CAPITOL TECHNOLOGY UNIVERSITY
1927

Situational Awareness towards Situational Understanding

Colonel John Boyd- OODA Loop



Boyd's theory of operating inside an adversary's decision cycle -or OODA loop- and its relationship to conflict was a bold new conception. His strategic aim was to isolate his adversary – physically, mentally, and morally – from his external environment by destroying his view of the world: his orientation (Spinney, 1997).



SA cannot be taught – it must be built through a series of focused experiences

CAPITOL TECHNOLOGY UNIVERSITY
1927

Critical issues this initiative will address

Employers require graduates to have:

- Work experience
- College Degrees
- Cyber Security Certifications
- Analytic Skills

Work Force

Persons working in this Specialty area may have job titles similar to:

- CND Analyst (Cryptologic)
- Cyber Security Intelligence Analyst
- Focused Operations Analyst
- Incident Analyst
- Network Defense Technician
- Network Security Engineer
- Security Analyst
- Security Operator
- Sensor Analyst

Source: NICE Framework

This initiative delivers:

- Real world work experiences to students in an operational environment
- Opportunities to earn certifications with operational experience specific to that certification
- Deep knowledge and experience in the NICE **protect** and **defend** specialty areas preparing them for entry level positions such as Incident Analyst

CAPITOL TECHNOLOGY UNIVERSITY
1927

Security Operations Centers (SOC)

Security Operations Centers (SOCs) to provide increased security and rapid response to events throughout their networks. Building a SOC can be a monumental task. Although the finer points of SOC deployment are very much network-specific, there are several major components that every organization must include: people, process, and technology. The three exist in all elements of security and should be considered equally critical components.

McAfee. Part of Intel Security (2013). *Creating and Maintaining a SOC: The details behind successful security operations centers.* Retrieved from http://www.mcafee.com/us/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf

CAPITOL TECHNOLOGY UNIVERSITY
1927

B.S. Cyber and Information Security Program

Bachelor of Science - 127-130 credits

Programming and Computers - 31 Credits

CS-130 Computer Science Fundamentals I
CS-150 Introduction to Programming Using C
CS-220 Database Management
CS-230 Computer Science Fundamentals II
CS-320 Database Administration
CS-418 Operating Systems
CT-152 Introduction to Unix
CT-206 Scripting Languages
CT-240 Internetworking with Routers and Switches
SE-458 Senior Project

Information Assurance - 27 Credits

IAE-201 Introduction to Information Assurance Concepts
IAE-301 Comprehensive Computer and Network Security*
IAE-315 Secure System Administration and Operation*
IAE-321 Applied Wireless Network Security*
IAE-325 Secure Data Communications and Cryptography* 3
IAE-402 Introduction to Incident Handling and Malicious Code* 3
IAE-405 Malware Analysis/Reverse Engineering* 3
IAE-406 Digital Forensics and the Investigative Process* 3
IAE-410 Penetration Testing* 3

Management - 6 Credits

BUS-174 Introduction to Business and Management 3
BUS-301 Project Management 3

Mathematics and Sciences - 17 Credits

MA-114 Algebra and Trigonometry 4
MA-124 Discrete Mathematics 3
MA-128 Introduction to Statistics 3
MA-261 Calculus I 4
Science Elective** 3

English Communications - 9 Credits

EN-101 English Communications I 3
EN-102 English Communications II 3
EN-408 Writing Seminar in Technical Research 3

Humanities/ Social Sciences - 18-19 Credits

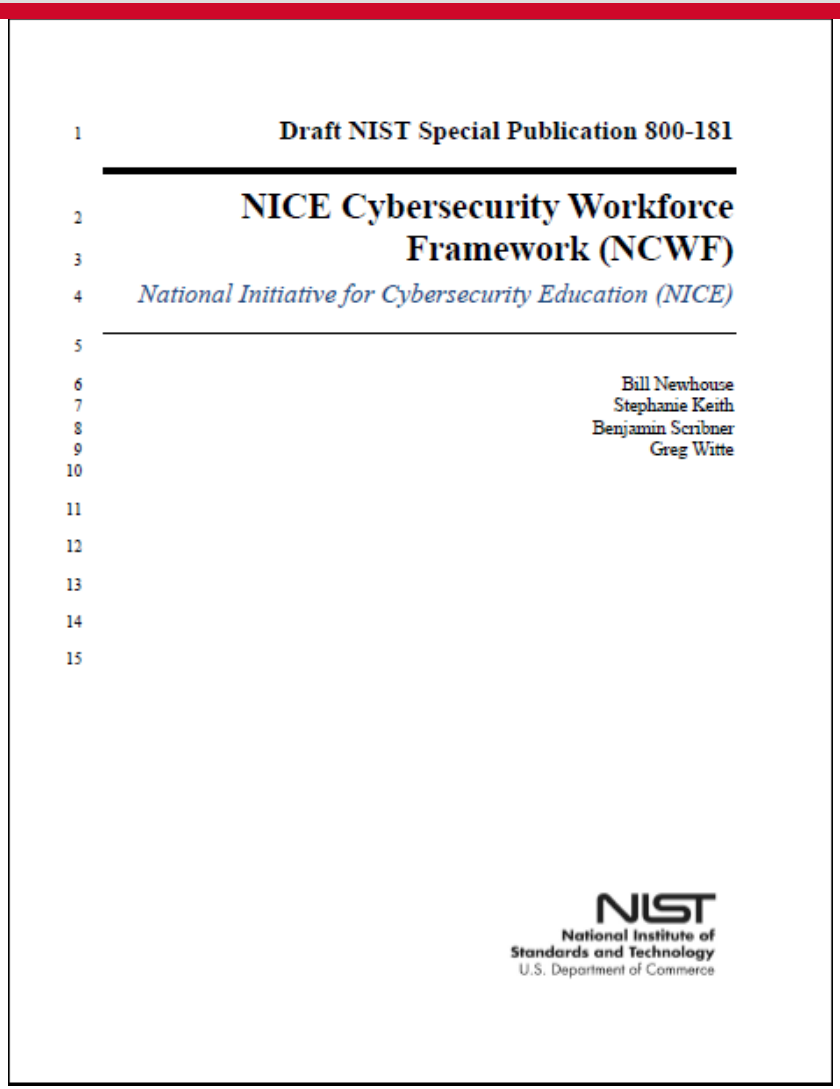
FS-100 Freshman Seminar 1
HU-331or HU-332 Arts and Ideas 3
SS-351 Ethics 3
Humanities Electives (2)** 6
Social Science Electives (2)** 6

General Electives 19-21 Credits***

CAPITOL TECHNOLOGY UNIVERSITY
1927

NIST SP 800-181

This publication describes the NICE Cybersecurity Workforce Framework (NCWF), the product 94 of many years of collaboration regarding workforce training and education. NCWF provides a 95 fundamental reference resource for describing and sharing information about cybersecurity work 96 roles, **the discrete tasks performed by staff within those roles**, and the knowledge, skills, and 97 abilities (KSAs) needed to complete the tasks successfully. As a common, consistent lexicon that 98 categorizes and describes cybersecurity work, the NCWF improves communication about how to 99 identify, recruit, develop, and retain cybersecurity talent. The NCWF is a resource from which 100 organizations or sectors can develop additional publications or tools focused on defining or 101 providing guidance on aspects of workforce development, planning, training, and education.



Draft NIST Special Publication 800-181

NICE Cybersecurity Workforce Framework (NCWF)

National Initiative for Cybersecurity Education (NICE)

Bill Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CAPITOL TECHNOLOGY UNIVERSITY

1927

NIST SP 800-181

Table 2 - NCWF Workforce Categories

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, and builds secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence
Collect and Operate (CO)	P c
Investigate (IN)	I t

Categories	Specialty Areas	Specialty Area Descriptions
		use information technology (IT) (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life-cycle.
Protect and Defend (PR)	Cybersecurity Defense Analysis (DA)	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.
	Cybersecurity Defense Infrastructure Support (INF)	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.
	Incident Response (IR)	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.
	Vulnerability Assessment and Management (VA)	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.

SOC operations specialty areas are covered in the Protect and Defend (PR) category

CAPITOL TECHNOLOGY UNIVERSITY
1927

Cyber Defense Analyst (511)

Work Role ID	**PR-DA-001**
Category	**Protect and Defend (PR)**
Specialty Area	**Cyber Defense Analysis (DA)**
Work Role Name	**Cyber Defense Analyst (511)**
Work Role Description	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs.) to analyze events that occur within their environments for the purposes of mitigating threats.
Tasks	T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0099, K0104, K0106, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0273, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0331, K0339, K0342
Skills	S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0167, S0169
Abilities	A0010, A0015, A0066

CAPITOL TECHNOLOGY UNIVERSITY
1927

Cyber Defense Infrastructure Support Specialist (521)

Work Role ID	**PR-INF-001**
Category	**Protect and Defend (PR)**
Specialty Area	**Cyber Defense Infrastructure Support (INF)**
Work Role Name	**Cyber Defense Infrastructure Support Specialist (521)**
Work Role Description	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software
Tasks	T0042, T0180, T0261, T0335, T0348, T0420, T0438, T0483, T0486
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0033, K0042, K0044, K0062, K0104, K0106, K0135, K0157, K0179, K0205, K0258, K0274, K0324, K0331, K0334, K0340
Skills	S0007, S0053, S0054, S0059, S0077, S0079, S0121, S0124
Abilities	[None specified]

CAPITOL TECHNOLOGY UNIVERSITY
1927

Cyber Defense Incident Responder (531)

Work Role ID	**PR-IR-001**
Category	**Protect and Defend (PR)**
Specialty Area	**Incident Response (IR)**
Work Role Name	**Cyber Defense Incident Responder (531)**
Work Role Description	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
Tasks	T0041, T0047, T0161, T0163, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0333, T0395, T0503, T0510
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0026, K0033, K0034, K0041, K0042, K0046, K0058, K0062, K0070, K0106, K0157, K0161, K0162, K0167, K0177, K0179, K0221, K0225, K0230, K0259, K0287, K0332
Skills	S0003, S0047, S0077, S0078, S0079, S0080, S0173
Abilities	[None specified]

CAPITOL TECHNOLOGY UNIVERSITY
1927

Vulnerability Assessment Analyst (541)

Work Role ID	**PR-VA-001**
Category	**Protect and Defend (PR)**
Specialty Area	**Vulnerability Assessment and Management (VA)**
Work Role Name	**Vulnerability Assessment Analyst (541)**
Work Role Description	Performs assessments of systems and networks within the NE or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Tasks	T0010, T0028, T0138, T0142, T0188, T0252, T0549, T0550
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0021, K0033, K0044, K0056, K0061, K0068, K0070, K0085, K0089, K0106, K0139, K0161, K0167, K0177, K0179, K0203, K0206, K0210, K0224, K0265, K0287, K0301, K0308, K0331, K0342, K0344, K0345
Skills	S0001, S0009, S0025, S0044, S0051, S0052, S0081, S0120, S0137, S0171
Abilities	A0001, A0044

CAPITOL TECHNOLOGY UNIVERSITY
1927

Tasks

These tasks can be structured in such as way to provide the student a progressive level of responsibility and advancing skill set within the SOC

Expert

Intermediate

Beginner

Work Role ID	PR-VA-001
Category	Protect and Defend (PR)
Specialty Area	Vulnerability Assessment and Management (VA)
Work Role Name	Vulnerability Assessment Analyst (541)
Work Role Description	Performs assessments of systems and networks within the NE or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.
Tasks	T0010, T0028, T0138, T0142, T0188, T0252, T0540, T0550
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0021, K0033, K0044, K0056, K0061, K0068, K0070, K0085, K0089, K0106, K0139, K0161, K0167, K0177, K0179, K0203, K0206, K0210, K0224, K0265, K0287, K0301, K0308, K0331, K0342, K0344, K0345
Skills	S0001, S0009, S0025, S0044, S0051, S0052, S0081, S0120, S0137, S0171
Abilities	A0001, A0044

CAPITOL TECHNOLOGY UNIVERSITY
1927

Tasks

Beginner

T0042 Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, anti-virus, and content blacklists) for specialized cyber defense applications.

T0043 Coordinate with enterprise-wide cyber defense staff to validate network alerts.

T0155 Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.

T0161 Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.

T0163 Perform cyber defense incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation.

T0170 Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.

CAPITOL TECHNOLOGY UNIVERSITY
1927

Tasks

Intermediate

T0020 Develop content for cyber defense tools.

T0023 Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.

T0047 Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.

T0138 Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.

T0142 Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.

T0164 Perform cyber defense trend analysis and reporting.

T0166 original drive) to see the intrusion as the user may have seen it, in a native environment. Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.

CAPITOL TECHNOLOGY UNIVERSITY
1927

Tasks

Advanced

T0010 Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.

T0028 Conduct and/or support authorized penetration testing on enterprise network assets.

T0041 Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.

T0088 Ensure cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.

CAPITOL TECHNOLOGY UNIVERSITY
1927

Integration

Education

Experience

Certifications

Work Force

The critical differentiator for both student and employer is a graduate with 4 years of practical experience defending cyber lab networks in a real time dynamic environment

CAPITOL TECHNOLOGY UNIVERSITY
1927

Way Ahead

- Discovering Information Technology and Operational Technology
- Map each BSCIS core course to KSA's associated with targeted specialties
- Complete categorizing the tasks for the (4) specialties and bin them properly (B,I,E)
- Students will choose a specialty to qualify in
- Develop challenges for students to complete for each task in that specialty
- Map B.S. degree courses to the specialty/tasks
- Map industry certifications to the specialty/tasks
- Pilot test students in "*externships*" performing those tasks from the eSOC

CAPITOL TECHNOLOGY UNIVERSITY
1927

Sponsors

Splunk>

Capitol Alumni Association

Student Senior Projects

- **NSA**
- **Booz Allen & Hamilton**
- **DoD Contractor**

CAPITOL TECHNOLOGY UNIVERSITY

1927

Questions

Educate. Innovate. Inspire.

CAPITOL TECHNOLOGY UNIVERSITY

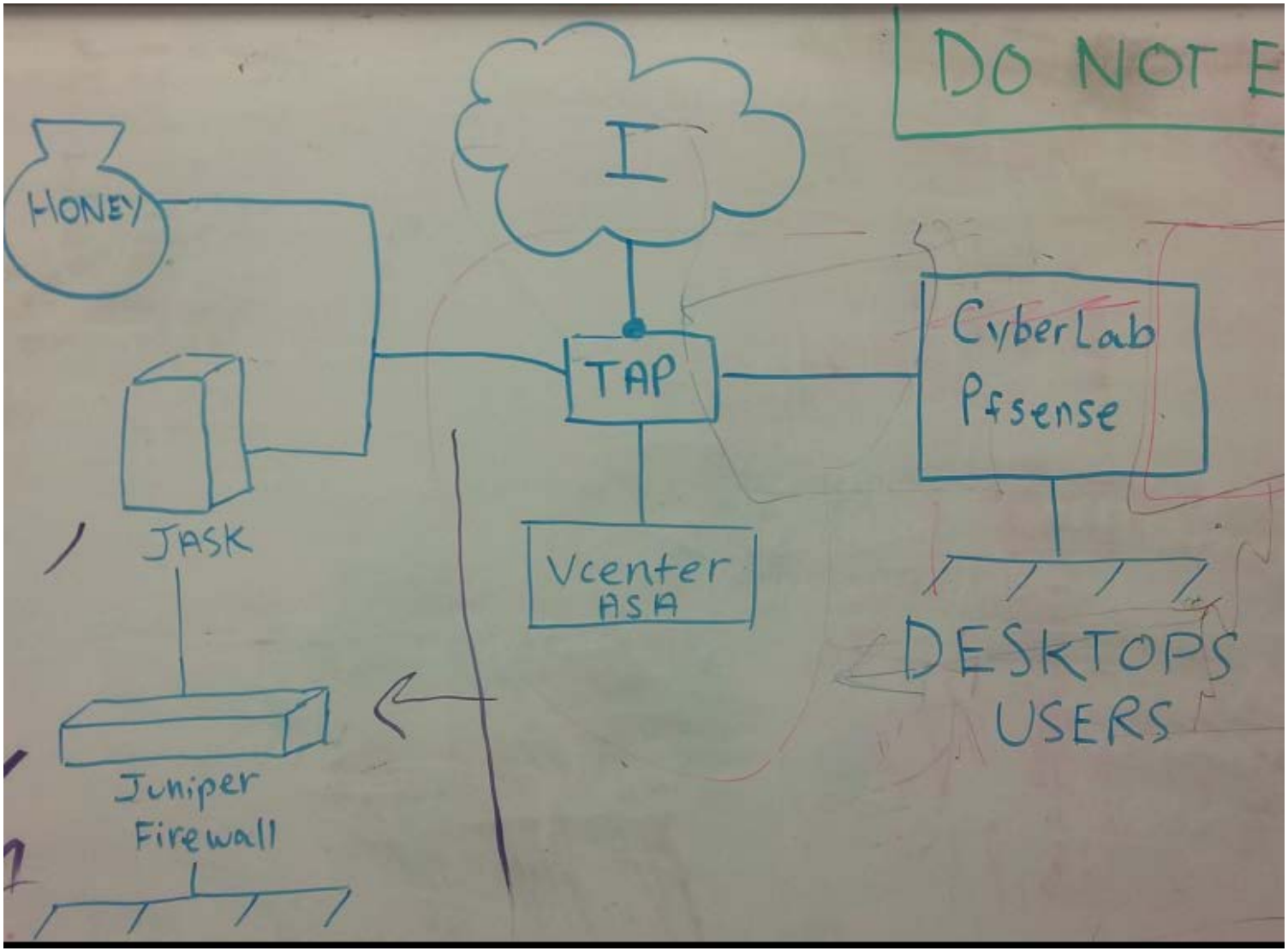
1927

Backup Slides

CAPITOL TECHNOLOGY UNIVERSITY

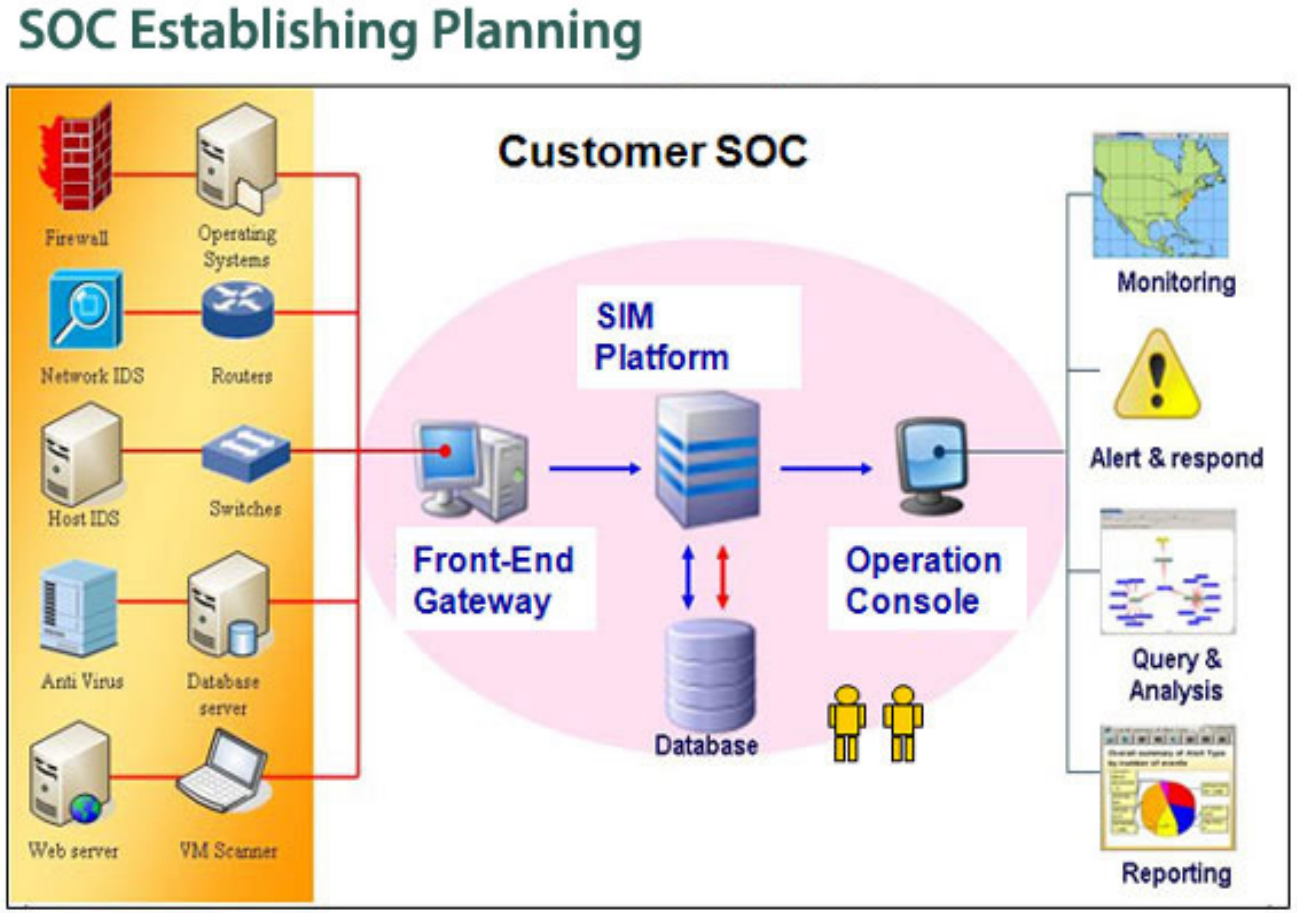
1927

Student SOC Design
Initial Operating Capability (IOC)



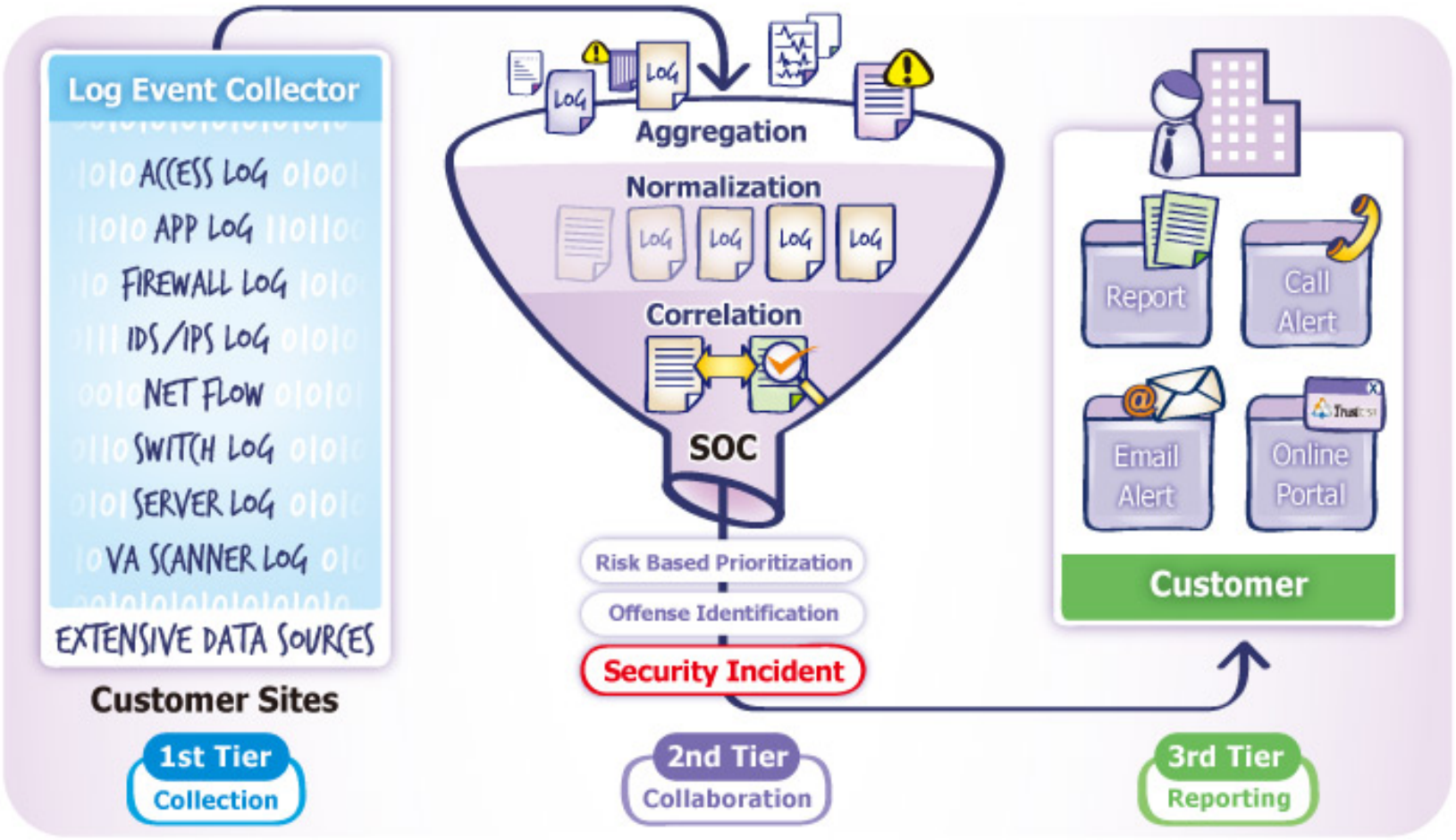
CAPITOL TECHNOLOGY UNIVERSITY
1927

Notional SOC Design



CAPITOL TECHNOLOGY UNIVERSITY
1927

Notional SOC Design



CAPITOL TECHNOLOGY UNIVERSITY
1927

References

- Acer Group (2011). *Security Operation Center (SOC) Planning and Implementation.* Retrieved from: http://www.aceredc.com/edc/english/a_1_main.asp?msid=4&ssid=7
- China Entercom (n.d.). *SOC.* Retrieved from: http://www.china-entercom.com/cn/product-services/security-operations-centers
- CBL Point of Contact: Xavier Allen
- Electric Power Research Institute (2013). *Guidelines for Planning an Integrated Security Operations Center.* Retrieved from http://www.metering.com/wp-content/uploads/2014/02/EPRI-Planning-ISOC-report.pdf
- McAfee. Part of Intel Security (2013). *Creating and Maintaining a SOC: The details behind successful security operations centers.* Retrieved from http://www.mcafee.com/us/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf
- RSA, The Security Division of EMC (2014, June). *Building An Intelligence-Driven Security Operations Center*. Retrieved from https://www.emc.com/collateral/technical-documentation/h11533-intelligence-driven-security-ops-center.pdf
- Torres, A. (2015, May). *Building a World-Class Security Operations Center: A Roadmap*. Retrieved from https://www.sans.org/readingroom/whitepapers/analyst/buildingworld-class-security-operations-center-roadmap-35907
- Whitman, M., Mattord, H., & Green, A (2014). *Principles of Incident Response & Disaster Recovery* (2nd ed.). Boston, MA: Course Technology, Cengage Learning.