VIRGINIA TECH™

Deloitte Cybersecurity Review Recommendations

RANDY MARCHANY
VIRGINIA TECH IT SECURITY OFFICE & LAB

PRIMARY AREAS OF OPPORTUNITY BY PRIORITY

Detailed below are the top 6 recommendations to improve Virginia Tech's cybersecurity program and overall security posture. Specific details for each recommendation are outlined in subsequent slides.

1 Enforce the CIS IG2 Minimum for Systems Processing Sensitive Data

Elevate security leveraging organizational standards already in place throughout the University.

Current Risk: There is opportunity for threat actors to breach VT assets/data due to weak and inconsistent security configurations
Impact: Heightened security baselines position VT to be proactive in security while enabling faster detection and recovery

2 Managed 24x7 Security Operations Center (SOC)

Increase coverage and decrease incident response time across crucial systems.

Current Risk: Incidents that occur outside of VT business hours may not be actioned fast enough, leading to further damage to VT assets
Impact: 24x7 coverage allows VT to protect, detect, and respond to threats at all times

3 Implement modern Identity & Access Management (IAM) solution and refine IAM governance model

Establishes automated lifecycle and access governance capabilities across University systems.

Current Risk: Proliferation of ad-hoc (not standardized) IAM implementations is magnifying security risks.
Impact: Implementing an IAM solution and integrating it with the University systems can enforce policy/standards-based access control.

4 Deploy an Endpoint Data Loss Prevention (DLP) Solution

Stop data exfiltration and breach attempts before data leaves the network.

Current Risk: There are minimal controls on how sensitive VT data (intellectual property, etc.) moves out of devices and across the internet
Impact: DLP can stop unauthorized movement of protected/high-risk data, and report on attempts as well as successful transfers to a 24/7 SOC

5 Full Deployment of Endpoint, Detect, and Respond (EDR) Solution

Increase visibility and control over the most crucial borders of the University's landscape: the endpoint.

Current Risk: Individual systems are not protected well enough, allowing threat actors to compromise them and traverse through VT
Impact: EDR deployment is a strong proactive approach to preventing systems from being successfully compromised along with its data

6 Develop Procedure Guides to Augment the Minimum Security Standards

Create consistency and document practices to empower the University to secure the infrastructure.

Current Risk: Consistency and correctness of security implementation is weak outside of Central IT, leading to weakened security posture
Impact: Procedure guides can aid in consistent and effective implementation of compliance standards and alleviate time to implement

Pipeline Phase	Project Name	Category	Percent Complete	Health Status	Start Date	End Date
Active	24x7 Security Operations Center (6.2)	Cybersecurity	26-50%	On Track	4/1/2022	12/31/2023
	Improved Endpoint Protection (6.4/6.5)	Cybersecurity	1-25%	On Track	5/12/2022	4/30/2024
	Improved Identity and Access Management (6.3)	Cybersecurity	1-25%	On Track	9/16/2022	12/31/2025
	IT Governance (1.2)	IT Governance	76-100%	At Risk	2/21/2022	11/30/2022
	Job Architecture (3.2)	IT Talent	76-100%	On Track	2/1/2022	6/30/2023
	New Minimum Security Standard Guides (6.6)	Cybersecurity	51-75%	On Track	6/10/2022	12/31/2022
	Scaled Up Program and Project Management (1.3)	IT Governance	76-100%	On Track	3/10/2022	11/30/2022
	Strengthen Controls (6.1)	Cybersecurity	1-25%	On Track	10/1/2021	6/30/2025

VIRGINIA TECH™

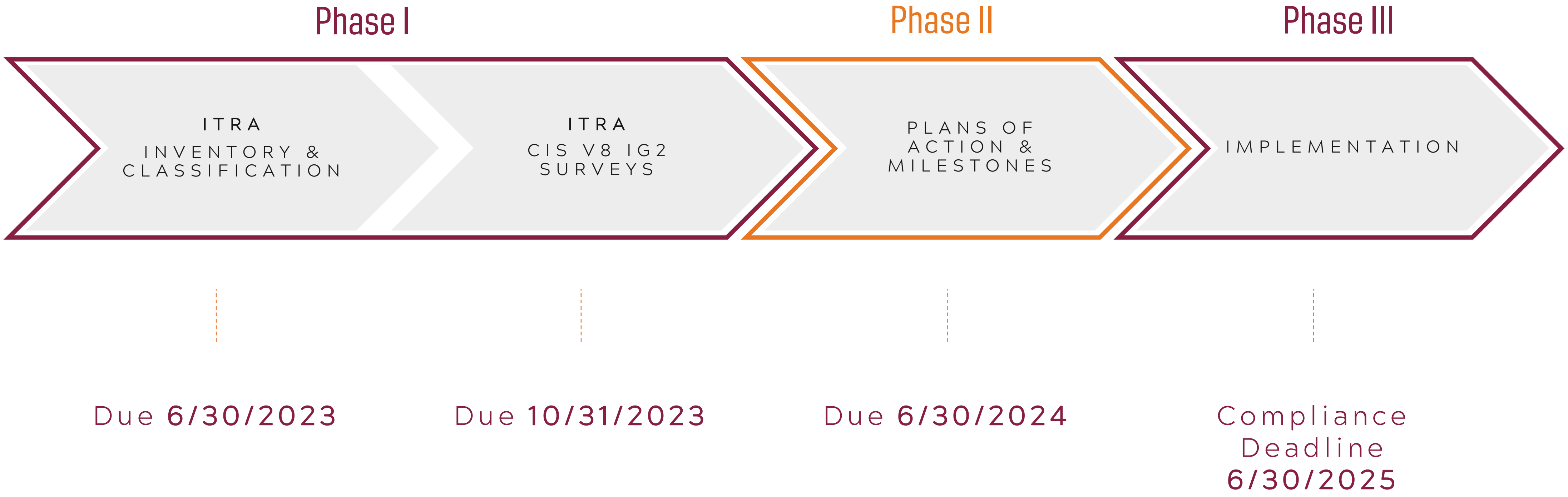
Recommendation 6.1
Ryan Orren, ITSO

Elevate VT to CIS v8 IG2

Goal:

Compliance with the Center for Internet Security (CIS) Critical Security Controls version 8, Implementation Group 2 (IG2) safeguards for units, systems, and applications that handle, process, or store sensitive (“high” and “moderate” risk) data across Virginia Tech.

Elevate VT to CIS v8 IG2



Phase I

ITRA

INVENTORY & CLASSIFICATION

Due 6/30/2023

ITRA

CIS V8 IG2 SURVEYS

Due 10/31/2023

Phase II

PLANS OF ACTION & MILESTONES

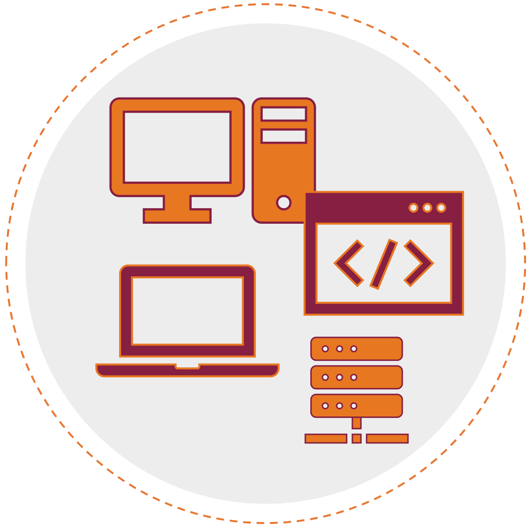
Due 6/30/2024

Phase III

IMPLEMENTATION

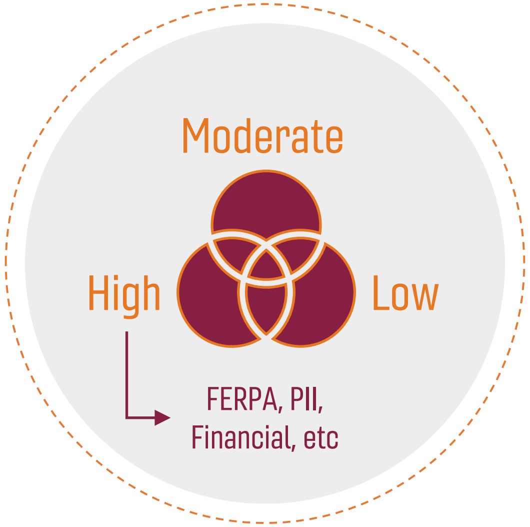
Compliance Deadline 6/30/2025

Phase I - IT Risk Assessments



Asset Inventory

Inventory of unit's hosts and "in-house" developed applications



Risk Classification

Determine data handled by assets and classify risk level accordingly

Assessment Survey

Complete questionnaire(s) based on CIS v8 IG2 controls

Due 6/30/2023

Due 10/31/2023

Phase II

Plans of Action and Milestones (PoA&M)

- Document control gaps, compliance options, plans of action, milestones and target dates
- IG2 compliance required for “High” & “Moderate” risk systems/applications/processes
- Plans should account for resource constraints, business process adjustments, etc.
- Exact format TBD
- Document instances where exceptions may be required (exception process TBD)

Due
6/30/2024

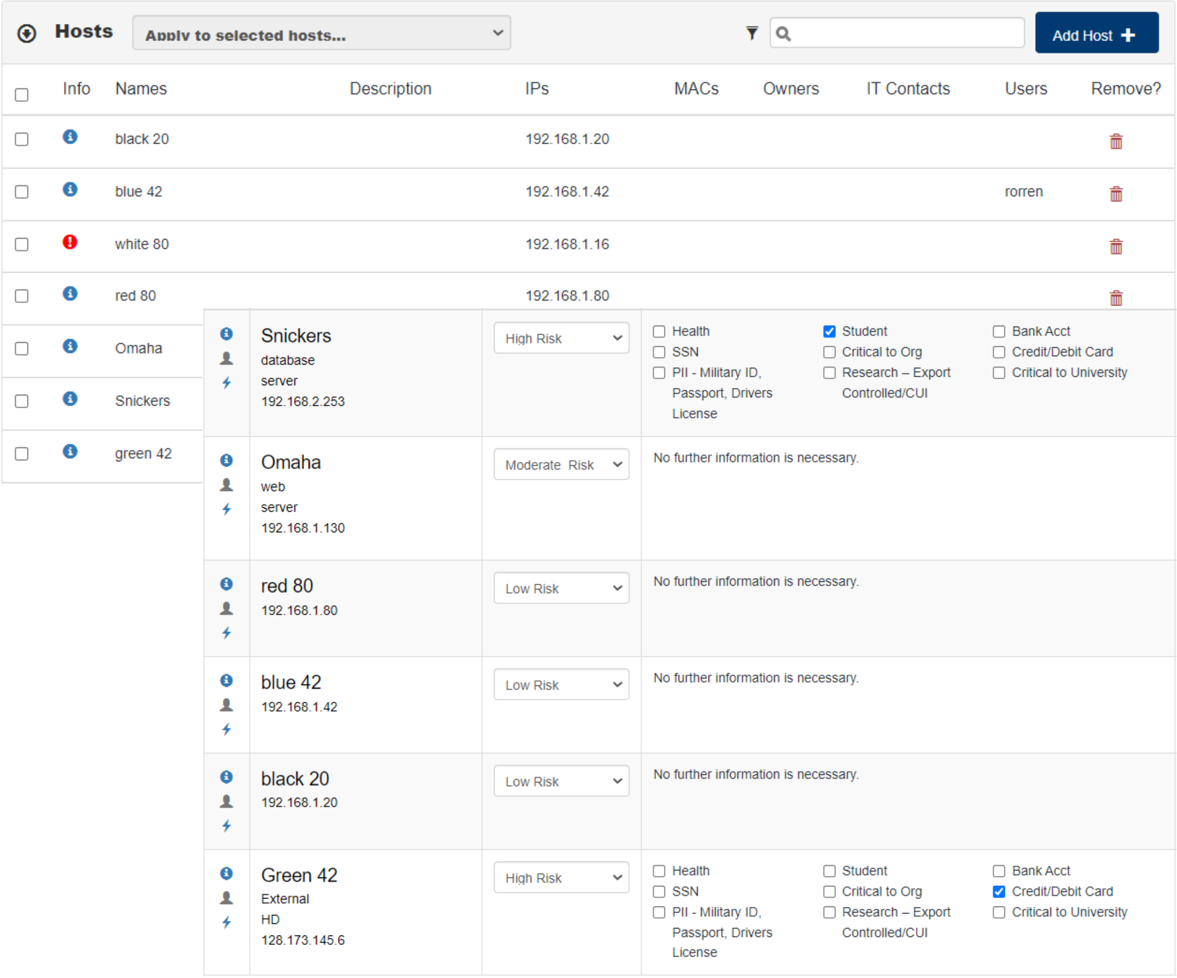
Phase III

Implementation

- Implement or adjust controls/safeguards as documented in PoA&M
- Request formal exception(s) if necessary for unit’s business requirements

Compliance Deadline
6/30/2025

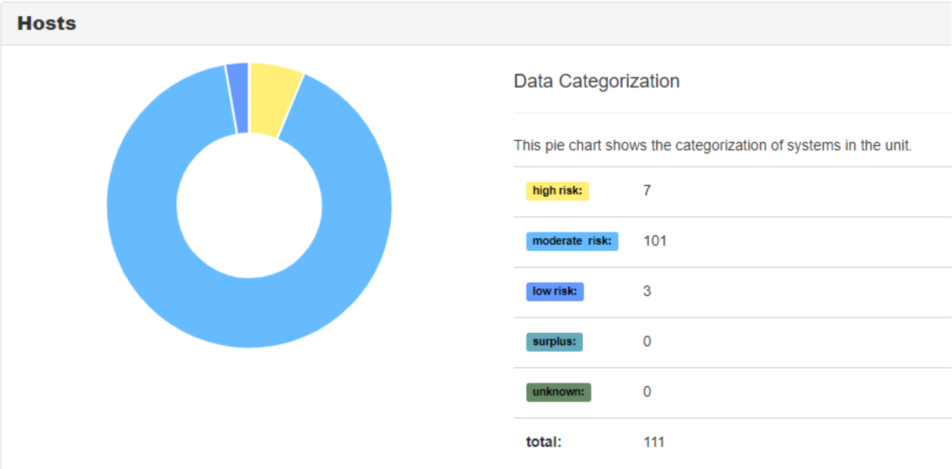
Isora GRC



⊕ **Hosts** Apply to selected hosts... 🔍 Add Host +

☐	Info	Names	Description	IPs	MACs	Owners	IT Contacts	Users	Remove?
☐	ℹ	black 20		192.168.1.20					🗑
☐	ℹ	blue 42		192.168.1.42				rorren	🗑
☐	!	white 80		192.168.1.16					🗑
☐	ℹ	red 80		192.168.1.80					🗑
☐	ℹ	Omaha							
☐	ℹ	Snickers							
☐	ℹ	green 42							

Snickers database server 192.168.2.253	High Risk	☐ Health ☐ SSN ☐ PII - Military ID, Passport, Drivers License	☑ Student ☐ Critical to Org ☐ Research – Export Controlled/CUI ☐ Bank Acct ☐ Credit/Debit Card ☐ Critical to University
Omaha web server 192.168.1.130	Moderate Risk	No further information is necessary.	
red 80 192.168.1.80	Low Risk	No further information is necessary.	
blue 42 192.168.1.42	Low Risk	No further information is necessary.	
black 20 192.168.1.20	Low Risk	No further information is necessary.	
Green 42 External HD 128.173.145.6	High Risk	☐ Health ☐ SSN ☐ PII - Military ID, Passport, Drivers License	☐ Student ☐ Critical to Org ☐ Research – Export Controlled/CUI ☐ Bank Acct ☑ Credit/Debit Card ☐ Critical to University

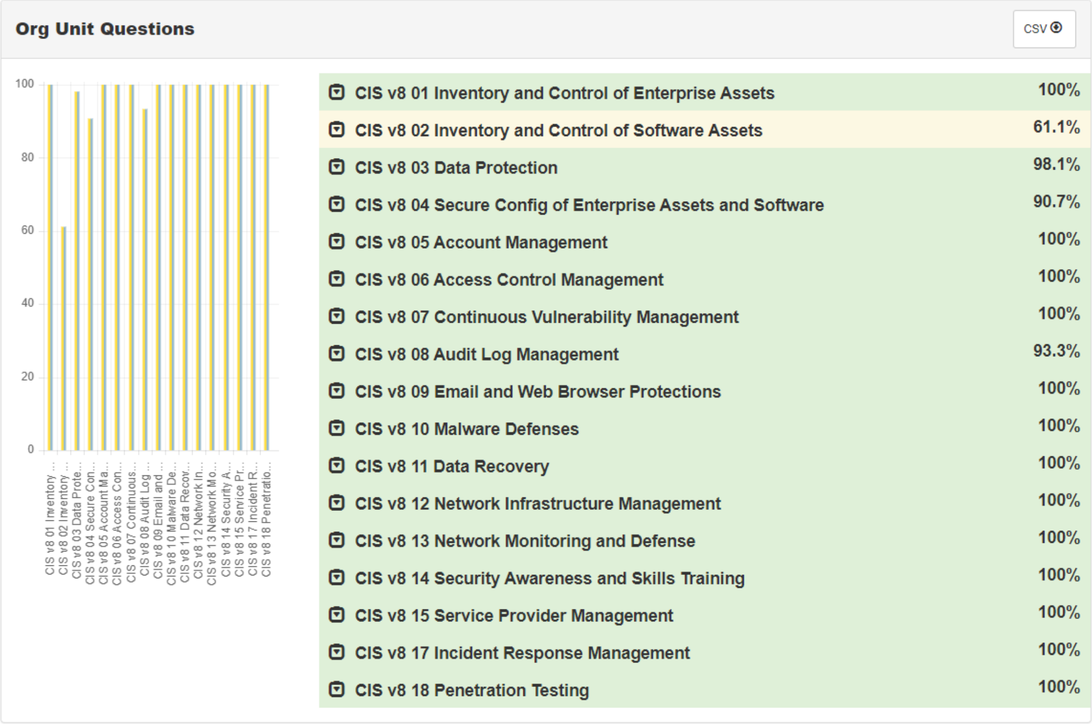


Hosts

Data Categorization

This pie chart shows the categorization of systems in the unit.

high risk:	7
moderate risk:	101
low risk:	3
surplus:	0
unknown:	0
total:	111

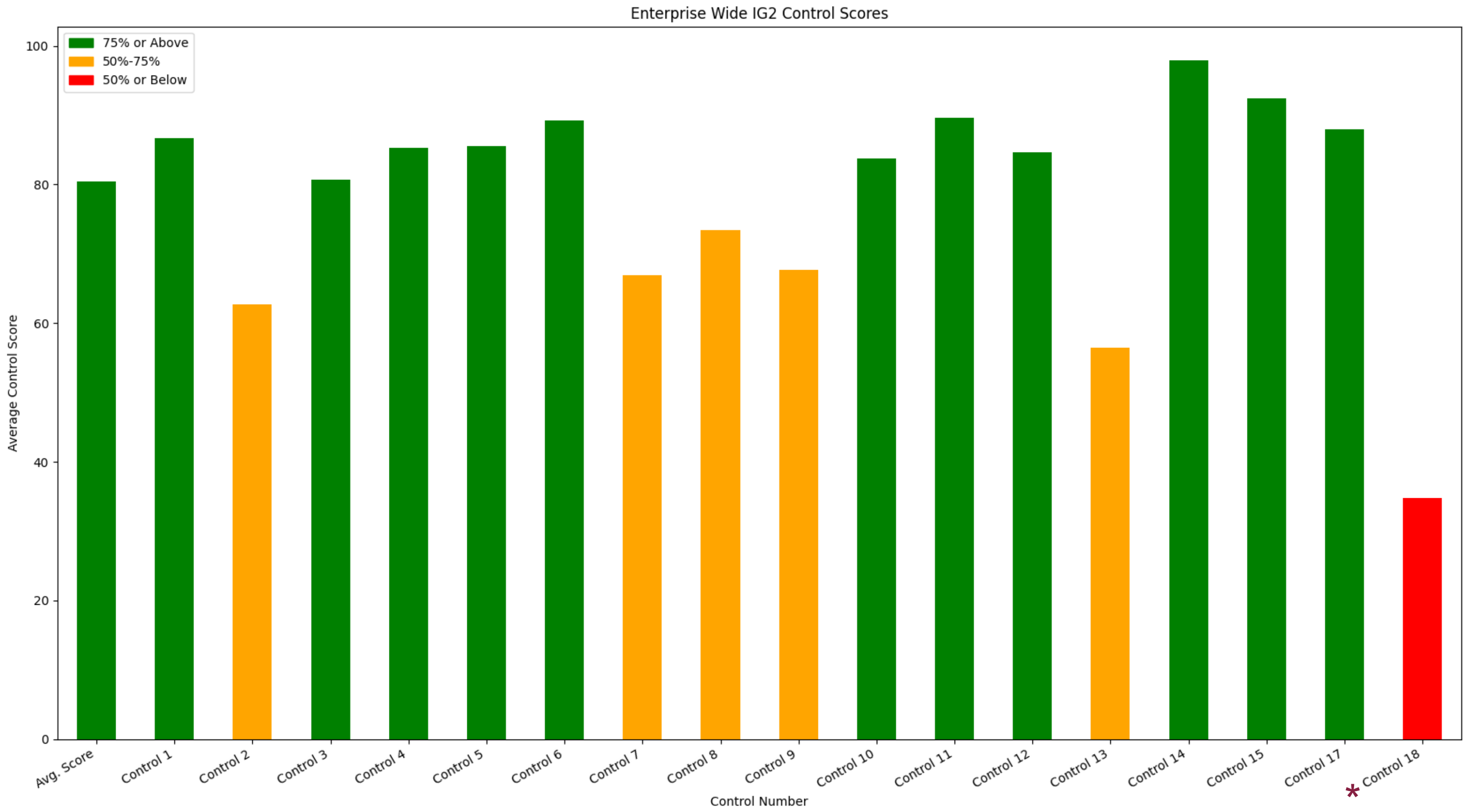


Org Unit Questions

CIS v8 01 Inventory and Control of Enterprise Assets	100%
CIS v8 02 Inventory and Control of Software Assets	61.1%
CIS v8 03 Data Protection	98.1%
CIS v8 04 Secure Config of Enterprise Assets and Software	90.7%
CIS v8 05 Account Management	100%
CIS v8 06 Access Control Management	100%
CIS v8 07 Continuous Vulnerability Management	100%
CIS v8 08 Audit Log Management	93.3%
CIS v8 09 Email and Web Browser Protections	100%
CIS v8 10 Malware Defenses	100%
CIS v8 11 Data Recovery	100%
CIS v8 12 Network Infrastructure Management	100%
CIS v8 13 Network Monitoring and Defense	100%
CIS v8 14 Security Awareness and Skills Training	100%
CIS v8 15 Service Provider Management	100%
CIS v8 17 Incident Response Management	100%
CIS v8 18 Penetration Testing	100%

Current Isora GRC stats

Org Units enrolled: **120**
Total hosts inventoried: **~19,650**
Total “in-house” apps inventoried: **193**



Resources & Contact

IT Risk Assessment page on ITSO site (w/ link to Isora GRC Assessment Guide)
https://security.vt.edu/policies/itra

Ryan Orren, Sr. IT Compliance Manager – rorren@vt.edu
Luke Watson, IT Risk & Compliance Analyst – wluke6@vt.edu

riskassessments@vt.edu
itso-g@vt.edu

Schedule your unit's ITRA Orientation or a follow-up Q&A session:
https://calendar.app.google/hejeSwtJg9JZ1XmP8

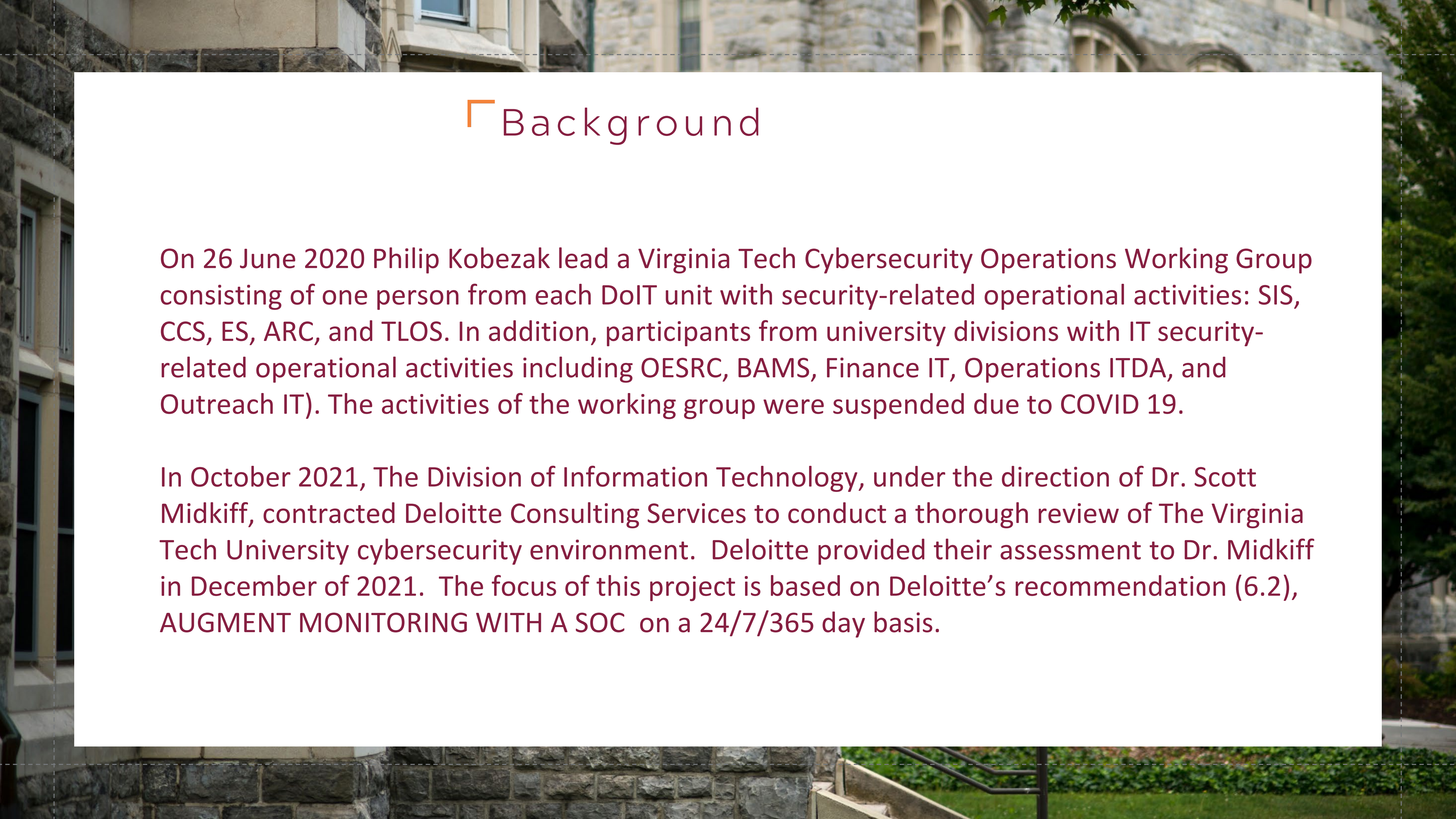
VIRGINIA TECH™

Recommendation 6.2
Zach Mitcham, ITSO

Deloitte Recommendation 6.2

AUGMENT MONITORING WITH A SOC

“Expanding the current capability of the IT Security Office and Enterprise Services from the current 8 hours a day, 5 days per week model of reaction to 24/7 would not only increase coverage for incidents but would also enable more proactive approaches to protecting the University against threats and brings the IT Security Office closer to real-time cyber defense.“



Background

On 26 June 2020 Philip Kobezak lead a Virginia Tech Cybersecurity Operations Working Group consisting of one person from each DoIT unit with security-related operational activities: SIS, CCS, ES, ARC, and TLOS. In addition, participants from university divisions with IT security-related operational activities including OESRC, BAMS, Finance IT, Operations ITDA, and Outreach IT). The activities of the working group were suspended due to COVID 19.

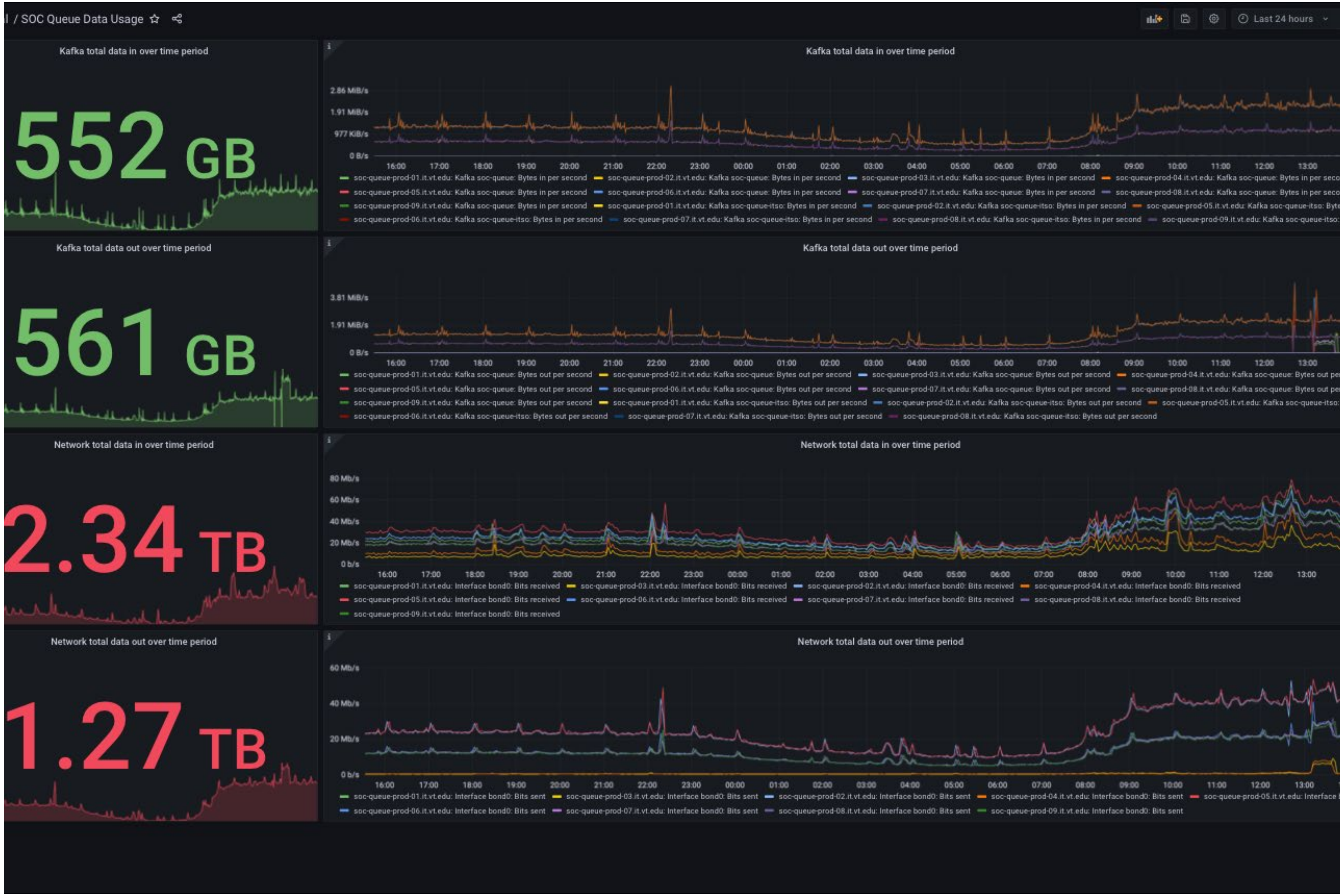
In October 2021, The Division of Information Technology, under the direction of Dr. Scott Midkiff, contracted Deloitte Consulting Services to conduct a thorough review of The Virginia Tech University cybersecurity environment. Deloitte provided their assessment to Dr. Midkiff in December of 2021. The focus of this project is based on Deloitte's recommendation (6.2), AUGMENT MONITORING WITH A SOC on a 24/7/365 day basis.

Vendor of Choice

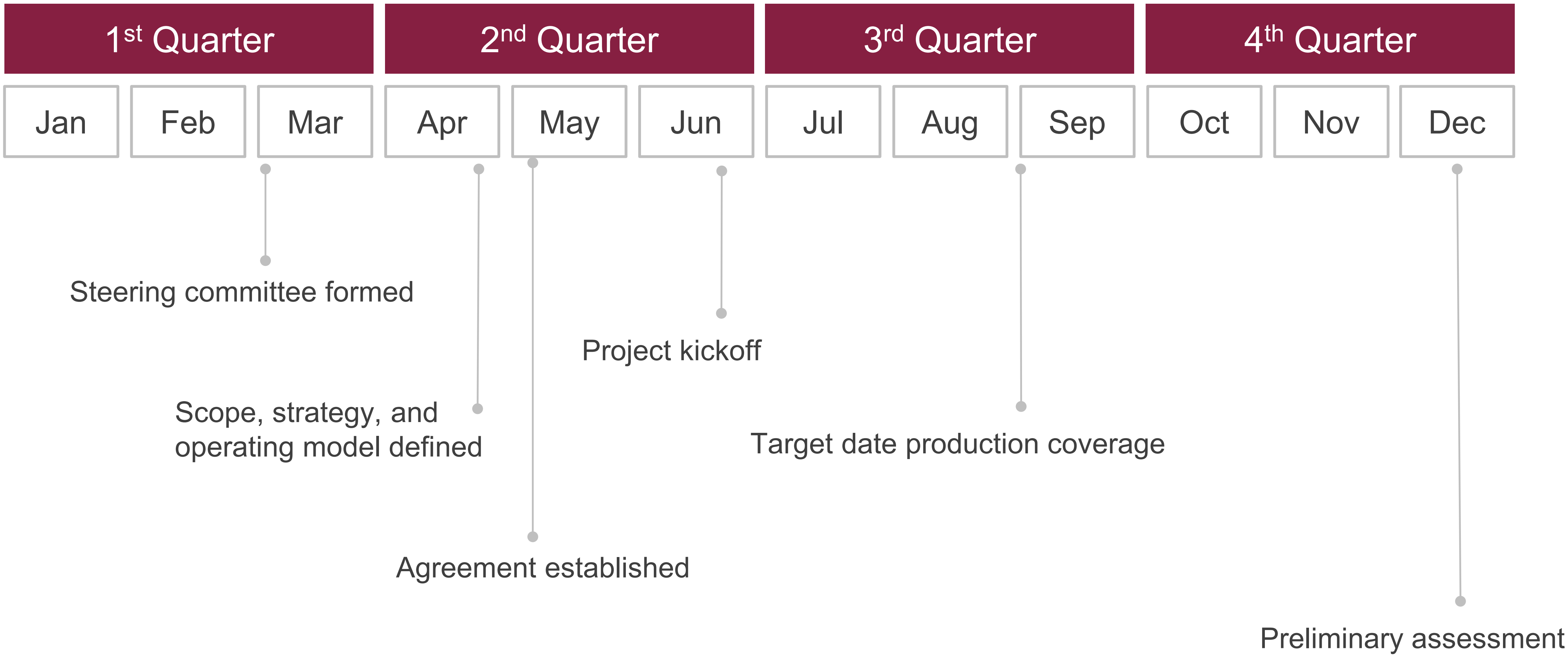
OmniSOC

OmniSOC is a 24×7×365 shared cybersecurity operations center (SOC) that is sector-specific for higher education and research. OmniSOC collects cybersecurity data from partners; integrates this data with other threat intelligence; conducts proactive threat hunting; and monitors, triages, and analyzes security events.

Daily Data Flow Snap Shot


l / SOC Queue Data Usage
Last 24 hours
Kafka total data in over time period
552 GB
Kafka total data in over time period
2.86 MiB/s
1.91 MiB/s
977 KiB/s
0 B/s
16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00
soc-queue-prod-01.it.vt.edu: Kafka soc-queue: Bytes in per second
soc-queue-prod-02.it.vt.edu: Kafka soc-queue: Bytes in per second
soc-queue-prod-03.it.vt.edu: Kafka soc-queue: Bytes in per second
soc-queue-prod-04.it.vt.edu: Kafka soc-queue: Bytes in per seco
soc-queue-prod-05.it.vt.edu: Kafka soc-queue: Bytes in per second
soc-queue-prod-06.it.vt.edu: Kafka soc-queue: Bytes in per second
soc-queue-prod-07.it.vt.edu: Kafka soc-queue: Bytes in per second
soc-queue-prod-08.it.vt.edu: Kafka soc-queue: Bytes in per seco
soc-queue-prod-09.it.vt.edu: Kafka soc-queue: Bytes in per second
soc-queue-prod-01.it.vt.edu: Kafka soc-queue-itso: Bytes in per second
soc-queue-prod-02.it.vt.edu: Kafka soc-queue-itso: Bytes in per second
soc-queue-prod-05.it.vt.edu: Kafka soc-queue-itso: Byte
soc-queue-prod-06.it.vt.edu: Kafka soc-queue-itso: Bytes in per second
soc-queue-prod-07.it.vt.edu: Kafka soc-queue-itso: Bytes in per second
soc-queue-prod-08.it.vt.edu: Kafka soc-queue-itso: Bytes in per second
soc-queue-prod-09.it.vt.edu: Kafka soc-queue-itso:
Kafka total data out over time period
561 GB
Kafka total data out over time period
3.81 MiB/s
1.91 MiB/s
0 B/s
16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00
soc-queue-prod-01.it.vt.edu: Kafka soc-queue: Bytes out per second
soc-queue-prod-02.it.vt.edu: Kafka soc-queue: Bytes out per second
soc-queue-prod-03.it.vt.edu: Kafka soc-queue: Bytes out per second
soc-queue-prod-04.it.vt.edu: Kafka soc-queue: Bytes out pe
soc-queue-prod-05.it.vt.edu: Kafka soc-queue: Bytes out per second
soc-queue-prod-06.it.vt.edu: Kafka soc-queue: Bytes out per second
soc-queue-prod-07.it.vt.edu: Kafka soc-queue: Bytes out per second
soc-queue-prod-08.it.vt.edu: Kafka soc-queue: Bytes out pe
soc-queue-prod-09.it.vt.edu: Kafka soc-queue: Bytes out per second
soc-queue-prod-01.it.vt.edu: Kafka soc-queue-itso: Bytes out per second
soc-queue-prod-02.it.vt.edu: Kafka soc-queue-itso: Bytes out per second
soc-queue-prod-05.it.vt.edu: Kafka soc-queue-itso:
soc-queue-prod-06.it.vt.edu: Kafka soc-queue-itso: Bytes out per second
soc-queue-prod-07.it.vt.edu: Kafka soc-queue-itso: Bytes out per second
soc-queue-prod-08.it.vt.edu: Kafka soc-queue-itso: Bytes out per second
Network total data in over time period
2.34 TB
Network total data in over time period
80 Mb/s
60 Mb/s
40 Mb/s
20 Mb/s
0 b/s
16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00
soc-queue-prod-01.it.vt.edu: Interface bond0: Bits received
soc-queue-prod-03.it.vt.edu: Interface bond0: Bits received
soc-queue-prod-02.it.vt.edu: Interface bond0: Bits received
soc-queue-prod-04.it.vt.edu: Interface bond0: Bits received
soc-queue-prod-05.it.vt.edu: Interface bond0: Bits received
soc-queue-prod-06.it.vt.edu: Interface bond0: Bits received
soc-queue-prod-07.it.vt.edu: Interface bond0: Bits received
soc-queue-prod-08.it.vt.edu: Interface bond0: Bits received
soc-queue-prod-09.it.vt.edu: Interface bond0: Bits received
Network total data out over time period
1.27 TB
Network total data out over time period
60 Mb/s
40 Mb/s
20 Mb/s
0 b/s
16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00
soc-queue-prod-01.it.vt.edu: Interface bond0: Bits sent
soc-queue-prod-03.it.vt.edu: Interface bond0: Bits sent
soc-queue-prod-02.it.vt.edu: Interface bond0: Bits sent
soc-queue-prod-04.it.vt.edu: Interface bond0: Bits sent
soc-queue-prod-05.it.vt.edu: Interface
soc-queue-prod-06.it.vt.edu: Interface bond0: Bits sent
soc-queue-prod-07.it.vt.edu: Interface bond0: Bits sent
soc-queue-prod-08.it.vt.edu: Interface bond0: Bits sent
soc-queue-prod-09.it.vt.edu: Interface bond0: Bits sent

24x7 SOC Timeline FY 2022



1st Quarter			2nd Quarter			3rd Quarter			4th Quarter		
Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec

Steering committee formed

Project kickoff

Scope, strategy, and
operating model defined

Target date production coverage

Agreement established

Preliminary assessment

* Estimated Go Live Mid December

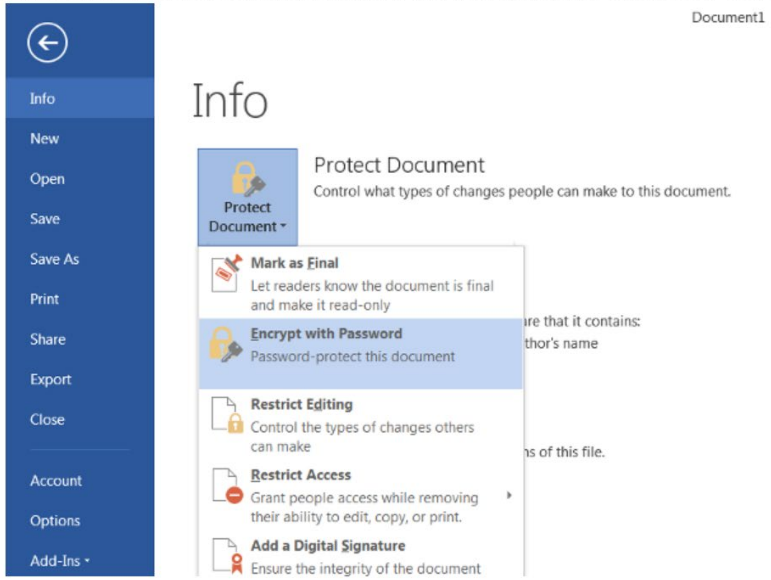
VIRGINIA TECH™

Recommendation 6.6

Develop Procedure Guides to Augment MinSec

- Drafts at https://code.vt.edu/rtilley/itso-procedures
- Current Minimum Security Standard v3.7
- 38 mid level steps
- 35 procedure guides completed and currently being verified
- Target Completion Date: 12/31/2022

2. Click the icon to Protect Document (or Worksheet / Presentation) and select "Encrypt with Password" from the dropdown menu.


Document1
Info
New
Open
Save
Save As
Print
Share
Export
Close
Account
Options
Add-Ins
Info
Protect Document
Protect Document
Control what types of changes people can make to this document.
Mark as Final
Let readers know the document is final and make it read-only
Encrypt with Password
Password-protect this document
Restrict Editing
Control the types of changes others can make
Restrict Access
Grant people access while removing their ability to edit, copy, or print.
Add a Digital Signature
Ensure the integrity of the document
re that it contains:
thor's name
s of this file.