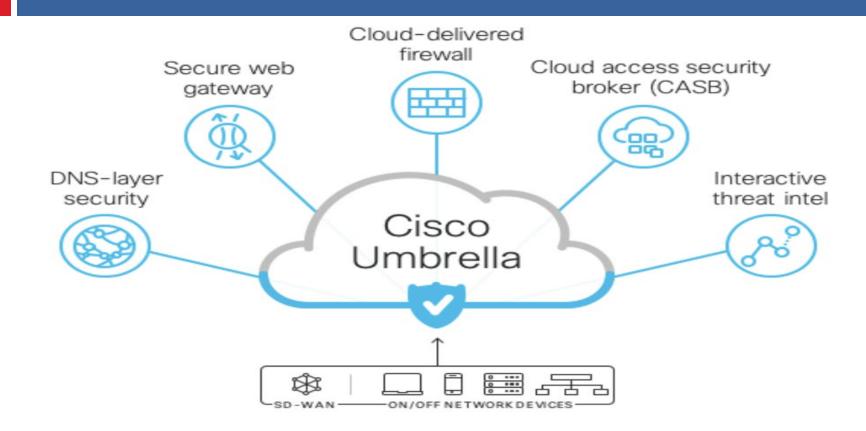


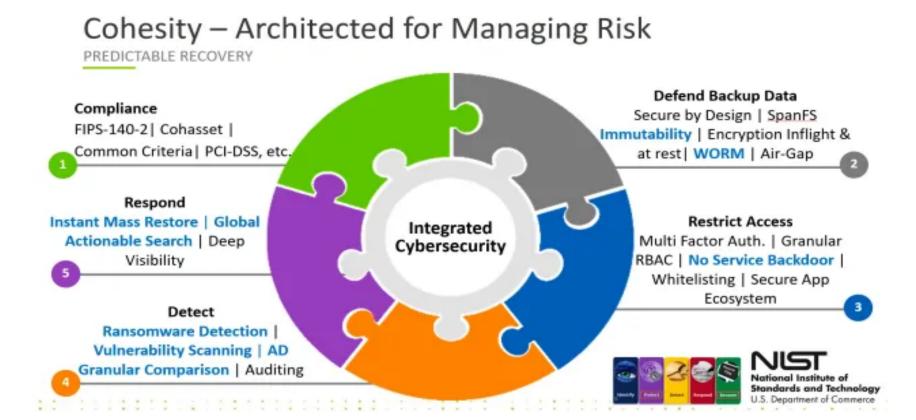
CYBERSECURITY POSTURE

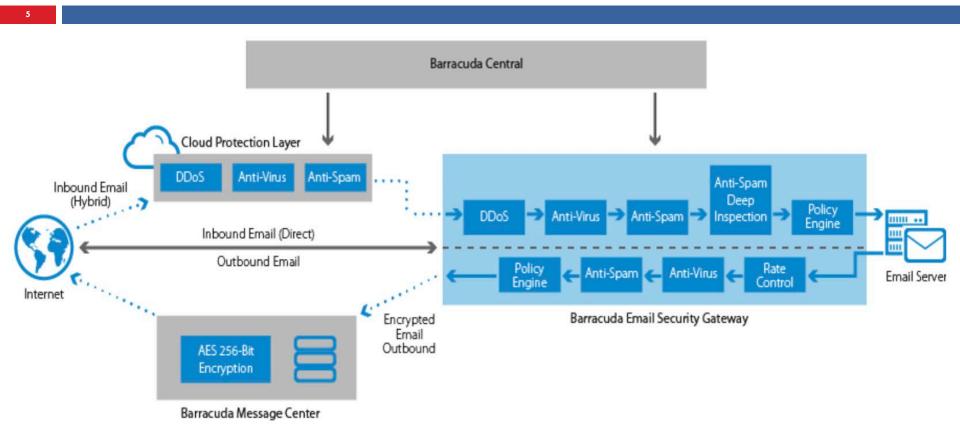
30 April 23, 2024

Background

- Cybersecurity is a critical aspect of our operations in the city, especially in today's digital landscape where threats are constantly evolving.
- This briefing aims to provide an overview of our cybersecurity posture, including implemented solutions, ongoing initiatives, and future plans to ensure the security and integrity of our systems and data.







MY DASHBOARDS + ALERTS & ACTIVITY + REPORTS * SETTINGS + GUEST (LOGOUT) Friday, 09 October 2020 16:13:40 **NPM Summary** MANAGE NODES VIEW MODE VIEW MODE All Nodes managed by NPM MPLS Network Cisco ACI Map HELD GROUPED BY VENDOR STATUS P Address 10 140 0200 IP ABBREST 10,21 0,230 American Power Conversion Corp. Auerage Response Time 2 ms Average Response from 310 ms Aveya Communication LOSA PSTREET NEWY EXCENT P AMMIN 10 1962 TO PARKS 10196219 O Cisco Average Response Time 2 ms. Average Response Time 1 ms. > O Up * O Cripical NEWY-2811-WAN Down - A Warning ▲ AUS-SUB-01 ▲ DEN-2968-1A ▲ DEN-3750-SwitchStack HIRDS TO THOUSE DV ▲ EAST-4506E-CORE ▲ EAST-9300-1stFI ▲ FIBRE-Tex-Mds9120 ▲ LON-3560-A51.dema.lab and the state of the color of ▲ LON-3560-AS2.demo.lab and the water measure to on-▲ LOSA-2821-WAN WEST-0603 8A87-45000 9:5Mpx 25 SP Address 10.025-5-1 P Assess 10-1-0-1 ▲ NX-7K-B-admin Average Response Tare 2 ms. Average Religionse Tyris: Tims: Average Resource Time 4 ms. P Address 10:12:1 ▲ SIN-3560-AS1.demo.lab P.ASSEN 10 105 0 250 Average Rescorde Tarie 2 ms. ▲ SIN-3560-A52.demo.lab HELP ▲ WEST-3850-CORE Interfaces with High Percent Utilization ▶ ■ Dell Computer Corporation List of Switch Stacks F5 Networks, Inc. RECEIVE TRANSMIT ► O IBM CAPTION IP ADDRESS MAC ADDRESS MEMBER COUNT DATA RING STATUS Nexus-2 port-channel31 - Po31

Ongoing Initiatives

- Legacy Application Replacement:
 - Scheduled replacement of legacy applications such as Navaline and PDRMS system to modernize our infrastructure and mitigate potential security vulnerabilities associated with outdated systems
- Cybersecurity and Incident Handling Plan:
 - Developed a comprehensive plan to effectively respond to cybersecurity incidents, ensuring timely detection, containment, eradication, and recovery
- Annual Cybersecurity Training:
 - Conducting annual cybersecurity training sessions for all employees to enhance awareness and ensure compliance

Future Plans

- Regular Security Assessments and Audits:
 - Instituting periodic security assessments and audits to identify vulnerabilities, assess risks, and validate the effectiveness of our cybersecurity measures (completed Network Assessment Apr 2024)
- Collaboration with External Partners:
 - Strengthening partnerships with external cybersecurity experts and agencies to stay abreast of emerging threats and leverage their expertise in enhancing our cybersecurity posture