CYBERSECURITY ENGINEERING

SESSION 1

TEXAS SKILLS DEVELOPMENT FUND
TRAINING PARTNERSHIP

AUSTIN COMMUNITY COLLEGE DISTRICT

Course Objective

01

Cyber Security Engineering

Systems Approach

02

Risk Analysis

Prioritization & Capabilities

03

Management Models

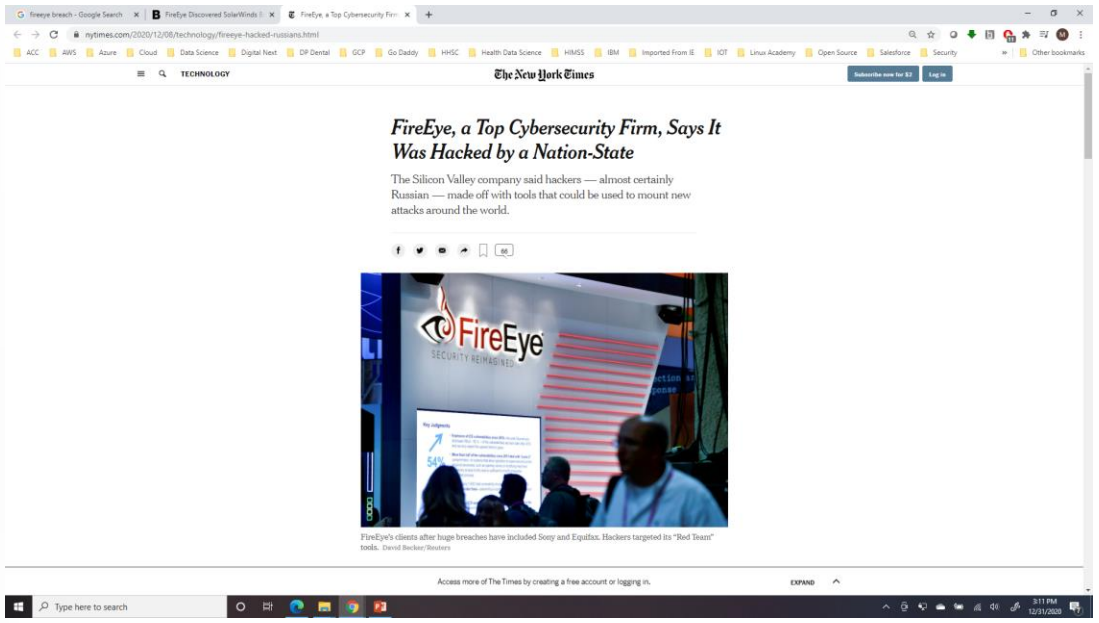
Critical Competencies

04

Cloud Security

Metrics & Best Practices

Let us start with the news …



TECHNOLOGY

The New York Times

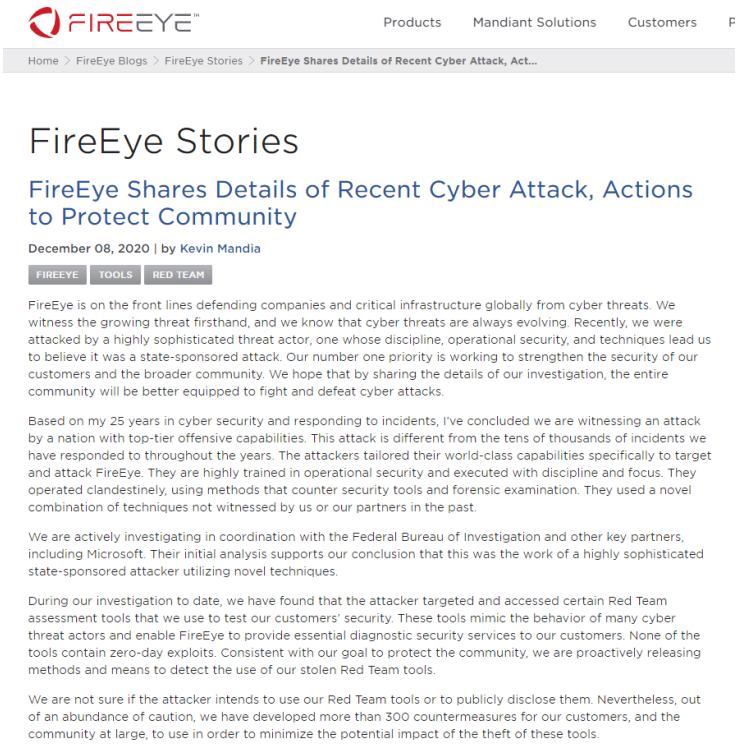
FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State

The Silicon Valley company said hackers — almost certainly Russian — made off with tools that could be used to mount new attacks around the world.

FireEye's clients after huge breaches have included Sony and Equifax. Hackers targeted its "Red Team" tools. David Becker/Reuters

Access more of The Times by creating a free account or logging in.

EXPAND



FIREEYE

Products Mandiant Solutions Customers

Home > FireEye Blogs > FireEye Stories > **FireEye Shares Details of Recent Cyber Attack, Act...**

FireEye Stories

FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community

December 08, 2020 | by Kevin Mandia

FIREEYE TOOLS RED TEAM

FireEye is on the front lines defending companies and critical infrastructure globally from cyber threats. We witness the growing threat firsthand, and we know that cyber threats are always evolving. Recently, we were attacked by a highly sophisticated threat actor, one whose discipline, operational security, and techniques lead us to believe it was a state-sponsored attack. Our number one priority is working to strengthen the security of our customers and the broader community. We hope that by sharing the details of our investigation, the entire community will be better equipped to fight and defeat cyber attacks.

Based on my 25 years in cyber security and responding to incidents, I've concluded we are witnessing an attack by a nation with top-tier offensive capabilities. This attack is different from the tens of thousands of incidents we have responded to throughout the years. The attackers tailored their world-class capabilities specifically to target and attack FireEye. They are highly trained in operational security and executed with discipline and focus. They operated clandestinely, using methods that counter security tools and forensic examination. They used a novel combination of techniques not witnessed by us or our partners in the past.

We are actively investigating in coordination with the Federal Bureau of Investigation and other key partners, including Microsoft. Their initial analysis supports our conclusion that this was the work of a highly sophisticated state-sponsored attacker utilizing novel techniques.

During our investigation to date, we have found that the attacker targeted and accessed certain Red Team assessment tools that we use to test our customers' security. These tools mimic the behavior of many cyber threat actors and enable FireEye to provide essential diagnostic security services to our customers. None of the tools contain zero-day exploits. Consistent with our goal to protect the community, we are proactively releasing methods and means to detect the use of our stolen Red Team tools.

We are not sure if the attacker intends to use our Red Team tools or to publicly disclose them. Nevertheless, out of an abundance of caution, we have developed more than 300 countermeasures for our customers, and the community at large, to use in order to minimize the potential impact of the theft of these tools.

FireEye Discovered SolarWinds Breach While Probing Own Hack

What happened …

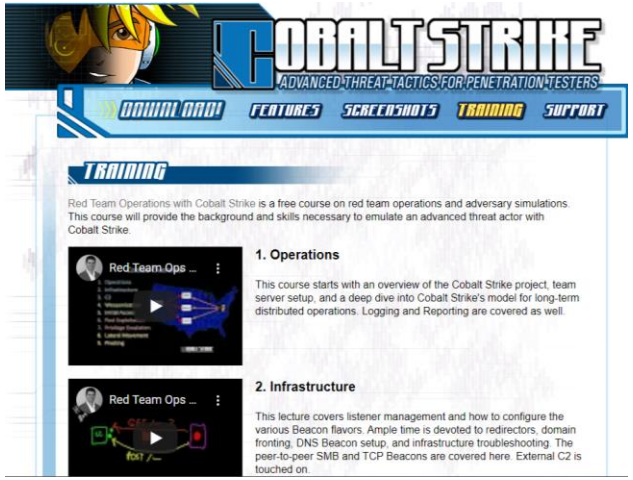
Continuous Updates: Everything You Need to Know About the SolarWinds Attack

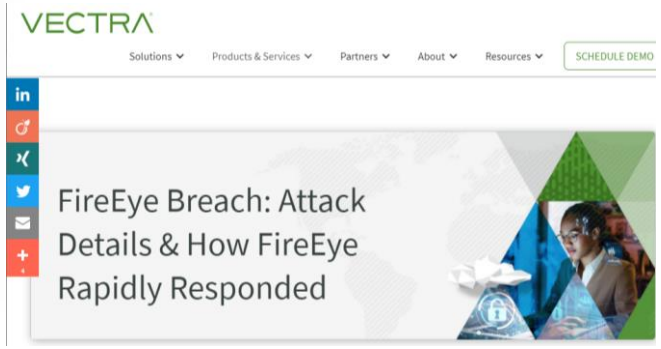
fireeye/**red_team_tool_countermeasures**

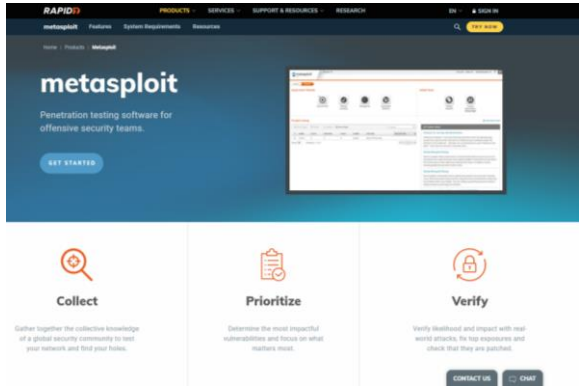
yara ClamAV red_team_tool_countermeasures

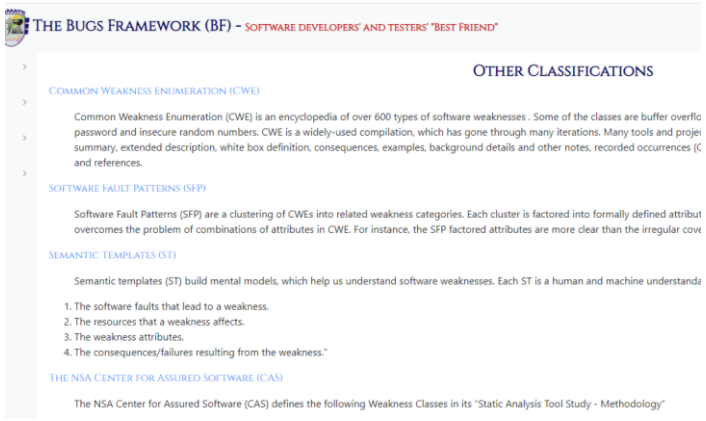
Solorigate/Sunburst : Theft of Cybersecurity Tools | FireEye Breach

National Vulnerability Database









Links …

https://samate.nist.gov/BF/Enlightenment/otherclassifications.html

https://blog.qualys.com/vulnerabilities-research/2020/12/09/theft-of-cybersecurity-tools-fireeye-breach

https://github.com/fireeye/red_team_tool_countermeasures/blob/master/CVEs_red_team_tools.md

https://github.com/fireeye/red_team_tool_countermeasures/blob/master/README.md

https://www.bloomberg.com/news/articles/2020-12-15/fireeye-stumbled-across-solarwinds-breach-while-probing-own-hack

https://www.cobaltstrike.com/training

https://docs.rapid7.com/metasploit/

https://blog.qualys.com/vulnerabilities-research/2020/12/09/theft-of-cybersecurity-tools-fireeye-breach

https://www.securityweek.com/continuous-updates-everything-you-need-know-about-solarwinds-attack

Links …

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9546

https://support.solarwinds.com/SuccessCenter/s/article/CVE-2019-9546-Orion-Platform-Vulnerability?language=en_US

https://www.solarwinds.com/securityadvisory

https://www.deepinstinct.com/2020/12/28/why-the-sunburst-malware-was-so-unique-and-what-weve-learnt-from-it/

https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

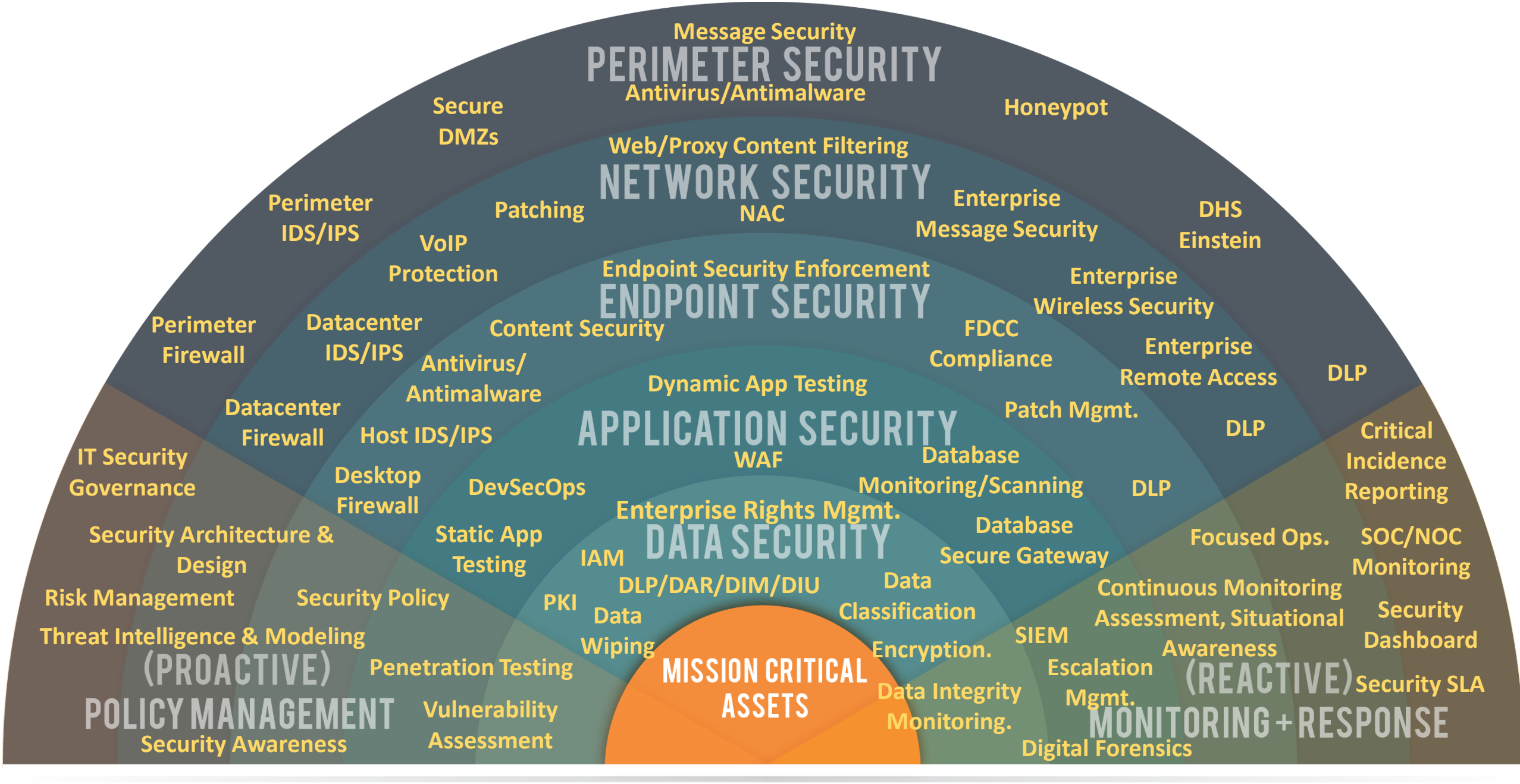
https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/

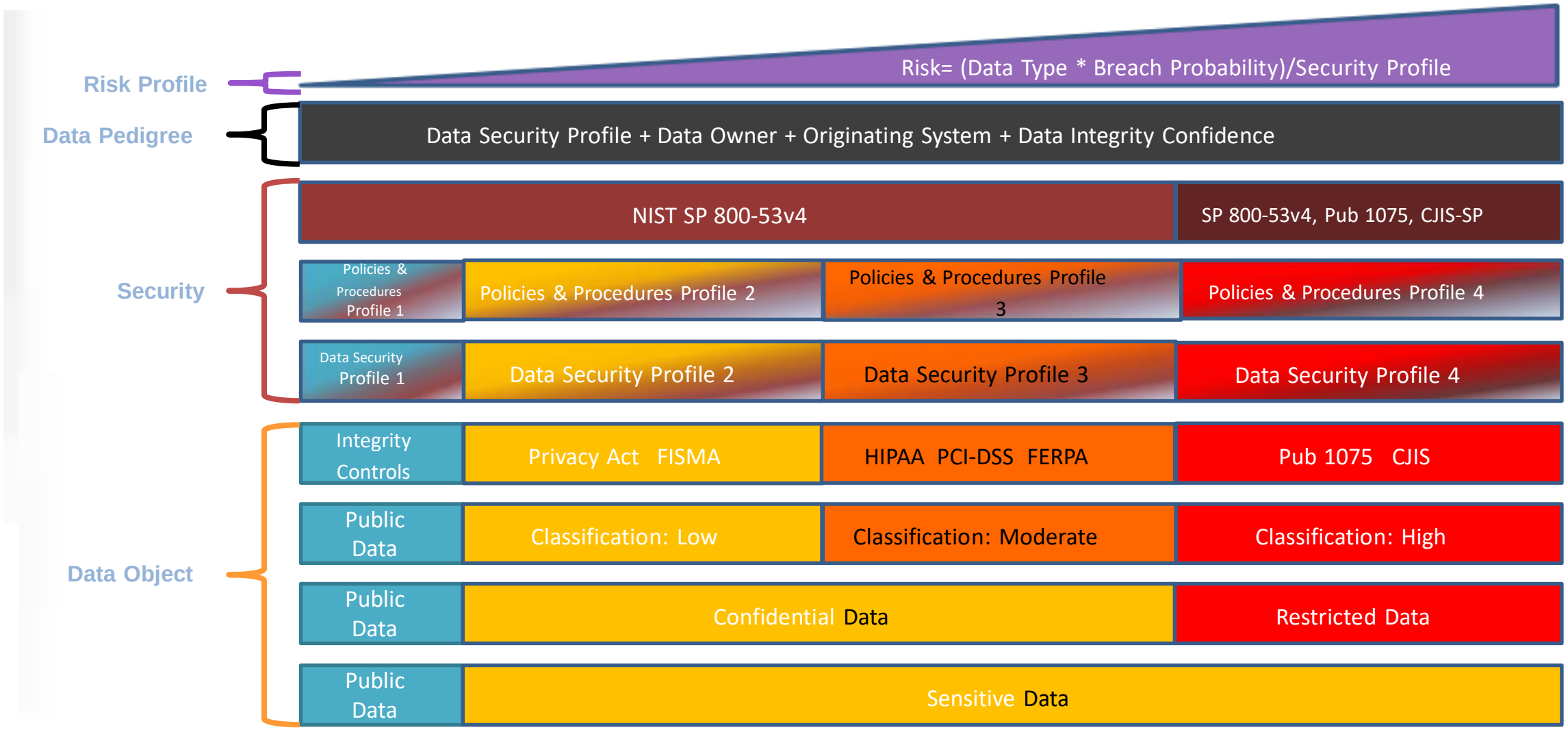
https://www.solarwinds.com/orion-platform#:~:text=The%20SolarWinds%C2%AE%20Orion%C2%AE%20Platform%20is%20a%20powerful%2C%20scalable,a%20single%20pane%20of%20glass.

Cybersecurity Domains

- Foundational Security
  - Essential boundary protection
- Data Protection
  - Data integrity, Data privacy
- Security Operations
  - Business security assessment
  - Management & Response
- Cloud Security
  - Cloud services security
- Application Security
  - Software security gaps/flaws
- Risk & Compliance
  - Enterprise, operational, 3rd party
  - Information Technology
  - Remediation
- Identity Management
  - Authentication, Authorization
  - Identity challenges, Exposure
- IoT/ICS
  - Analytics, Operations, Assets
  - Communication Protocols
  - Remote monitoring, Detection

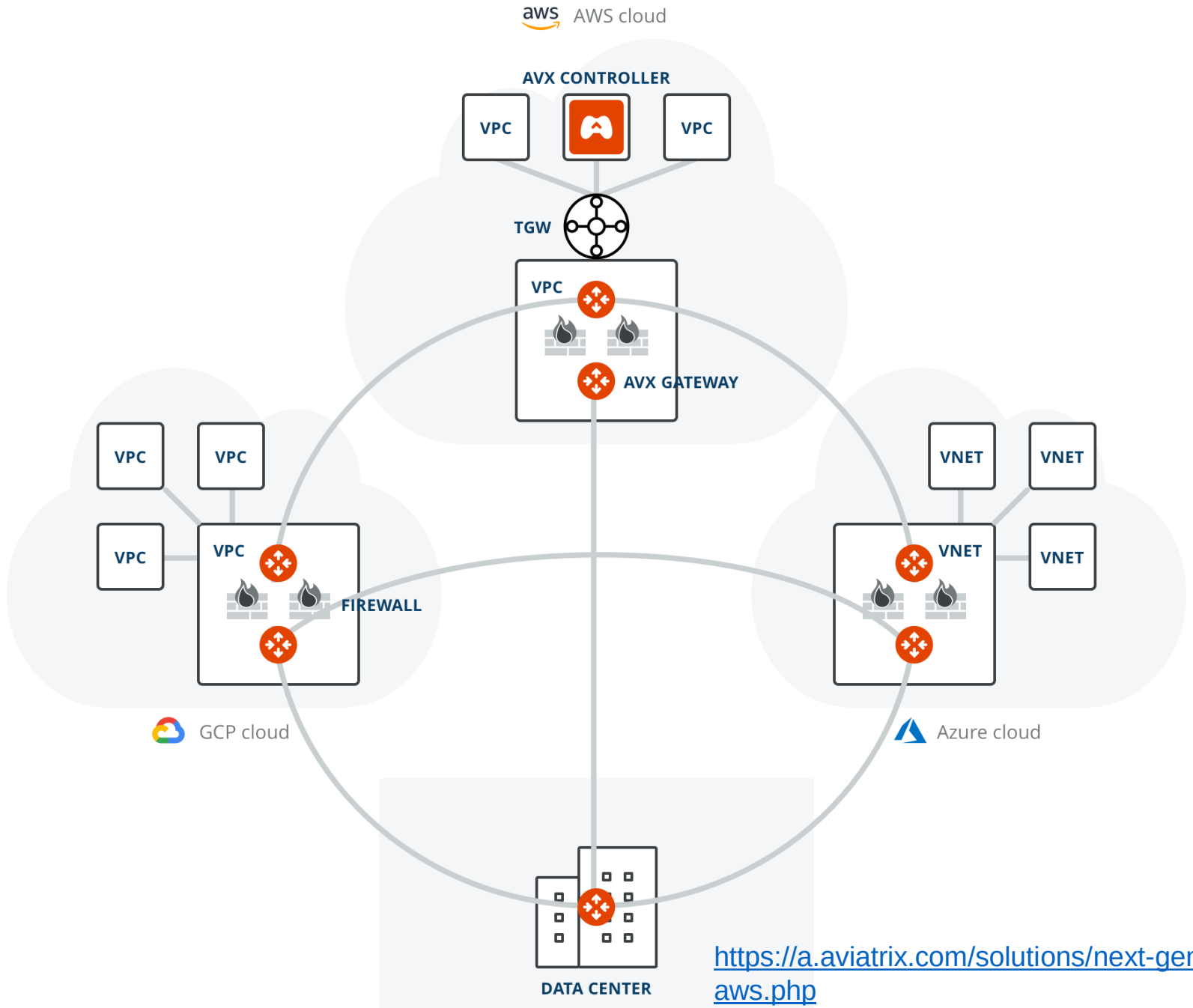
https://www.optiv.com/sites/default/files/2019-08/Navigating-the-Security-Landscape_WhitePaper-_Web.pdf


Message Security
PERIMETER SECURITY
Antivirus/Antimalware
Secure DMZs
Honeypot
Web/Proxy Content Filtering
NETWORK SECURITY
Perimeter IDS/IPS
Patching
NAC
Enterprise Message Security
DHS Einstein
VoIP Protection
Endpoint Security Enforcement
ENDPOINT SECURITY
Enterprise Wireless Security
Perimeter Firewall
Datacenter IDS/IPS
Content Security
FDCC Compliance
Enterprise Remote Access
DLP
Antivirus/ Antimalware
Dynamic App Testing
Datacenter Firewall
Host IDS/IPS
APPLICATION SECURITY
Patch Mgmt.
DLP
Critical Incidence Reporting
IT Security Governance
WAF
Database Monitoring/Scanning
Desktop Firewall
DevSecOps
DLP
Enterprise Rights Mgmt.
Security Architecture & Design
Static App Testing
DATA SECURITY
Database Secure Gateway
Focused Ops.
SOC/NOC Monitoring
IAM
DLP/DAR/DIM/DIU
Data Classification
Continuous Monitoring
Risk Management
Security Policy
PKI
Data Wiping
Assessment, Situational Awareness
Security Dashboard
Threat Intelligence & Modeling
SIEM
Encryption.
(PROACTIVE)
Penetration Testing
MISSION CRITICAL ASSETS
Escalation Mgmt.
(REACTIVE)
Security SLA
Data Integrity Monitoring.
POLICY MANAGEMENT
Vulnerability Assessment
MONITORING + RESPONSE
Security Awareness
Digital Forensics

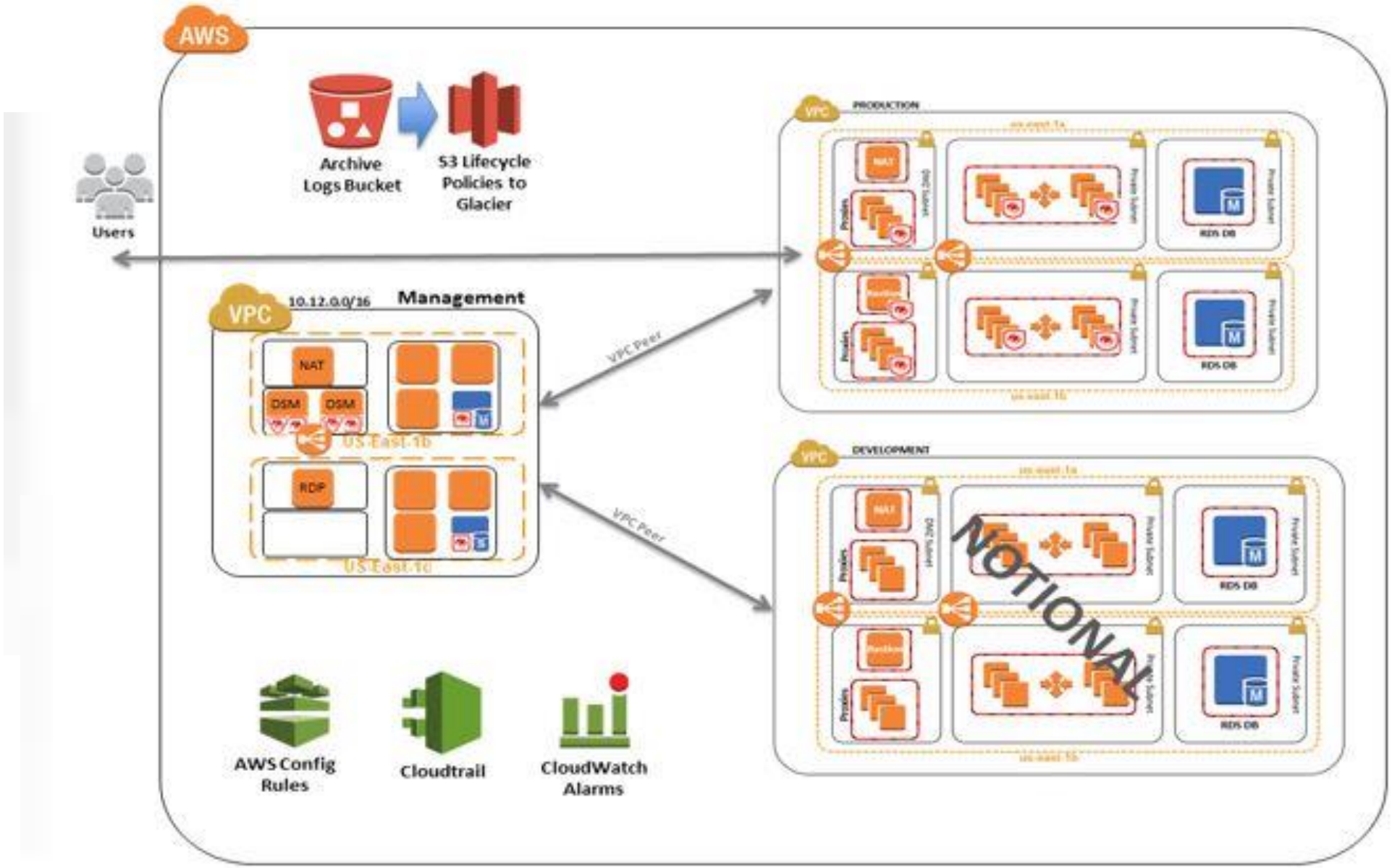

Risk Profile
Risk= (Data Type * Breach Probability)/Security Profile
Data Pedigree
Data Security Profile + Data Owner + Originating System + Data Integrity Confidence
Security
NIST SP 800-53v4
SP 800-53v4, Pub 1075, CJIS-SP
Policies & Procedures Profile 1
Policies & Procedures Profile 2
Policies & Procedures Profile 3
Policies & Procedures Profile 4
Data Security Profile 1
Data Security Profile 2
Data Security Profile 3
Data Security Profile 4
Data Object
Integrity Controls
Privacy Act FISMA
HIPAA PCI-DSS FERPA
Pub 1075 CJIS
Public Data
Classification: Low
Classification: Moderate
Classification: High
Public Data
Confidential Data
Restricted Data
Public Data
Sensitive Data

Cloud Networking

- Network
  - Subnet – internal IP addresses (not globally routable)
  - Routing Table – Specify & allow routes for outbound
  - Security Groups and Access Control Lists
  - Gateways – Connections for outside networks
- Hybrid Cloud Connectivity
  - Transit Network Hubs
    - Visibility and control across all layers
    - High-Availability
    - End-to-end Encryption
    - Intelligence
    - Traffic Engineering and Optimal Path Prioritization
    - Repeatable Network Design
    - Multi-Cloud Network Access Policy

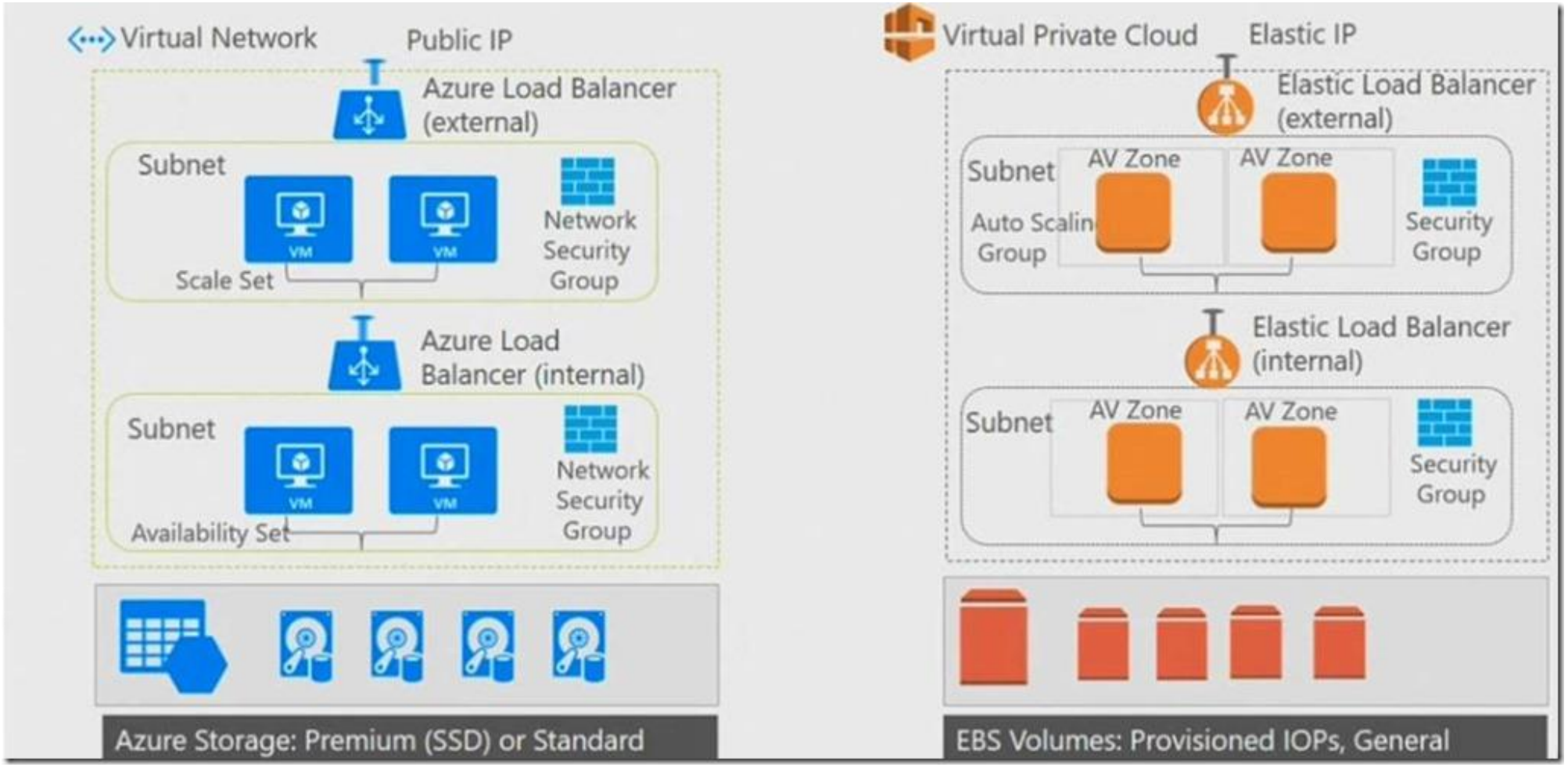


https://a.aviatrix.com/solutions/next-gen-transit-network-aws.php



https://aws.amazon.com/blogs/publicsector/automating-compliance-architecting-for-fedramp-high-and-nist-workloads-in-aws-govcloud-us/

IaaS Connections



[Differentiating-between-azure-virtual-network-vnet-and-aws-virtual-private-cloud-vpc]

Cloud Security Landscape

http://www.josephfloyd.com/blog/cloud-security-landscape

Foundational Security

Network, Data Center, Endpoint

Network

Firewall, Wireless, Intrusion Detection & Prevention, Network Access Control
SSL visibility, Secure Network, Secure Web Gateway, DDoS mitigation
Remote-access Software-defined Perimeter

FIREWALL PROVIDERS

Barracuda Networks
Check Point
Cisco
Endian
Enghouse Networks
F5
Forcepoint
Fortinet
GE/Wurldtech
Huawei
Juniper Networks
Leidos
Netgate
Palo Alto Networks
Sangfor
SonicWall
Sophos
Trend Micro

WIRELESS PROVIDERS

Aruba
AccelTex
Aerohive Networks
AirPatrol
AnaLynk Wireless
Arista/Mojo Networks
Arris
Broadcom
Cisco
Cradlepoint
Edgecore Networks
Extreme Networks
Fluke Networks
Fortinet
Juniper Networks
Meru Networks
Mojix
Riverbed Technology
7Signal
WatchGuard Technologies
Zebra/Motorola

INTRUSION DETECTION SYSTEMS/ INTRUSION PREVENTION SYSTEMS PROVIDERS

Check Point
Cisco
CyberX
Fortinet
Juniper Networks
McAfee
Netshield (formerly SnoopWall)
Palo Alto Networks
Reservoir Labs
Trend Micro
WatchGuard Technologies

NETWORK ACCESS CONTROL PROVIDERS

Aruba
Forescout
InfoExpress
Netshield (formerly SnoopWall)
Portnox
Saviynt

SSL VISIBILITY PROVIDERS

ExtraHop
F5 Networks
Fidelis Cybersecurity
FireEye
Gemalto
Gigamon
Ixia
Palo Alto Networks
SonicWall
Symantec
Thales

DDoS MITIGATION PROVIDERS

Arbor Networks
Check Point
Cloudflare
F5 Networks
FlowTraq
Fortinet
Imperva
Radware

SECURE WEB GATEWAY PROVIDERS

Authentic8
Cato Networks
Cisco
F5 Networks
Forcepoint
Fortinet
GFI Software
McAfee
Menlo Security
Netgate
OPAQ
Palo Alto Networks
Proofpoint/Weblife.io
Symantec
WatchGuard Technologies
Zscaler

REMOTE ACCESS SOFTWARE-DEFINED PERIMETER PROVIDERS

AGAT Software
Aporeto
Attila Security
Cisco
Cyxtera
Fortinet
LogMeIn
NCP Engineering
Palo Alto Networks
Pulse Secure
Safe-T
Securelink
Tempered Networks

Endpoint Protection

Protection, Detection & Response, Application Control

ENDPOINT PROTECTION SUITE PROVIDERS

AhnLab
Avast
Bitdefender
Carbon Black
Check Point
Cylance
Deep Instinct
Ensilo
ESET
F-Secure
Fortinet
Kaspersky
McAfee
Minerva Labs
Morphisec
Nyotron
Panda Security
Rubica
Sophos
Symantec
Trend Micro
Webroot

ENDPOINT DETECTION AND RESPONSE PROVIDERS

Carbon Black
Check Point
CounterTack
CrowdStrike
Cybereason
Cylance
Deep Instinct
Emsisoft
Endgame
ESET
eShore Ltd
Fidelis Cybersecurity
FireEye
Malwarebytes
McAfee
Nehemiah Security
Palo Alto Networks
RSA
SentinelOne
Tanium
Ziften