NORTH Dakota | Information Technology

Be Legendary.™

Team North Dakota

# EMPOWER PEOPLE
# IMPROVE LIVES
# INSPIRE SUCCESS

Senate Appropriations Sub Committee
Bismarck, ND

# Topics for today

- Framing the real cyber security problem
- Data on cyber security situation
- Service Management
- Open Conversation / Q&A

# Framing the Real Cyber Problem

NORTH Dakota | Human Services

Be Legendary.™

## Cyber impacts for DHS

- Numerous ransomware and phishing issues
  - Highly disruptive to the teams
  - Costly to fix (~$100K per event)
  - Causes downstream issues with Federal partners
- Very high risks due to systems and data held

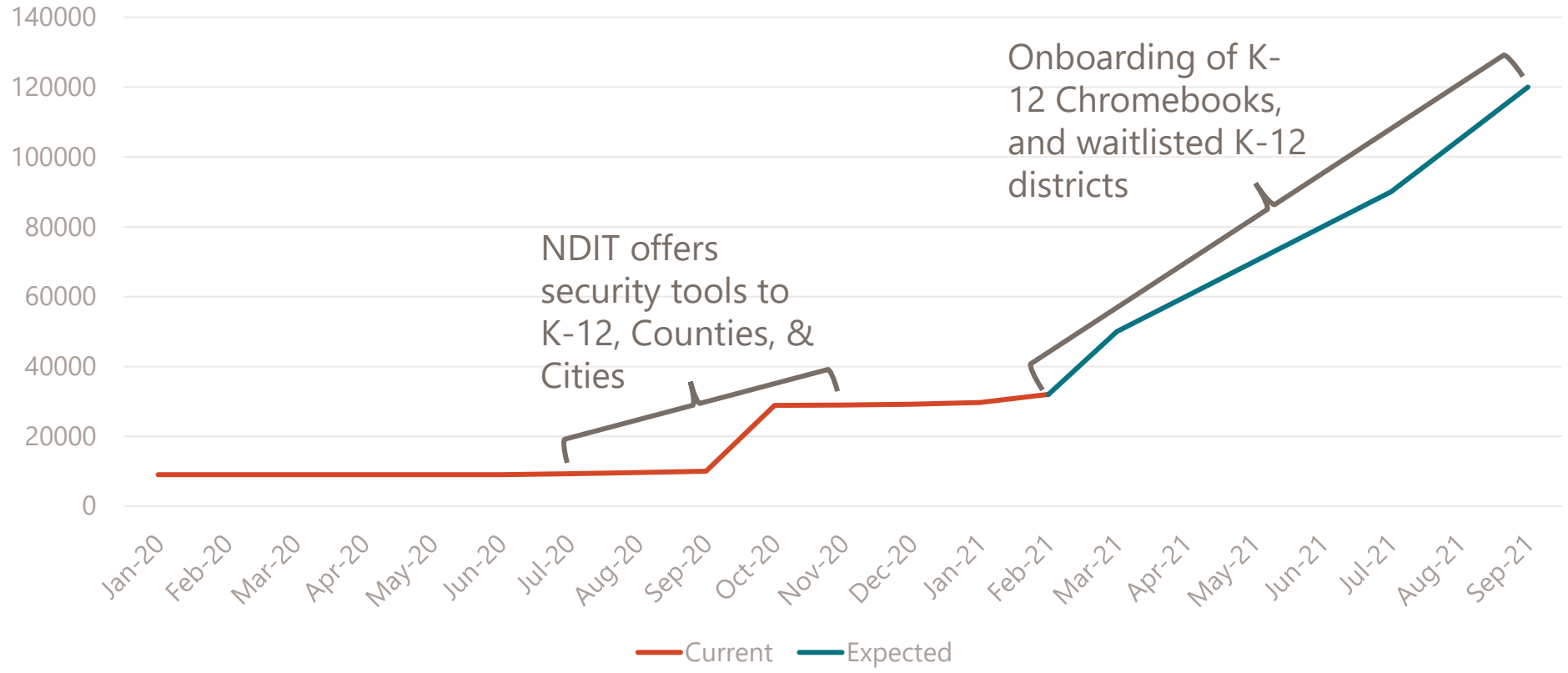
Chris Jones
Executive Director


Please
STOP

# Cybersecurity Management Data

# 4X GROWTH OF SECURITY PRODUCT ADOPTION IN 2021

The total cost in tools and services for every County, City, and School District in North Dakota to obtain basic security functionality is $413,882,000[1] per Biennium.

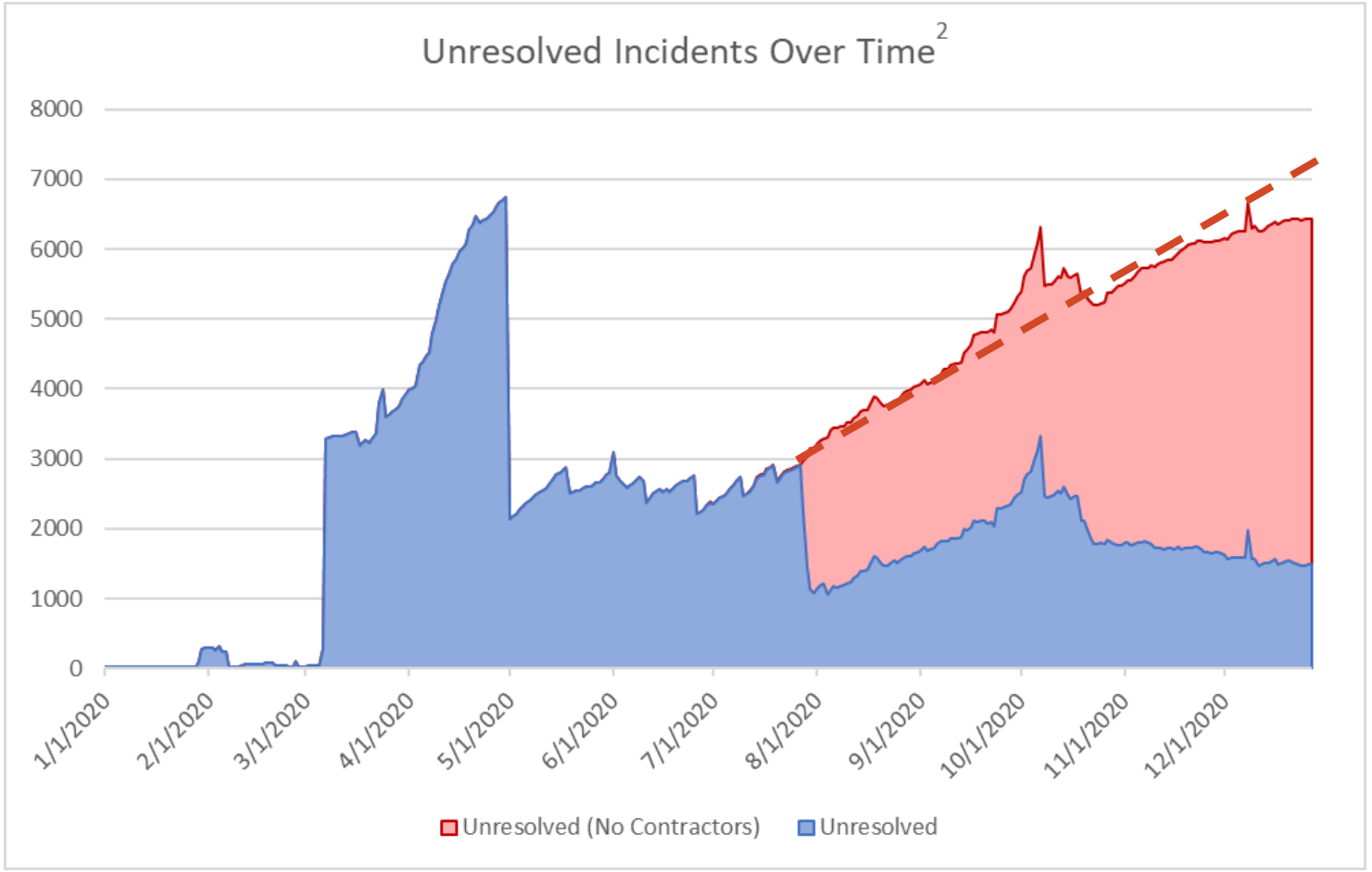



Based on Endpoint Detection and Response Toolset and Vulnerability Management Toolset quotes from 11/24/2020 for small government organizations (see Appendix) and industry average Security Analysts per endpoint from: Osterman Research - The Evolving State of Network Security, 2018, Cited by InfoSecurity group (September 2018). https://www.infosecurity-magazine.com/news/security-staffing-low-in-midsized/

# IMPACT OF MAINTAINING CURRENT FTE

Over 74,000 unresolved incidents by next biennium

Tens or Hundreds of Million Dollars Lost

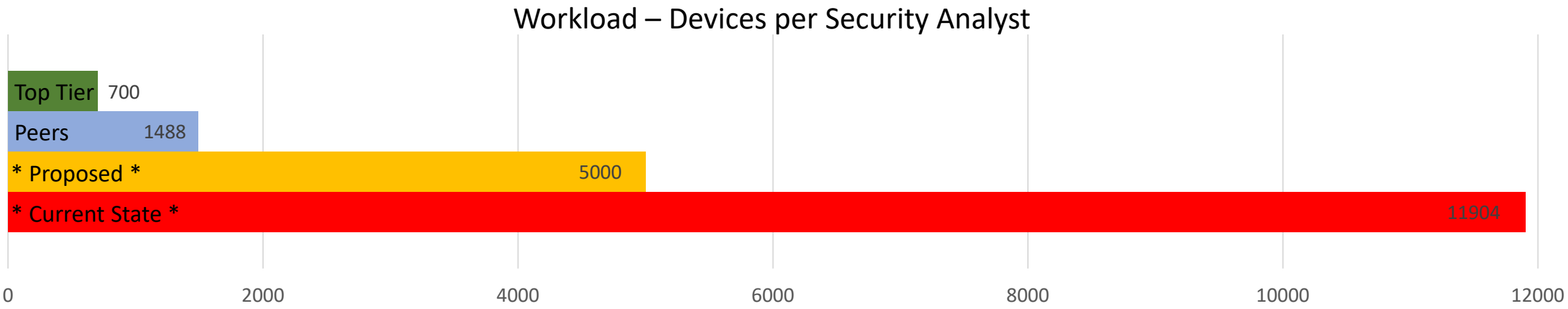



1. Averages based on Cortex XSOAR data

# Cybersecurity Workload is 8X Higher than Peers

## Significant Human Cost

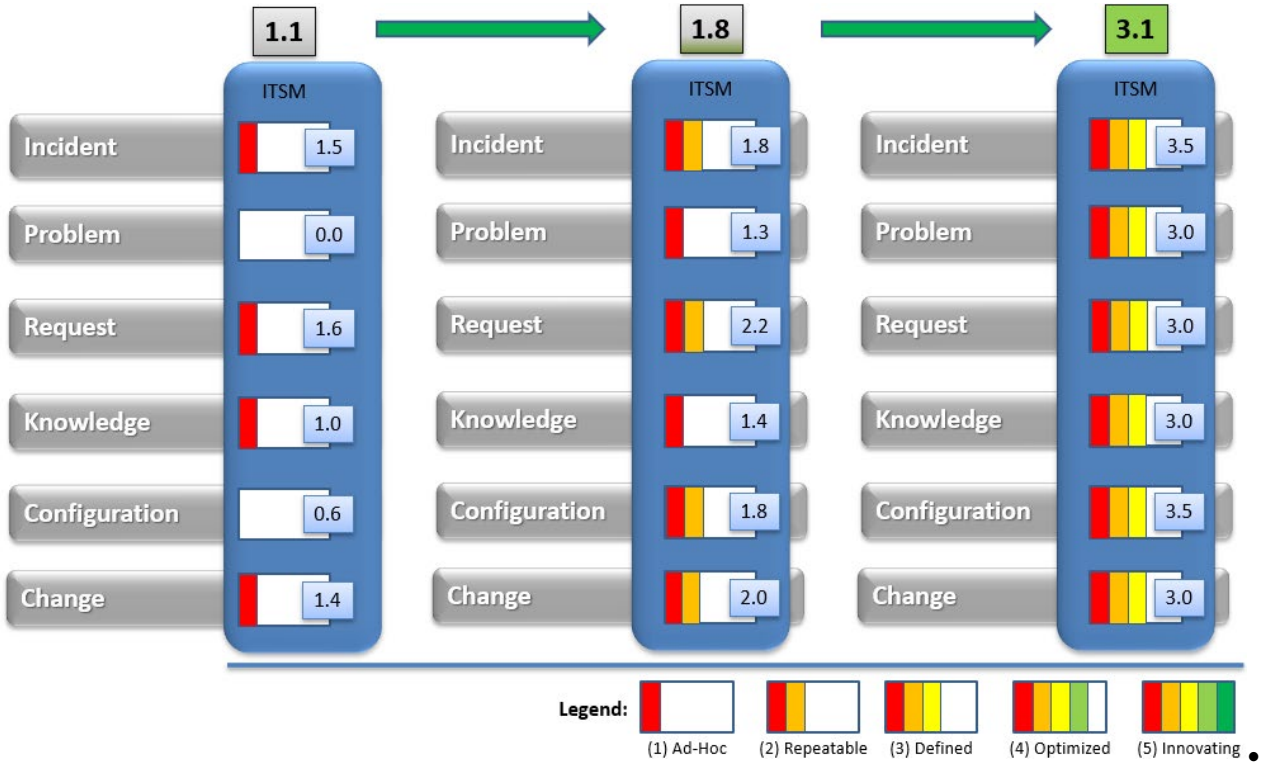
- 50 to 80 Hour Work Weeks
- 3/4 will lose PTO this biennium
- All staff is always on call
- No or Very Little Time Off

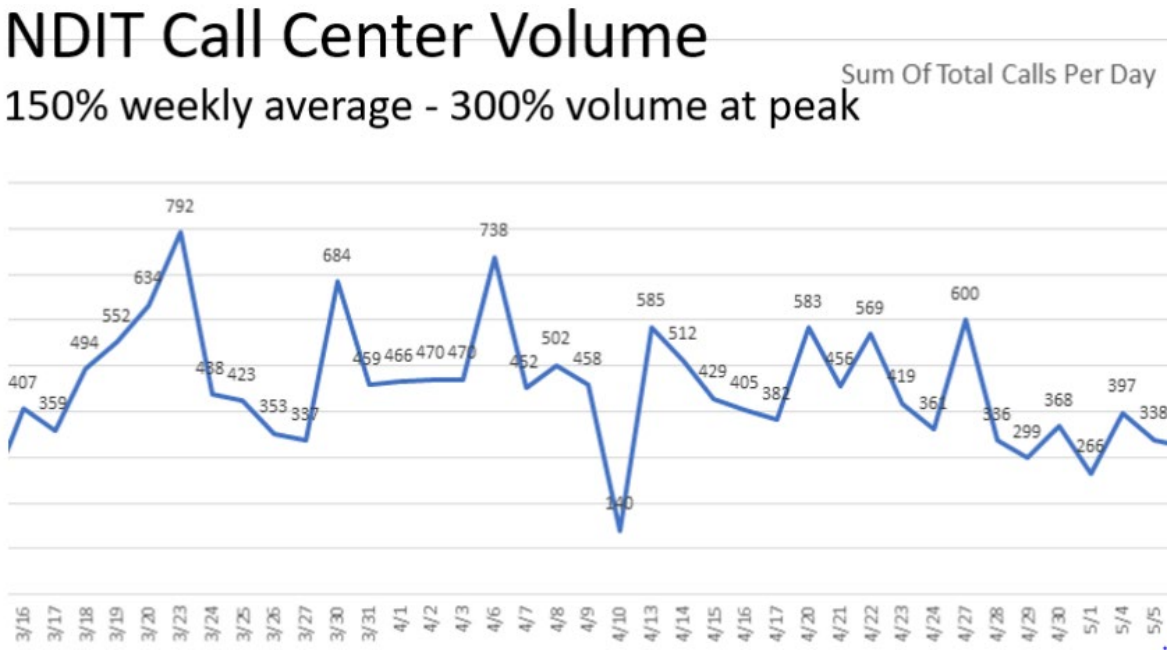



1. Based on industry average of 1 analyst per 1,488 endpoints for large organizations documented in Osterman Research - The Evolving State of Network Security, 2018, Cited by InfoSecurity group (September 2018). https://www.infosecurity-magazine.com/news/security-staffing-low-in-midsized/

# Service Management

# Service Management

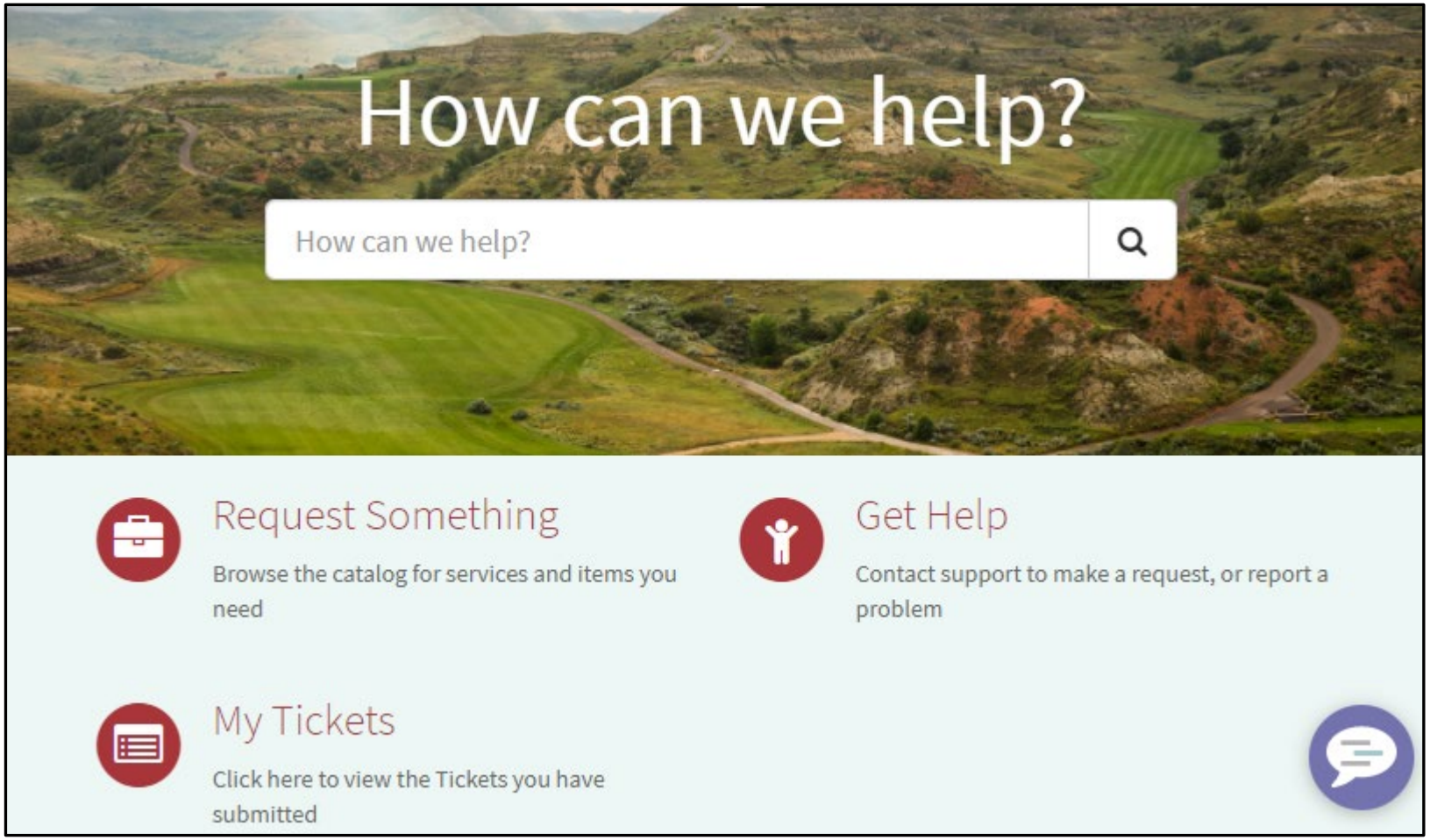



2.3
Target EOY 21

3.1
Target EOY 22

- **Ad-Hoc** – Unpredictable and reactive
- **Repeatable** – Processes are managed but not standardized
- **Defined** – Processes are standardized across the organization
- **Optimized** – Visibility, predictability across organization
- **Innovating** – Strong governance for all process and functions




96.2%
Satisfaction

96.1%
Recommend NDIT

2,694
Avg Weekly Incidents

71%
First Call Resolution

0.12 Day
First Call Resolution Time

1.4 Day
Avg Resolution Time

# Voice Solution

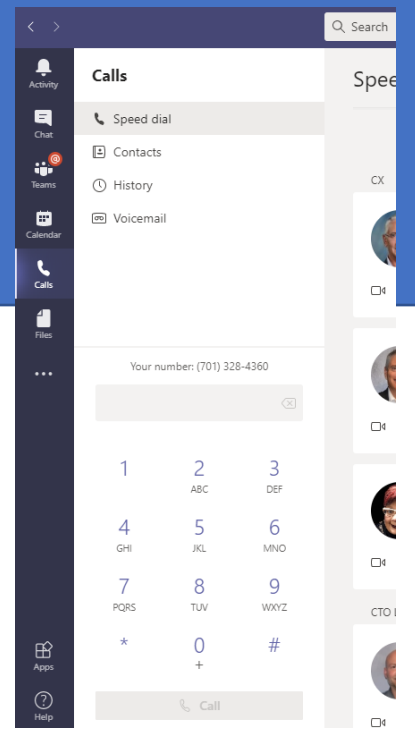
# Voice Solution:

## Avaya Voice:

- Traditional Voice Solution
- End of Life or near End of Life infrastructure
- Poor mobile and telework solution
- Limited integrations

## Teams Voice:

- Modern Voice Solution
- Software part of the owned 0365 bundle
- Significantly improved mobile and telework experience
- Integrated experienced with MS Teams that is already the standard collaboration tool
- Cost Avoidance:
  - $1.4M estimated in desk phones (strongly encouraging softphones – desk phones are available)
  - $1.2M estimated core infrastructure




# Appendix Materials

# Service Management Data

# Feedback Methodology

Approach:  As part of the overall maturity of the service management program all processes and approaches are being evaluated. In addition, the toolsets used to manage the program has been replaced to ensure we have both quality processes and toolsets.

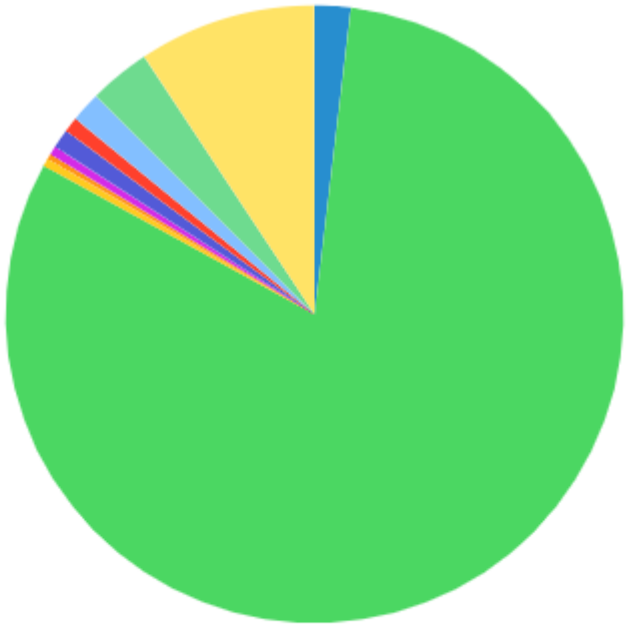
Current Approach:  The new toolset went live July 2020.  As such, the feedback approach was changed at that time.  The current approach is a shorter survey and a request for feedback is not included with every incident.  The best practice approach is to use a random sampling which currently equates to a 1 in 4 chance of being requested to complete a survey.  This approach continues to be evaluated and has resulted in a higher percentage of surveys completed.  Response rate is now 379 per month which is a 24% increase.

Prior Approach:  The prior toolset and approach equated to a survey request for each and every incident. This approach included 5 questions which are on the slides below and resulted in an average of 304 responses.

# Customer Feedback

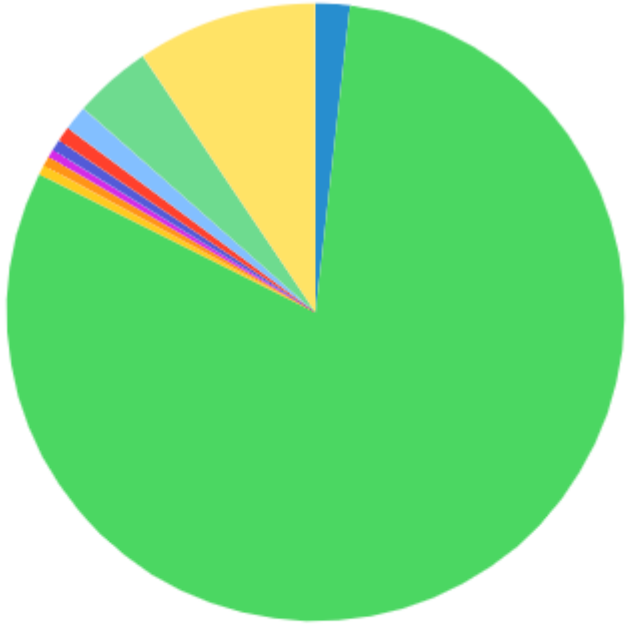
Customer feedback from July 2020-Jan 2021

How likely would you recommend to friend or colleague?



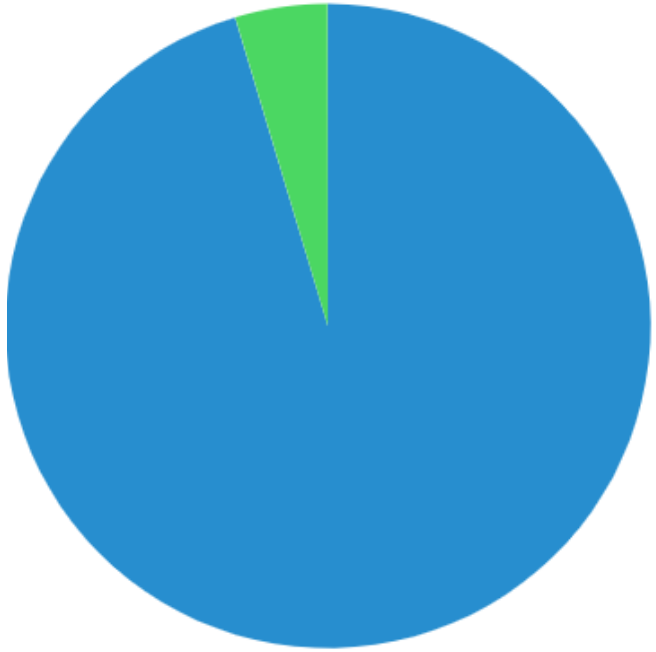
1 = 41 (1.89%)
3 = 6 (0.28%)
6 = 17 (0.78%)
9 = 202 (9.29%)
10 = 1,764 (81.1%)
4 = 10 (0.46%)
7 = 34 (1.56%)
2 = 9 (0.41%)
5 = 22 (1.01%)
8 = 70 (3.22%)

How would you rate your overall satisfaction with the service you received?



1 = 39 (1.79%)
3 = 11 (0.51%)
6 = 17 (0.78%)
9 = 205 (9.43%)
10 = 1,753 (80.6%)
4 = 9 (0.41%)
7 = 28 (1.29%)
2 = 11 (0.51%)
5 = 13 (0.6%)
8 = 89 (4.09%)

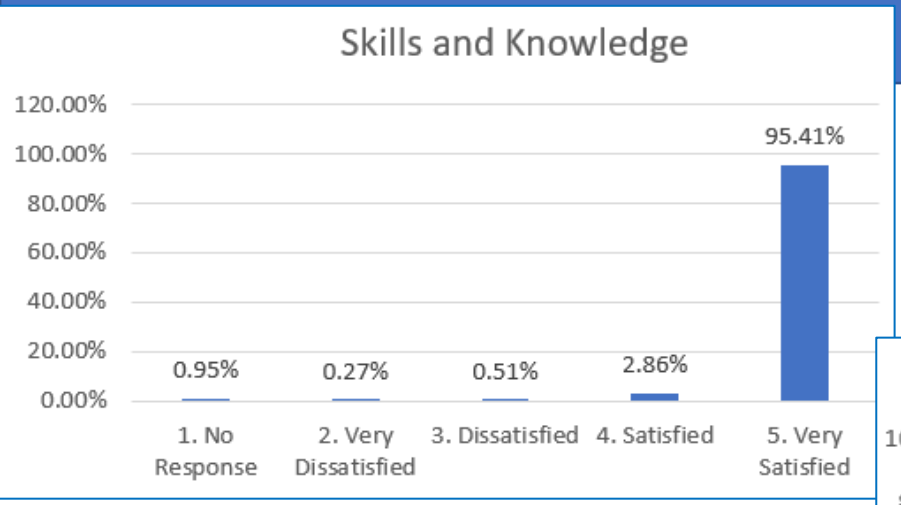
Would you like us to contact you?

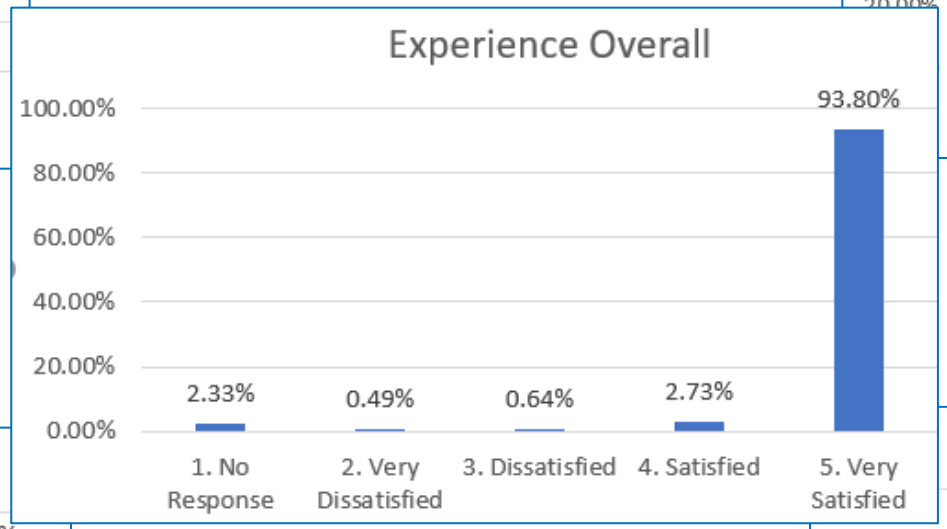


No = 2,074 (95.36%)
Yes = 101 (4.64%)

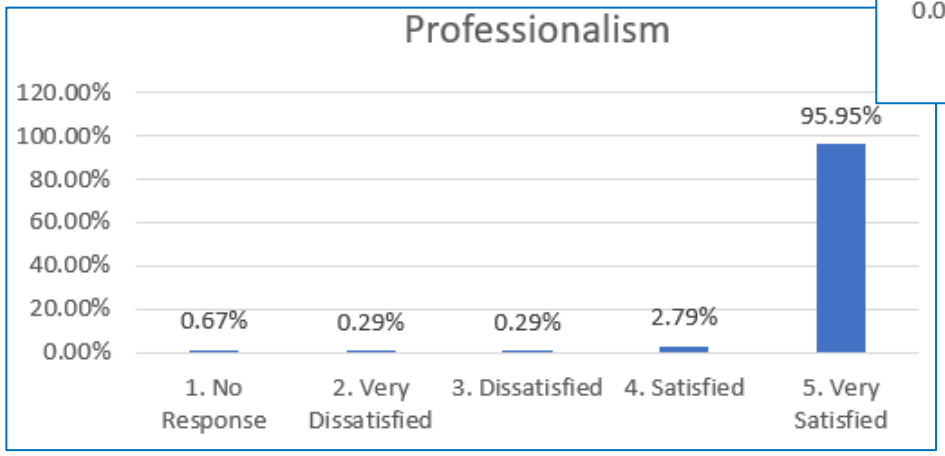
# Customer Feedback

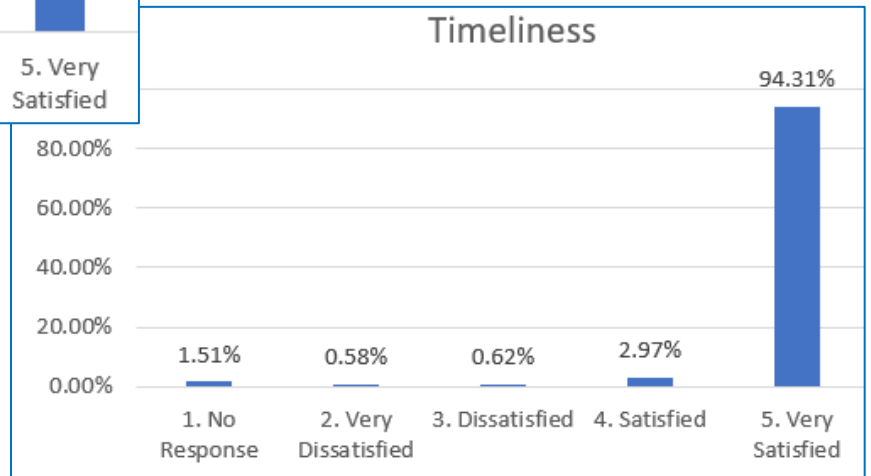
Customer feedback from Jan 2019 – June 2020



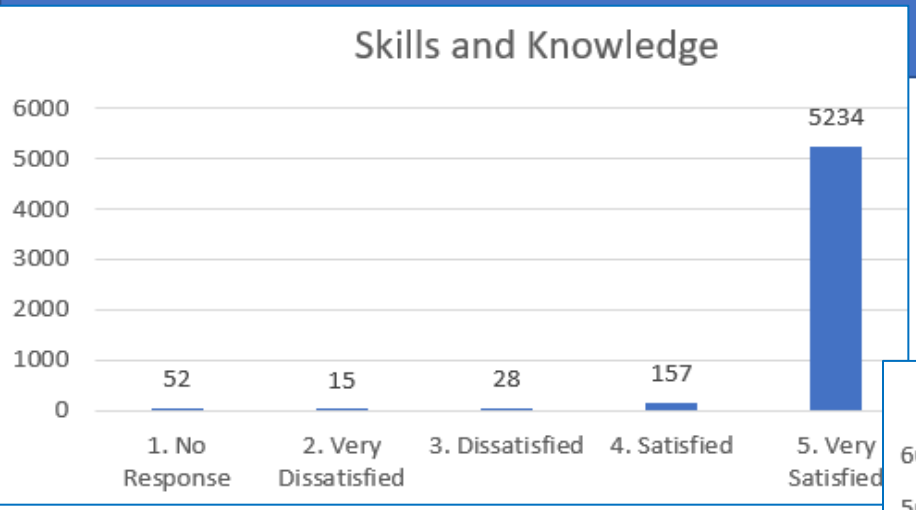


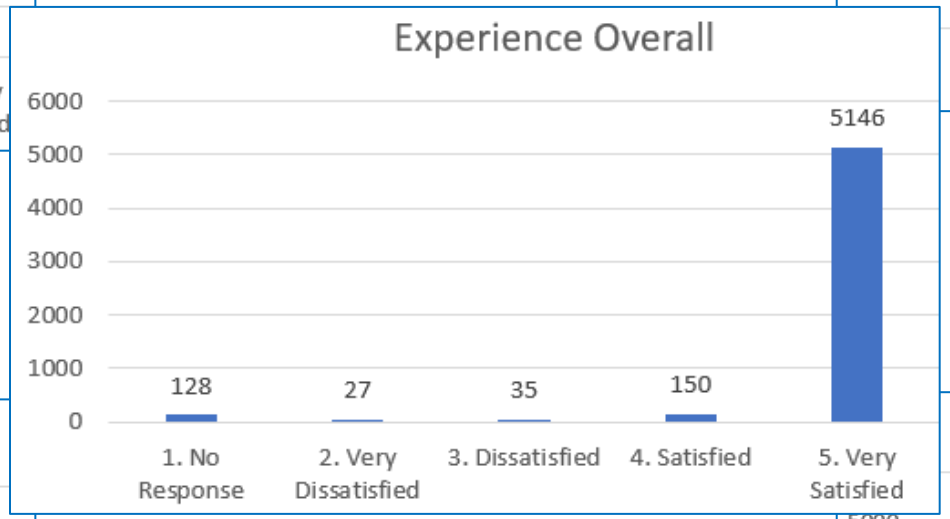


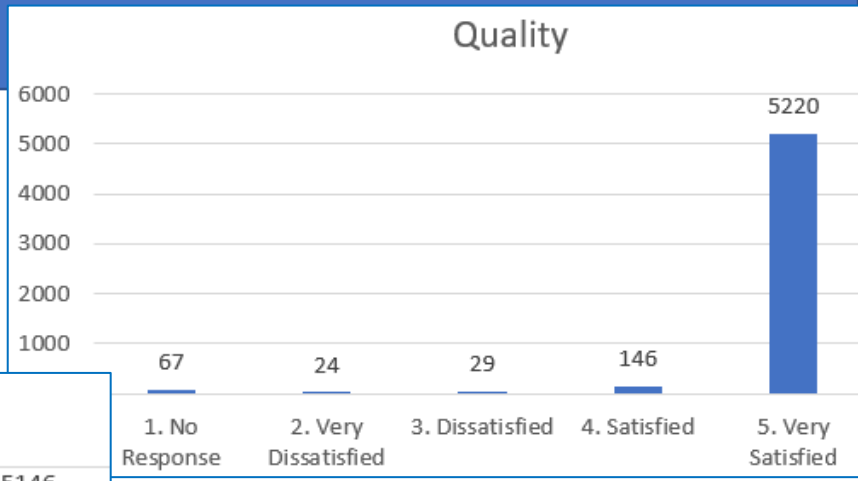



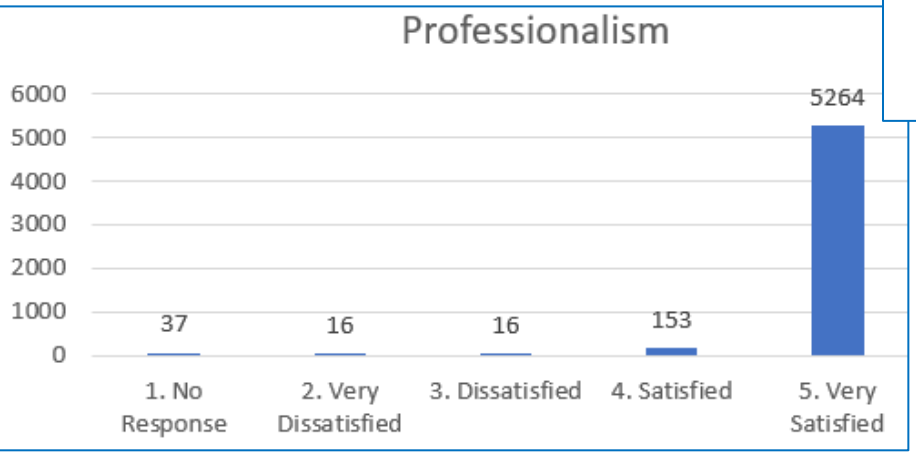
# Customer Feedback

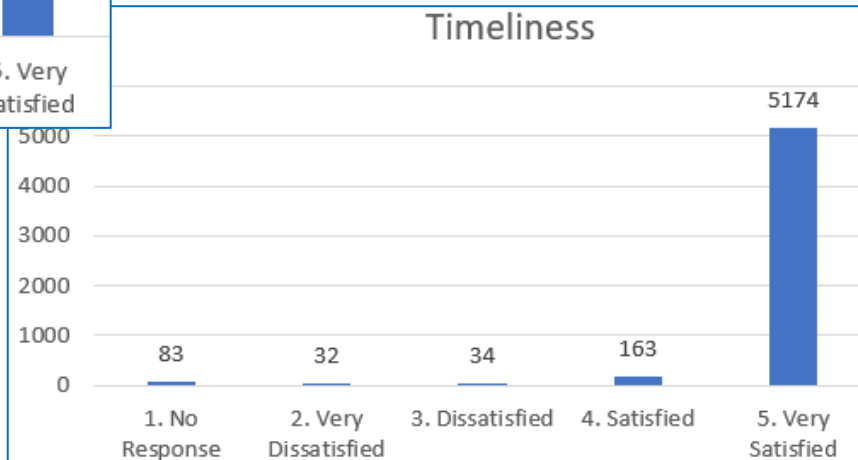
Customer feedback from Jan 2019 – June 2020



# Industry Benchmarks

How do we compare to other government organizations?

## IT Service Management

**Summary:** November 2020 | **Your Industry:** Government

ALL | **INCIDENT** | PROBLEM | CHANGE | SERVICE CATALOG

27.85
Percentile

0.7%

% of high priority incidents

1.1%
Benchmark

View trend

55.9
Percentile

73.2%

% of incidents resolved on first assignment

67.4%
Benchmark

View trend

44.95
Percentile

1.4%

% of reopened incidents

2.6%
Benchmark

View trend

66.46
Percentile

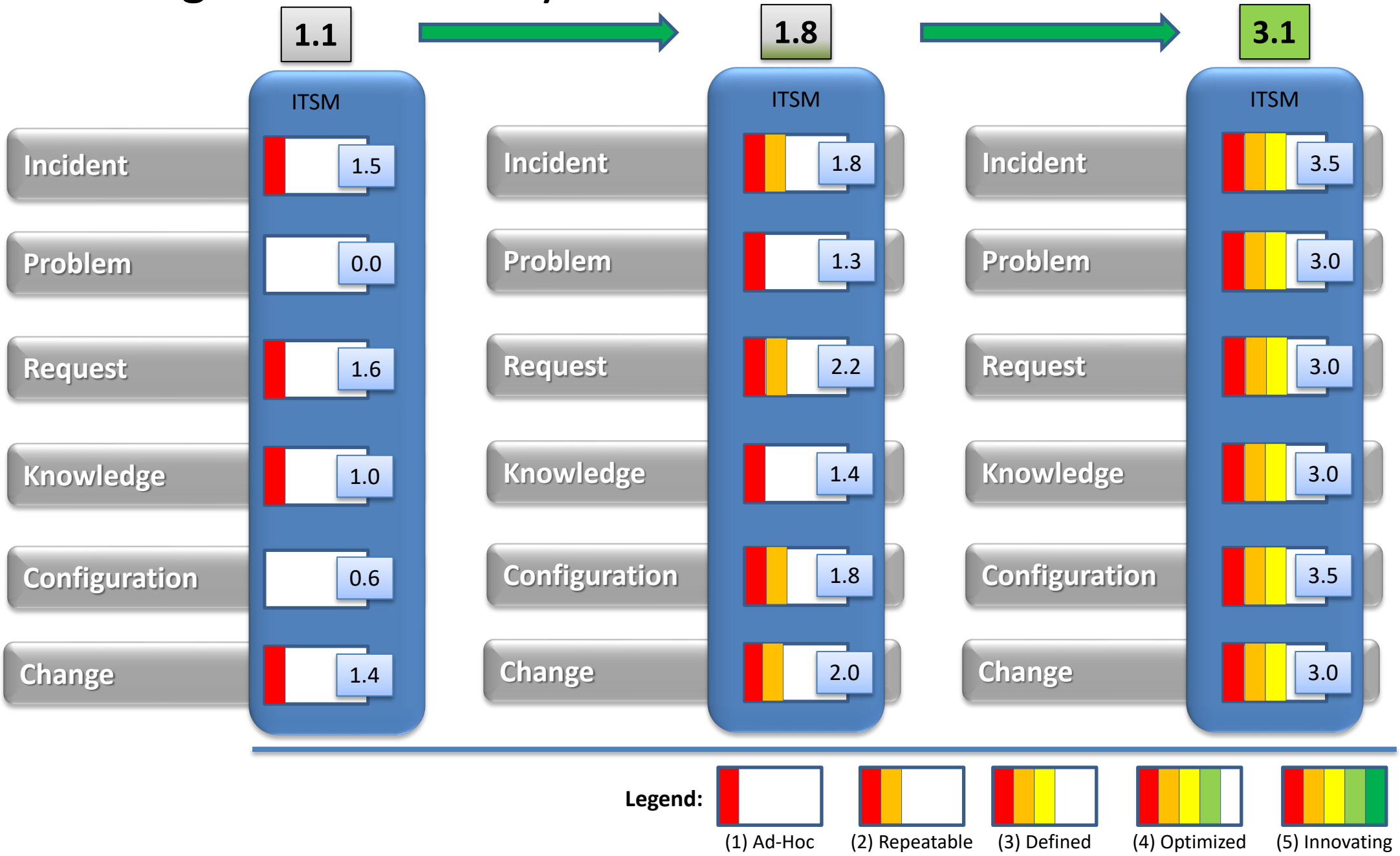
3 hours

Average time to resolve a high priority incident

21d 20h
Benchmark

View trend

# Service Management Maturity Assessment

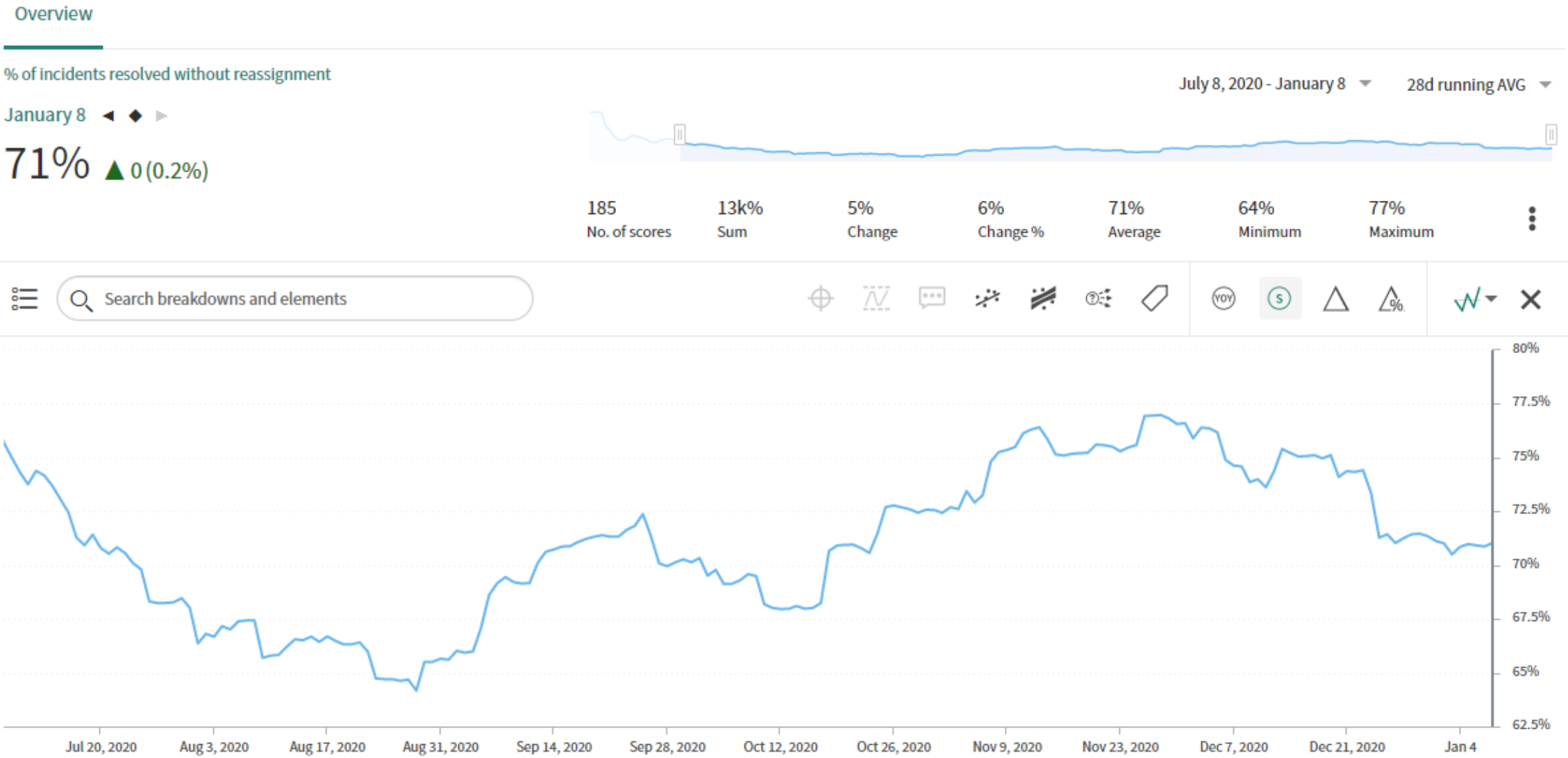


# Incidents – 7 Day Sum

Number of Tickets per Week

# Incidents – First Call Resolution

First Call Resolution: The percentage of calls resolved without the need of escalation beyond first contact

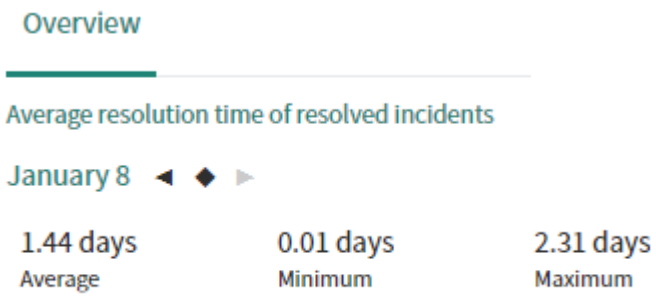


# Incidents – Mean Time to Resolve

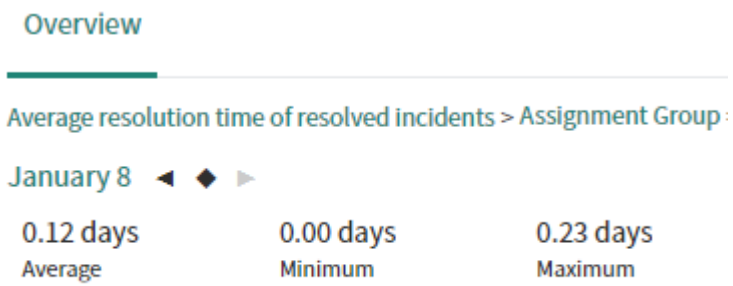
**When is an incident resolved?**

- When the customer acknowledges resolution
- When confidence is high the incident is resolved but the customer is non-responsive

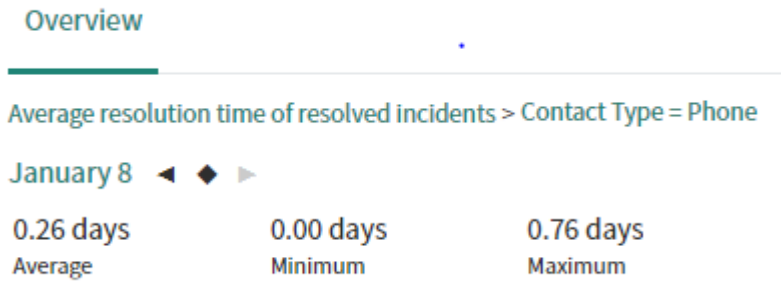
## Overall




## First Call Resolution – Mean Time to Resolve




## Incidents created by calling the service desk

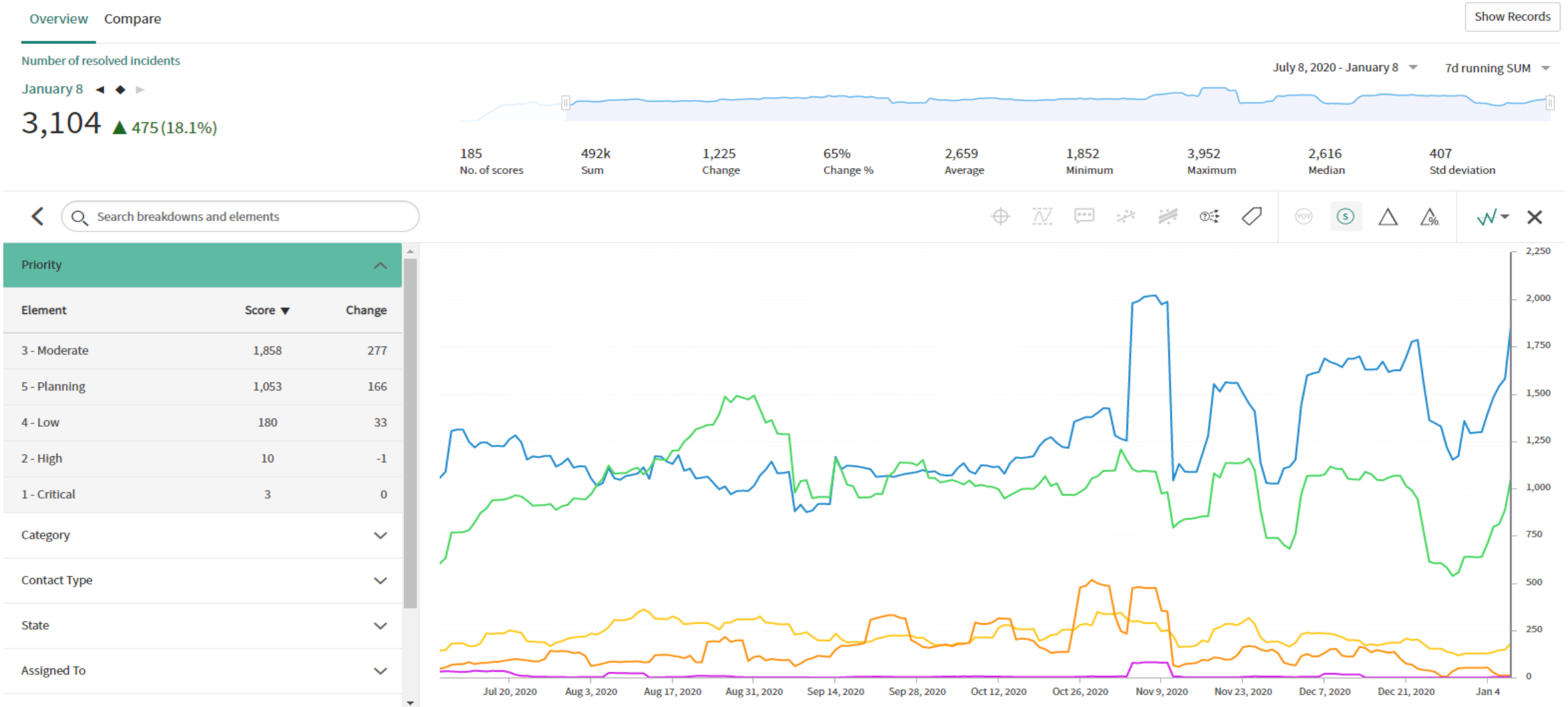



## Incidents created by emailing the service desk


** Resolution times increase when waiting on electronic confirmation from customers*

# Incidents – Resolved by Priority

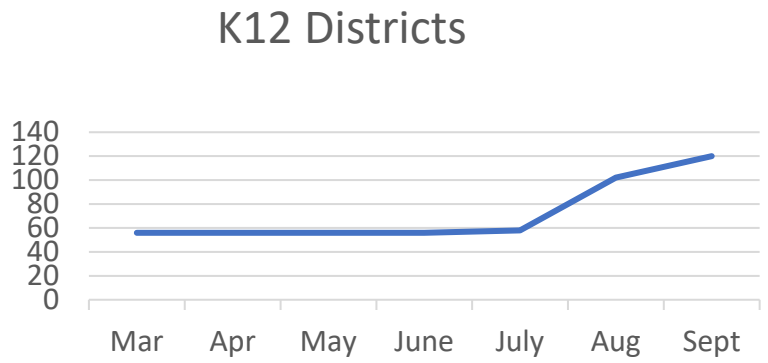
Priority: Tickets are given a priority number 1-5 based on impact and urgency

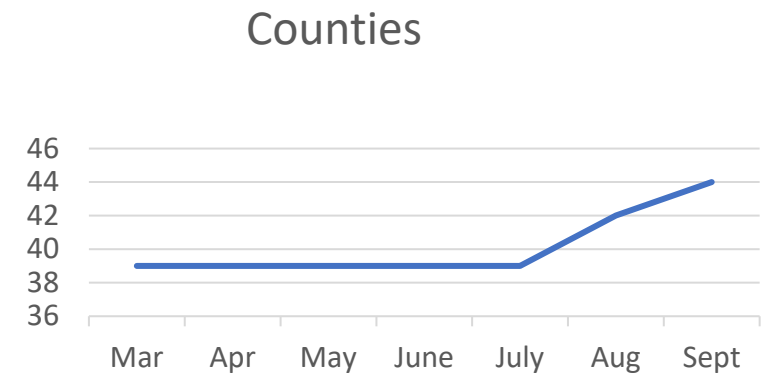


# Cybersecurity Data

# Whole of State Approach

- The number of K-12 Districts, Cities, and Counties supported by NDIT has **Doubled** since the COVID-19 outbreak;
  - 120 Districts total with more implementing,
  - Expect 75% of all K-12 districts using NDIT resources by mid-summer,
- Similar increase in County and City Governments using NDIT resources;
- Deliver about $413,882,000 in people, processes, and technology.



# Cyber Risk in North Dakota

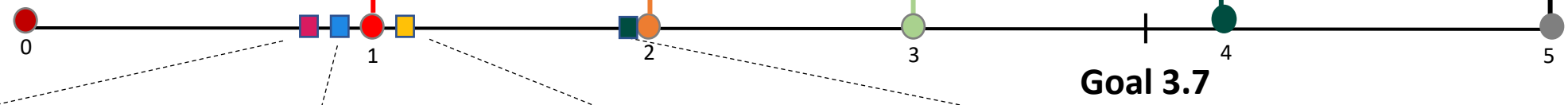
**Extremely low level of maturity**
Independent Small Business, Private Equity, Law Firms

**Small and Midsized Organizations**
Operate in unregulated industries with little to no security

**Average Large Organizations**
Typical lightly regulated industry with bare minimum controls

**Regulated Institutions, States, and Multinationals**
Include states, banks, credit unions and health organizations that spend sufficient funds to secure PII and sensitive data

**Department of Defense**
Nations, federal government, intelligence and military communities that provide the highest level of security to sensitive and restricted data

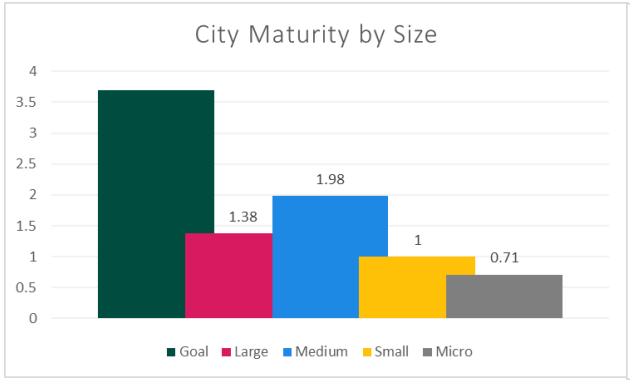


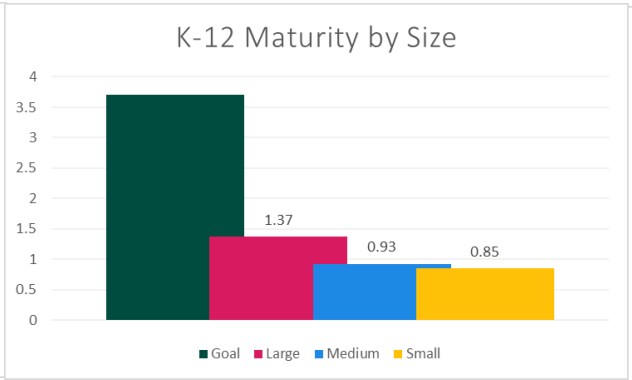

## Cities - 0.76
97 Reporting Cities

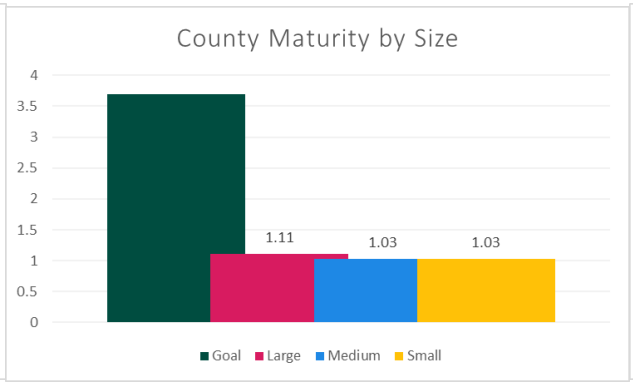
## K12 - 0.97
104 Reporting K12

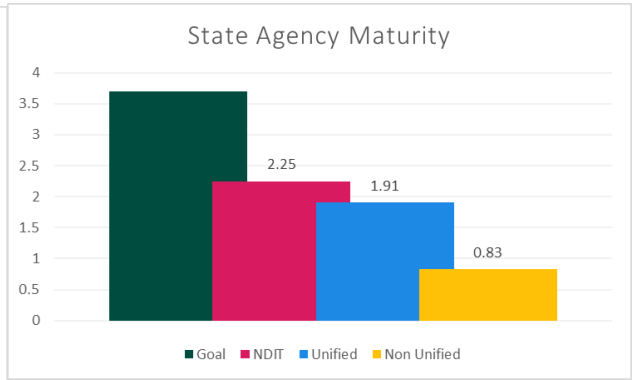
## Counties - 1.05
29 Reporting Counties

## State Agencies - 1.91
ND. Gov.



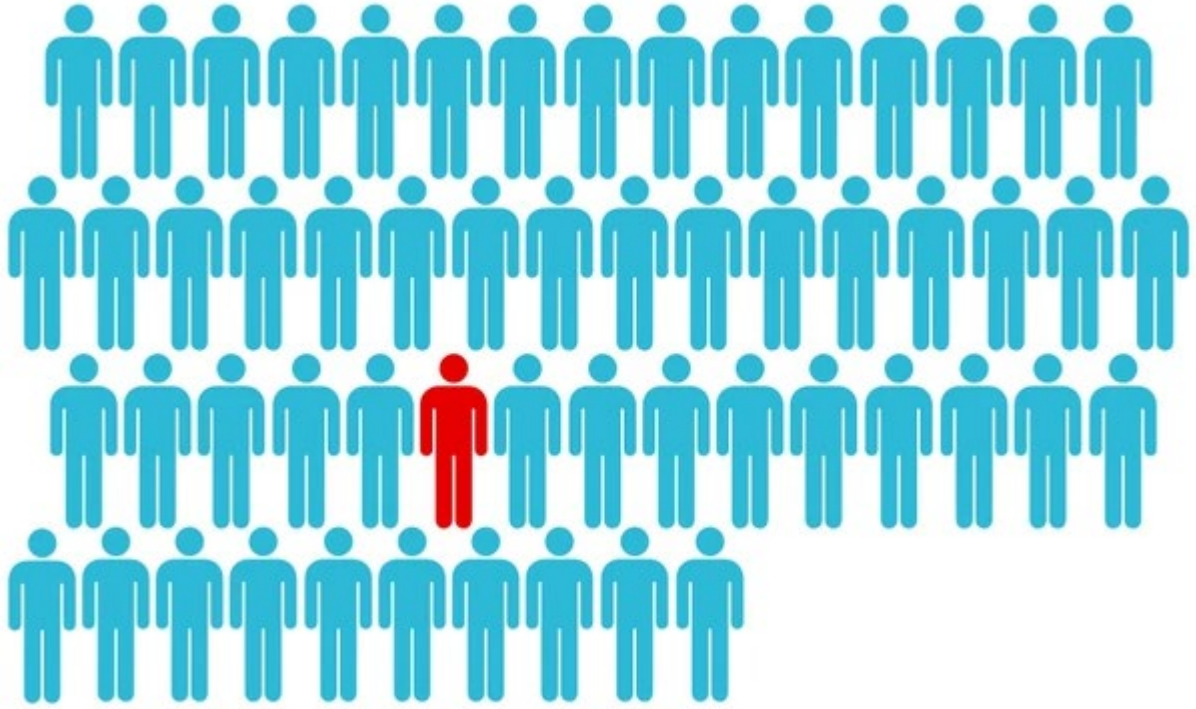



# Most Entities Lack the Needed Cyber Skillset

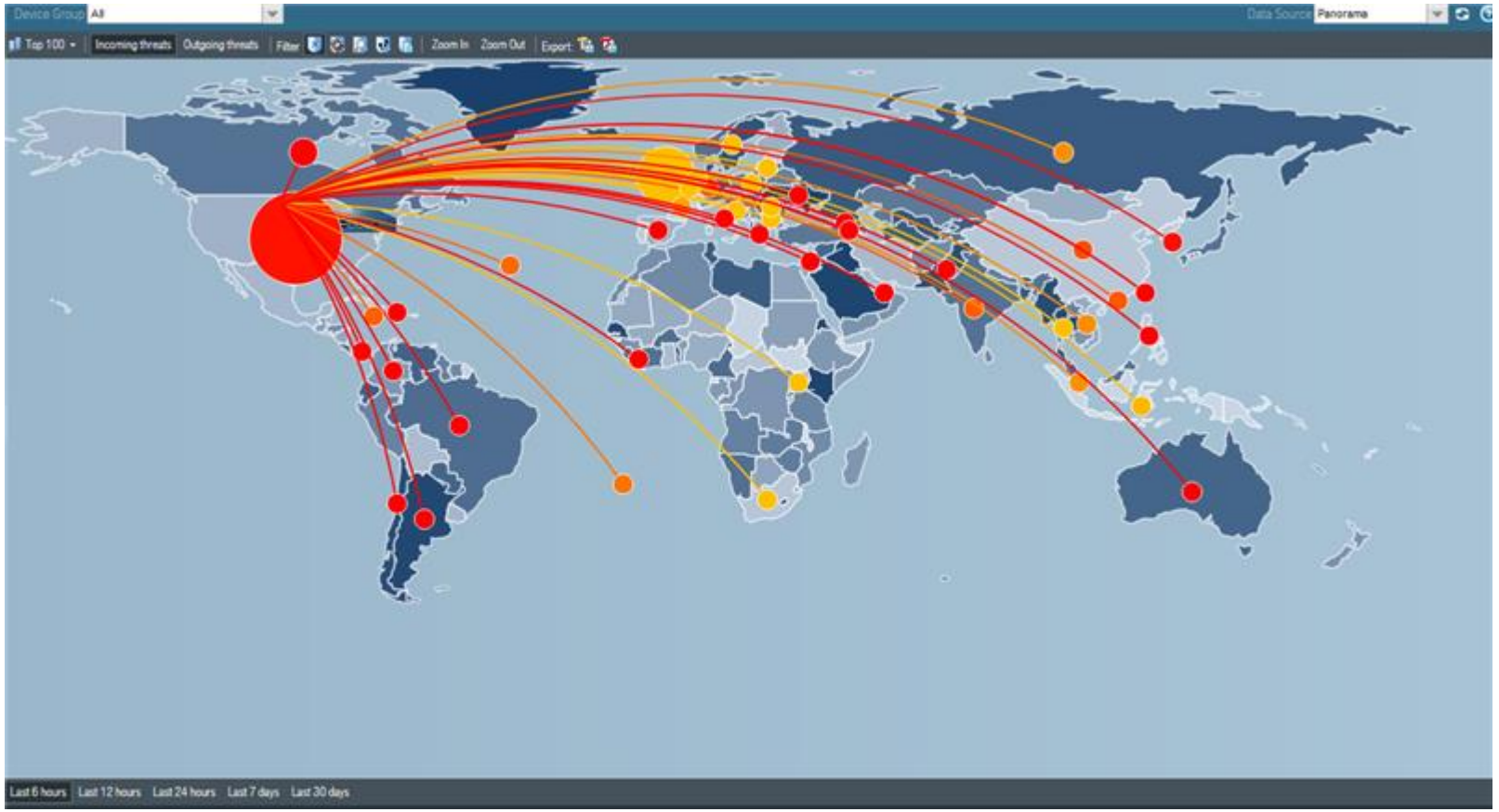
Almost all respondents understood the need to have someone responsible for cybersecurity.

**Only 1% percent of cities, counties, and K-12 schools have full-time cybersecurity staff**

- Ongoing training and experience are needed to properly defend from and respond to security events.
- National Initiative for Cybersecurity Careers and Studies defines 33 specialty areas and 52 different roles for cybersecurity staff



# External Threats




North Dakota receives over 177 Million detected attacks per month[1] from external threats including:

- Nation States,
- Corporate Espionage, and
- Organized Crime Syndicates.

1. Based on ¼ Sampling of 2020 Firewall logs from June 2020, August 2020, October 2020, and Last 30 days (as of December 20, 2020) - Logs available in appendix

# Risk Calculations

Risk Formula:

*1 Year Risk = [(629 PSDs *Exposure Factor) * Average Cost of Ransomware Response] + Average Cost of State Damages

*Risk per biennium = Yearly Risk * 2

Where…

- Exposure Factor: 46% for US Public Sector Ransomware Exposure[1]
- Average Response Cost: $1,090,489 Average (50/50 payed & unpaid)[2]
  - Ransom not payed $732,520
  - Ransom payed $1,448,458
- Average Cost of State Damages: $8,000,000 damages to government per ~160,000 Assets[3]

So…

[(629 * 46%) * ($1,090,489)] + $8,000,000 = Yearly Risk: $323,522,087.26

And…

Risk per biennium = $647,044,174.52

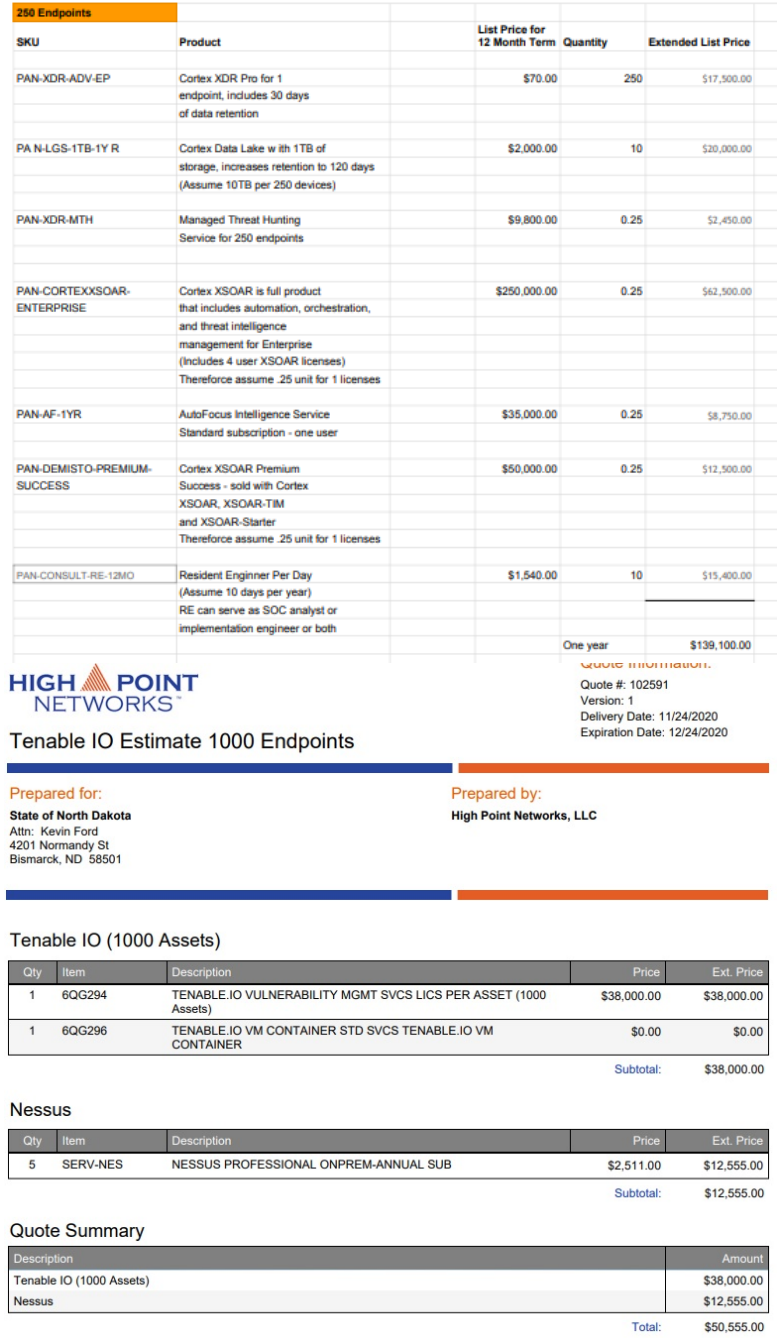
1. Based on 46% exposure reported for Government Entities From: THE STATE OF RANSOMWARE 2020 Results of an independent study of 5,000 IT managers across 26 countries; Sophos Security (May 2020). https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
2. Based on average cost to mitigate attack for both payed and unpaid ransoms from: THE STATE OF RANSOMWARE 2020 Results of an independent study of 5,000 IT managers across 26 countries; Sophos Security (May 2020). https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
3. Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts; Baltimore Sun (May 2019). https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html

# Tool Cost Calculations Per PSD

$149,000 Per Organization Per Year

- $ 118,000.00 for Endpoint Detection and Response (Per Organization Per Year)
  - Quoted Palo Alto Networks11/24/2020
- $31,000 for Asset Vulnerability Management (Per Organization Per Year)
  - Quoted Highpoint Networks 11/25/2020

1. Methodology: Price is lowest quote from quotes provided directly by the vendor and 2 retailers for the same products provided by NDIT security. Does not include the cost of integration or support. Assumes average 270 endpoints per municipal organization.



250 Endpoints

| SKU | Product | List Price for 12 Month Term | Quantity | Extended List Price |
|---|---|---|---|---|
| PAN-XDR-ADV-EP | Cortex XDR Pro for 1 endpoint, includes 30 days of data retention | $70.00 | 250 | $17,500.00 |
| PA N-LGS-1TB-1Y R | Cortex Data Lake w ith 1TB of storage, increases retention to 120 days (Assume 10TB per 250 devices) | $2,000.00 | 10 | $20,000.00 |
| PAN-XDR-MTH | Managed Threat Hunting Service for 250 endpoints | $9,800.00 | 0.25 | $2,450.00 |
| PAN-CORTEXXSOAR-ENTERPRISE | Cortex XSOAR is full product that includes automation, orchestration, and threat intelligence management for Enterprise (Includes 4 user XSOAR licenses) Thereforce assume .25 unit for 1 licenses | $250,000.00 | 0.25 | $62,500.00 |
| PAN-AF-1YR | AutoFocus Intelligence Service Standard subscription - one user | $35,000.00 | 0.25 | $8,750.00 |
| PAN-DEMISTO-PREMIUM-SUCCESS | Cortex XSOAR Premium Success - sold with Cortex XSOAR, XSOAR-TIM and XSOAR-Starter Thereforce assume .25 unit for 1 licenses | $50,000.00 | 0.25 | $12,500.00 |
| PAN-CONSULT-RE-12MO | Resident Enginner Per Day (Assume 10 days per year) RE can serve as SOC analyst or implementation engineer or both | $1,540.00 | 10 | $15,400.00 |
| | | | One year | $139,100.00 |

HIGH POINT NETWORKS

Quote #: 102591
Version: 1
Delivery Date: 11/24/2020
Expiration Date: 12/24/2020

Tenable IO Estimate 1000 Endpoints

Prepared for:
State of North Dakota
Attn: Kevin Ford
4201 Normandy St
Bismarck, ND 58501

Prepared by:
High Point Networks, LLC

Tenable IO (1000 Assets)

| Qty | Item | Description | Price | Ext. Price |
|---|---|---|---|---|
| 1 | 6QG294 | TENABLE.IO VULNERABILITY MGMT SVCS LICS PER ASSET (1000 Assets) | $38,000.00 | $38,000.00 |
| 1 | 6QG296 | TENABLE.IO VM CONTAINER STD SVCS TENABLE.IO VM CONTAINER | $0.00 | $0.00 |
| | | | Subtotal: | $38,000.00 |

Nessus

| Qty | Item | Description | Price | Ext. Price |
|---|---|---|---|---|
| 5 | SERV-NES | NESSUS PROFESSIONAL ONPREM-ANNUAL SUB | $2,511.00 | $12,555.00 |
| | | | Subtotal: | $12,555.00 |

Quote Summary

| Description | Amount |
|---|---|
| Tenable IO (1000 Assets) | $38,000.00 |
| Nessus | $12,555.00 |
| Total: | $50,555.00 |

# Labor Cost Assumptions Per PSD

- At least $180,000 per County/City/K-12 District per Year
  - 1.44 FTE per organization to use the tools and respond to findings[1]
  - Assumed IT FTE Cost of $125,000 Per Year

1. Based on industry average of 1 analyst per 189 devices average for small organizations from: Osterman Research - Osterman Research - The Evolving State of Network Security, 2018, Cited by InfoSecurity group (September 2018). https://www.infosecurity-magazine.com/news/security-staffing-low-in-midsized/

# Firewall Event Sampling

| | Sept | Aug | June |
|---|---|---|---|
| Flood | | 174,540,000 | 213,930,000 |
| Vuln | | 15,250,000 | 20,360,000 |
| Scan | | 2,760,000 | 3,350,000 |
| Spyware | | 1,040,000 | 2,020,000 |
| Packet | | 64,290 | 43,830 |
| virus | | 9,900 | 6,390 |
| Wildfire | | 13,730 | 11,010 |
| | | 193,677,920 | 239,721,230 |

| | Oct | Last 30 days |
|---|---|---|
| **Flood** | 40,230,000 | 259,008,000 |
| **Vuln** | 1,580,000 | 16,880,000 |
| **Scan** | 549,110 | 2,240,000 |
| **Packet** | 4,670 | 354,360 |
| **Spyware** | 4,210 | 304,300 |
| **Virus** | 8 | 23,810 |
| **Wildfire** | 27 | 12,830 |
| **Total** | **42,368,025** | **278,823,300** |

# Citations


- THE STATE OF RANSOMWARE 2020 Results of an independent study of 5,000 IT managers across 26 countries; Sophos Security (May 2020). https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
- Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts; Baltimore Sun (May 2019). https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html
- Osterman Research - The Evolving State of Network Security, 2018, Cited by InfoSecurity group (September 2018). https://www.infosecurity-magazine.com/news/security-staffing-low-in-midsized/
- Code.org North Dakota State Fact Sheet (2018). https://code.org/advocacy/state-facts/ND