Improved Endpoint Protection (IEP), Microsoft Defender for Endpoint (MDE) and You!

DCSS Fall 2023 presentation

V1.0 - 20231106

Marc DeBonis

Director – Collaborative Computing Solutions

http://ccs.vt.edu

Background

IT TRANSFORMATION LOOKING AHEAD

			Activity			
Priority	#	Recommendation	FY22	FY23	FY24	FY25
0	0.0	Establish the IT Transformation program office	X			
1	1.2	Establish a University-wide IT governance model	X	X		
2	3.2	Standardize job classifications for IT staff across VT	X	X	X	
3	1.3	Establish University-wide IT PMO and IT enterprise architecture functions		X	X	
4	6.4	Deploy an endpoint data loss prevention (DLP) solution		X	X	
4	6.5	Full deployment of endpoint detect and respond (EDR) solution		X	X	
5	6.2	Managed 24x7 security operations center (SOC)		X		
6	6.3	Reshape identity through identity and access management (IAM)		X	X	
7	6.1	Enforce the CIS IG2 minimum for systems processing sensitive data	X	X		
8	6.6	Develop procedure guides to augment the minimum security standards		X		
9	4.2	Deploy a common integration layer		X	X	
10	4.1	Enhance data governance		X	X	
11	2.2	Streamline software procurement		X		
12	5.1	Implement university-wide CMDB processes and tools		X	X	
13	3.1	Revise DoIT's organizational model		X	X	
	1.1	Define the University-wide IT operating model		X		
	2.1	Optimize funding model			X	X
	4.3	Rationalize application portfolio		X	X	X
	4.4	Establish data center consolidation strategy/cloud enhancement		X	X	X
	4.5	Define strategy for adopting managed services and SaaS solutions			X	
	5.2	Enhance maturity of core ITSM processes			X	X

Key

- Funded through reallocation or budget not needed
- Budget request submitted for FY 2023
- Budget not yet analyzed or requested

What is EDR

- EDR
  - Endpoint Detection & Response
  - "What happened and what is currently happening on an endpoint?"
  - e.x. - A ransomware dropper installed via a web drive-by

  - We are utilizing the University supported M365 A3->A5 license "bump" to utilize MDE for the EDR solution

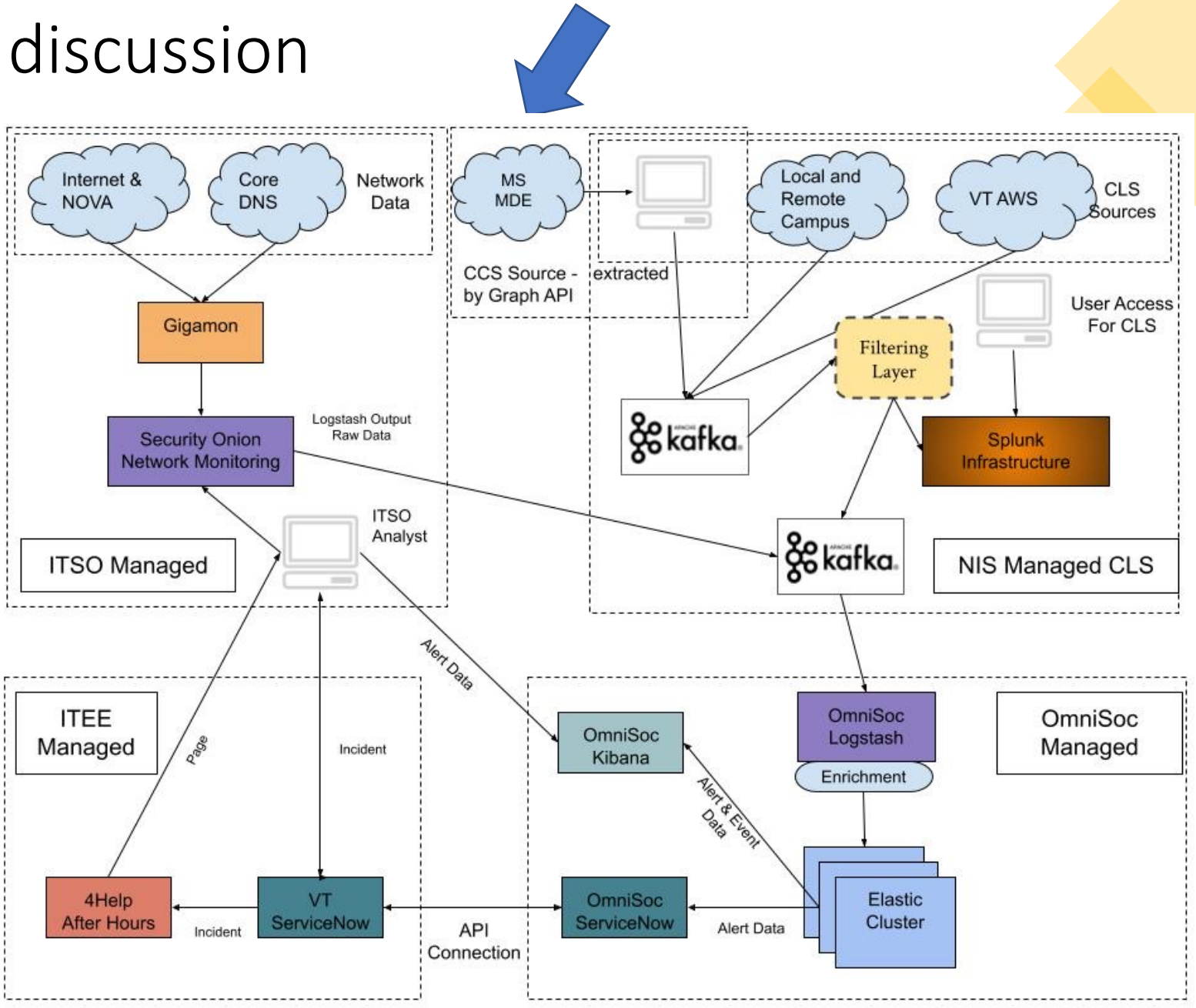
  - In scope, all University owned endpoints (laptops, desktops)
    - Includes Windows, MacOS, Linux OSes
    - Does not include server OSes
    - Does not include mobile devices

Status

- Charter signed (September 2022)
- Steering Committee formed (October 2022)
- CCS position hired (February 2023)
- Microsoft Defender for Endpoint (MDE) in operational mode
- Deployment numbers are good, but we're aiming for GREAT!

MDE and ITSO access discussion

- ITSO graphic regarding event ingestion
- Discussion of MDE data sending to SOC
- Status of providing ITSO access to M365\MDE security roles



Showing ROI (Return on Investment)

- As of 10/6/2023 12,152 endpoints (was 7,604) endpoints running MDE, 36 departments (was 29) departments enrolled in service
  - This represents 56% of endpoints registered in ISORA (back in May 2023)
- From 12/14/2022 to 11/9/2023, the service detected and mitigated:

•High Alerts
  - •3 high-severity malware attacks prevented
  - •4 instances of multiple threat families blocked
  - •5 ransomware-linked emerging threats prevented

•Medium Alerts
  - •2 instances of multiple threat families blocked
  - •2 instances of connection to C2 blocked
  - •12 instances of exploit/execution on one or multiple endpoints prevented
  - •9 instances of PowerShell executed by suspicious process prevented
  - •8 instances of general exploits, defense evasion, and persistence blocked

•Low Alerts
  - 7 instances of hosts file hijacking prevented
  - 7 instances of multiple threat families blocked
  - 54 active malware/general exploit executions prevented
  - 1 instance of ransomware prevented
  - 12 remote-shell backdoor exploits prevented
  - 23 trojans blocked
  - 3 keyloggers prevented
  - 38 hacktools prevented
  - 67 potentially unwanted apps (PUAs) blocked

•Informative
  - 685 PUAs blocked
  - 771 active malware/exploit attempts blocked
  - 45 malware detected in gz, iso, or pst files and blocked
  - 5 suspicious connections blocked by network protection
  - 4 instances of multiple threat families blocked

MDE is here to assist you!

- Identify, mitigate and eliminate the impact of attacks against your user's endpoints
- Installation and setup is much easier and less time consuming than dealing with the aftermath of a ransomware attack!

11/2/2023 11:55:34 AM	'Nemucod' malware was prevented	TrojanDownloader:JS/Nemucod.SA	Malware	Informational	New
11/1/2023 9:07:00 AM	Mimikatz credential theft tool	HackTool:Win32/Mimikatz!pz	CredentialAccess	High	Resolved
10/31/2023 2:02:08 PM	Download of file associated with digital currency mining		UnwantedSoftware	Medium	New
10/27/2023 3:21:13 PM	An active 'SilentCleanupUACBypass' malware in a command line was prevented from executing	VirTool:Win32/SilentCleanupUACBypass.A	Malware	Low	Resolved

IEP University-level communication

- Initiative dashboard
  - https://evpcoo.vt.edu/Initiatives/ittransformation/dashboard.html
- IT Transformation IEP project
  - https://evpcoo.vt.edu/Initiatives/ittransformation/projects/cybersecurity/improved-endpoint-protection.html
  - This includes the new FAQ
- BOV resolution
  - "RESOLUTION ON INFORMATION TECHNOLOGY MONITORING"
  - https://vtx.vt.edu/articles/2023/03/bov-march-2023-overview.html
- Pending updates to policy 7010 and 7035 to further support IEP

How to get involved

- Contact your Organizational Unit (OU) admin to discuss endpoint management next steps
  - To determine your OU admin
    - Go to http://mycat.ccs.vt.edu and log in with your Hokies account
    - Note your OU Admin(s)
  - Contact them for endpoint UEM setup and EDR sign-up
    - Available UEM solutions include JAMF, Intune, BigFix, GPO, Ansible, etc.
    - They should submit a SN ticket to request signing up for UEM (if not already) and MDE
- Log into Service Now, search for term "MDE"
  - RITM: "Microsoft Defender for Endpoint Service"
  - KB: "Understanding Microsoft's Defender for Endpoint"