Item No. 5
Town of Atherton

CITY COUNCIL STAFF REPORT – STUDY SESSION

TO: **HONORABLE MAYOR AND CITY COUNCIL**

THROUGH: **GEORGE RODERICKS, CITY MANAGER**

FROM: **ANTHONY SUBER, DEPUTY CITY MANAGER / CITY CLERK**

DATE: **MAY 5, 2021**

SUBJECT: **CYBERSECURITY REPORT**

RECOMMENDATION

Receive an informational report on the Town's cybersecurity protection measures as recommended by the San Mateo County Grand Jury report on ransomware.

BACKGROUND

On October 7, 2020, the San Mateo County Grand Jury released a report entitled "Ransomware: It Is Not Enough To Think You Are Protected" which advised local agencies to evaluate cybersecurity measures and protocols. The report also directed agencies to ensure adequate measures are taken to mitigate risks and provide recovery options. The report recommended the Town instruct the Information Technology Division (IT) to assess cybersecurity strategies, address possible shortcomings, and report to Council on this assessment. On December 16, 2020, Council approved a response letter to the San Mateo County Grand Jury, signed by Mayor Lewis. The Town agreed with the Grand Jury findings and committed to addressing the recommendations.

This informational Study Session is being held to comply with the Grand Jury's recommendations. Another recommendation was to engage with cyber-defense resources from the Department of Homeland Security Cybersecurity & Infrastructure Security Agency (DHS-CISA). Atherton's IT personnel are experienced with performing cyber hygiene assessments and have coordinated routine cyber assessments for the Town in partnership with CISA. These will be coordinated monthly intrusion tests. IT will continue to monitor available options from DHS-CISA for enhanced services. Lastly, over the coming year, IT will be taking additional cybersecurity measures and enhancing our cybersecurity strategic efforts. A component of those measures includes implementing Managed Detection and Response (MDR) software. This is a cybersecurity service that will provide intrusion detection of malware and malicious activity within our network and assist in rapid incident response to eliminate those threats with consistent remediation actions. The Town's expected MDR will combine a technology solution with external outsourced security analysis.

The Grand Jury report include some specific concerns, which included the following:

1. System Security. This includes firewalls, anti-malware/antivirus software, use of network segmentation or subnets, strong password policies, and updating / patching regularly.
2. Backup & Recovery. In the event of an attack, can you shut down your system quickly? What is being backed up, how it is being backed up, when are backups run, and where are the backups being stored? Have backups been tested? Can you fully restore a server from a backup?
3. Prevention. Turning on email filtering, setting up message rules to warn users, providing employee training on phishing and providing a reporting system to flag suspect content.

Each item listed are important components of a robust cybersecurity program, and the Town has all of these in place. There are however several additional measures to be outlined. Cybersecurity should involve a comprehensive program of policies and governance, strong technical defenses and software, and appropriate action / staff response.

We can begin with defining some important terms for reference:

- Cybersecurity – technologies, processes, and practices designed to protect networks, devises, programs, and data from attach, damage, or unauthorized access.
- Cyberattacks – efforts aimed at accessing, changing, or destroying sensitive information, extorting money, or interrupting business operations.
- Phishing – email claiming to be from a legitimate source meant to induce individuals to provide sensitive information or as a vector for malware.
- Malware – "malicious software" designed to damage or disrupt computer systems, capture data, and/or extort payment (e.g. ransomware).
- Ransome – a type of malware on a host machine that prevents access to data until a ransom is paid.

This report will not detail the various types of malware and cyberattacks including phishing but instead focus on our approach to cybersecurity. Cybersecurity is an important component of our overall risk management. This approach is influenced and based on guidance provided by the Center for Internet Security (CIS). CIS is a nonprofit organization of cybersecurity professionals whose mission is to "identify, develop, validate, promote, and sustain best practice solutions for cyber defense and build and lead communities to enable an environmental of trust in cyberspace". CIS proved a set of 'CIS Controls™' which are "a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks". CIS Controls are based on the US Government National Institute of Standards and Technology (NIST) Cybersecurity Framework. CIS Controls provide a helpful and more easily actionable guide based on the NIST standard. The NIST Cybersecurity Framework was initiated in 2013 by Presidential Executive Order directing NIST to work with stakeholders to develop the voluntary framework in a collaboration between industry and government. NIST is used by government agencies at all levels, as well as private organizations. NIST has worked to develop cybersecurity risk frameworks for voluntary use. The Frameworks are designed to identify, "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls," that may be voluntarily adopted.

There are 20 CIS Controls organized into three basic groups: Basic, Foundational, and Organizational. Each Control has several Sub-Controls which are comprehensive and detailed. There are also three "Implementation Groups" based on the size and complexity of organizations which are used to determine which Sub-Controls should apply. The remainder of this report will briefly list CIS Controls under the Basic group and highlight examples of Sub-Controls within that list which IT has in place as appropriate for the Town. This is not intended to be an exhaustive description of our application of all Controls and Sub-Controls, and certain specifics and details are omitted from this public document for security purposes.

The follow CIS Controls are referred to as Basic.

CIS Control 1: Inventory and Control of Hardware Assets. IT maintains a detailed hardware inventory and utilizes a centralized remote management tool for Town Personal Computers (PCs). Efforts are made to ensure unauthorized or unmanaged devices are not given access to the network. Per policy, departments are expected to purchase technology through IT, or at a minimum consult with IT prior to any technology hardware purchases.

CIS Control 2: Inventory and Control of Software Assets. IT maintains an applications list and documentation library for all known software. IT is in the process of auditing our current licenses and programs to have the ability to run reports of software installed on Town computers. Per policy, departments are to purchase software through IT, or at a minimum consult with IT prior to any software purchases. IT seeks to avoid software that is unsupported by the vendor, or that does not have regular security updates. However, this is an area where the use of certain necessary software for Town functions makes us unable to fully address security concerns.

CIS Control 3: Continuous Vulnerability Management. IT utilizes anti-malware/antivirus scanning tools and performs anti-malware/antivirus scanning of Town computers. IT deploys operating system and other software patches to all PCs in a timely manner through a remote management tool.

CIS Control 4: Controlled use of Administration Privileges. IT controls IT administrative accounts, changes default passwords on systems, and follows other best practices including the use of strong passwords and multi-factor authentication. IT limits access to elevated administrative privileges and scripting tools. Of note, this is a primary method for attackers to spread inside a target.

CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers. IT utilizes PC imaging tools to establish standard configurations and maintain secure PC images. Mobile devices (iPads) used for Town business purposes are centrally managed. However, other mobile devices (individual mobile phones) are user managed for user convenience.

CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs. This Control includes the activation of system audit logging and logs being collected, managed, and analyzed. This requires significant resources, and specific expertise is required to perform most analyses. To address this Control with limited resources, IT will be purchasing and implementing Managed Detection and Response (MDR) services, described earlier in this report.

The Controls referenced here under the Basic group are amongst those used to form a strong framework for protecting the Town's digital assets. These Controls are helpful when considering where to apply limited technology resources, what policies to implement, and where organizational change can occur to make work practices more cyber-secure.

These Controls and practices are not a one-sized fits all solution to cybersecurity and there is no magic solution for cybersecurity IT to deploy to protect the Town. This is an ongoing and evolving program that includes policies and governance, technical defenses, and diligent staff actions. It is a collaborative effort that includes ongoing attention, adherence to policies, cyber trainings, and being cyber-aware. Our users must be equipped with current information, best practices, and appropriate policies as the first line of defense to these cyber threats.

POLICY FOCUS

The policy focus for this item is a discussion and overview of the Town's cybersecurity program. This is an informational session and there are policy areas for Council discussion and review. The Grand Jury required that the Town respond to the findings and recommendations within the report. Staff provided those responses at the December 16, 2020 meeting and received Council support.

FISCAL IMPACT

There is no budget impact associated with this action.

PUBLIC NOTICE

Public notification was achieved by posting the agenda, with this agenda item being listed, at least 72 hours prior to the meeting in print and electronically. Information about the project is also disseminated via the Town's electronic News Flash and Atherton Online. There are approximately 1,200 subscribers to the Town's electronic News Flash publications. Subscribers include residents as well as stakeholders – to include, but be not limited to, media outlets, school districts, Menlo Park Fire District, service provides (water, power, and sewer), and regional elected officials.

ATTACHMENTS

1. Cybersecurity Presentation

Town of Atherton

Cybersecurity Report Presentation

May 5, 2021

AGENDA/OVERVIEW

- Grand Jury findings and recommendations
- Cybersecurity risks
- Cybersecurity Framework
- Types of attacks and protective measures
- Additional considerations

Grand Jury Findings & Recommendations

- Findings emphasizing the threat and costs of ransomware to public entities, and the importance of cybersecurity assessments and plans

- The Town agreed with all 8 findings

- Recommendation that the Town direct the IT Department to assess cybersecurity strategies, address any shortcomings, and make a report to the Council

- This report is one of the final steps in the process of addressing these recommendations

Grand Jury Findings & Recommendations

Specific concerns of the grand jury:

1. System Security. This includes firewalls, anti-malware/antivirus software, use of network segmentation or subnets, strong password policies, and updating/patching regularly

2. Backup & Recovery. In the event of an attack, can you shut down your system quickly? What is being backed up, how it is being backed up, when are backups run, and where are the backups being stored? Have backups been tested? Can you fully restore a server from a backup?

3. Prevention. Turning on email filtering, setting up message rules to warn users, providing employee training on phishing and providing a reporting system to flag suspect content

Cybersecurity Risks & Types of Attacks

What are types of Phishing:

- **Mass Phishing** – Mass, large-volume attack intended to reach as many people as possible
- **Spear Phishing** – Targeted attack directed at specific individuals or companies using gathered information to personalize the message and make the scam more difficult to detect
- **Whaling** – Type of spear phishing attack that targets "big fish," including high-profile individuals or those with a great deal of authority or access
- **Clone Phishing** – Spoofed copy of a legitimate and previously delivered email, with original attachments or hyperlinks replaced with malicious versions, which is sent from a forged email address so it appears to come from the original sender or another legitimate source
- **Advance-Fee Scam:** Requests the target to send money or bank account information to the cybercriminal

Cybersecurity Risks & Types of Attacks

Ransomware: malware that restricts access to a computer until a ransom is paid

- Cryptos, Wipers, Lockers

Cybersecurity Risk Examples

From: service@paypal.com
Subject: Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

Click here to verify your account

Actual link URL: http://80.179.238.73/ ... paypal/

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

Thank you for using PayPal! The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at http://www.paypal.com/securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

Bank of America Higher Standards

Military Bank

Dear Customer,
Bank of America Military Bank is doing a 20$ Reward Survey. Bank of America Military Bank will add $20 credit to your account just for taking part in our quick 5 easy question survey. To get advantage of this offer click on the link below.

< URL REMOVED >

This message has been sent only to our special customers.

Thank you,

Bank of America Military Bank Customer Service

Reply Reply All Forward
Thu 11/16/2017 9:14 AM
Amazon Gifts <amazon_gifts@priimerewardsusa.com>
[BULK] Last day to use your $50 from Amazon.com is TODAY
To Helpdesk
This message was sent with Low importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

Bing Maps + Get more apps

amazon

Hello helpdesk,

Your previous order with Amazon.com qualified your account to receive a reward worth over $50.

Activate below your new GIFT

ACTIVATE REWARD > >

Amazon Prime

Amazo Account #959643-861238
Gift #: 188642

Please note that this message was sent to the following e-mail address: helpdesk@acorntechcorp.com

See more about Amazon Gifts.

From: VoiceMail System [mailto:newvoicemai@www.ee.co.uk]
Sent: Monday, November 05, 2018 7:11 AM
To: Chris Lu <Chris.Lu@acorntech.com>
Subject: (800) 829 4933 left you a voice message

Microsoft Office 365

A voice message was received from **+1 (800) 829 4933** on **November 05, 2018** at **09:58 AM**.

Message ID: **VOM-05-11-2018** | Length: **0:52 secs**

Listen to Voice Message Now

https://www.tinyurl.com/november5voicemail2018
Click or tap to follow link.

You can save this message here: Recorded Voice-Message.wav

Thank you.

Microsoft

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052 USA

You are receiving this email because you have subscribed to Microsoft Office 365.
Copyright 2017 Microsoft Corporation Privacy Statement

Cybersecurity Framework

Basic Controls:

- Inventory and Control of Hardware Assets
- Inventory and Control and Software Assets
- Continuous Vulnerability Management
- Controlled Use of Administrative Privileges
- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, etc.
- Maintenance, Monitoring and Analysis of Audit Logs

Protective Measures

Multi-factor authentication

- Password policies
- Change after 90 days
- Avoid weak (e.g.): 123456, Password, Letmein, abc123
- Email filtering

Cyber-awareness training

- Users are our first line of defense
- Ongoing awareness program

Endpoint management

- Anti-malware, scanning, updates

System monitoring

- Network, server, services

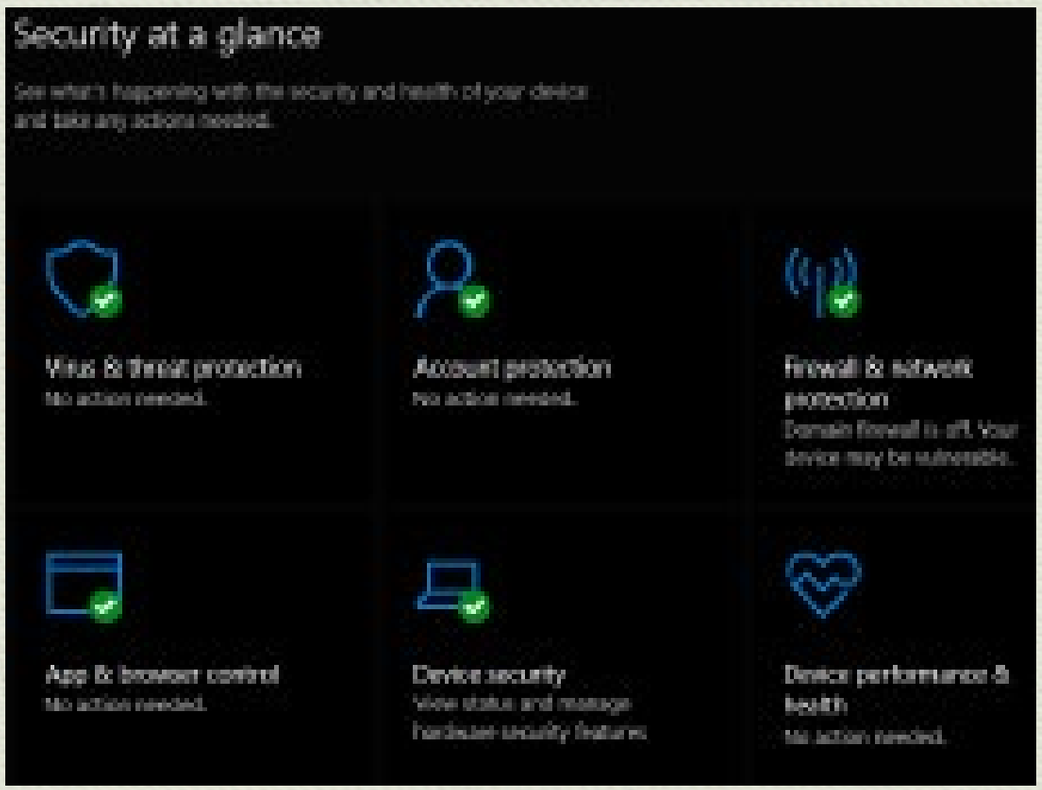
City policies, practices

- Independently verify any change request coming through email

Protective Measures

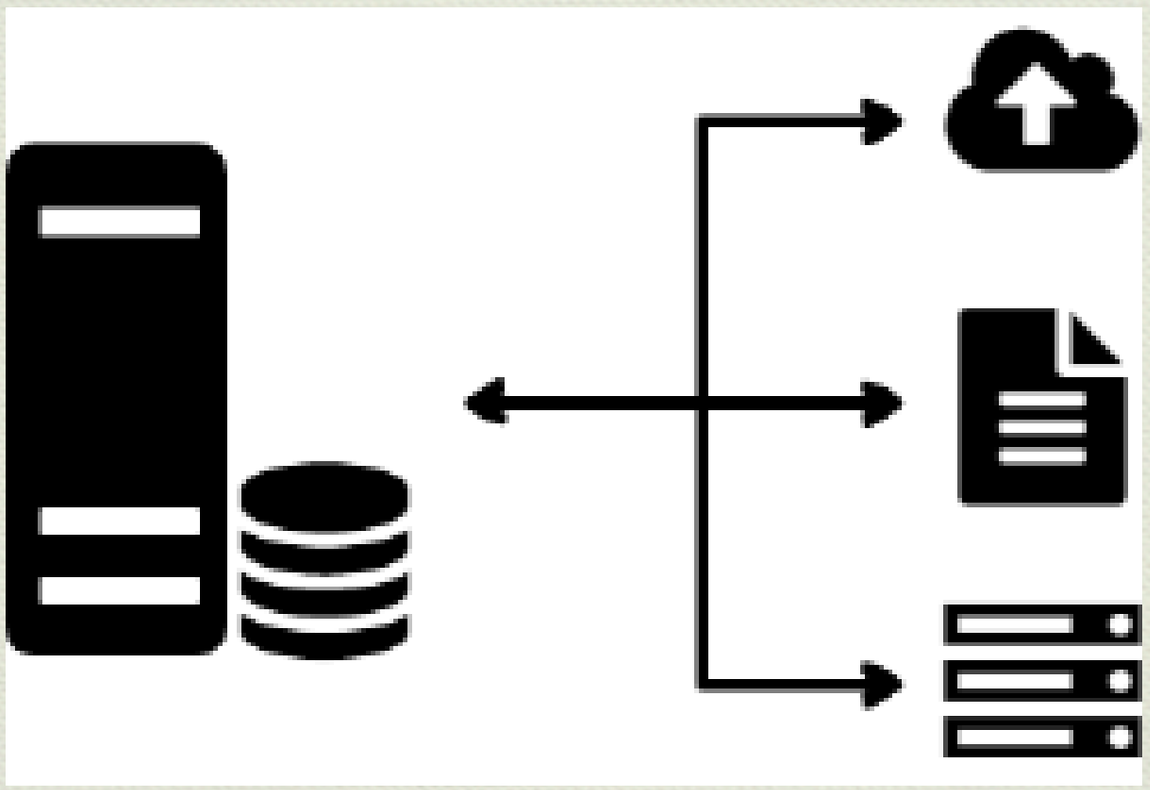
Virus / malware protection

- Updated anti-malware software
- Malware removal tools



Backup and recovery

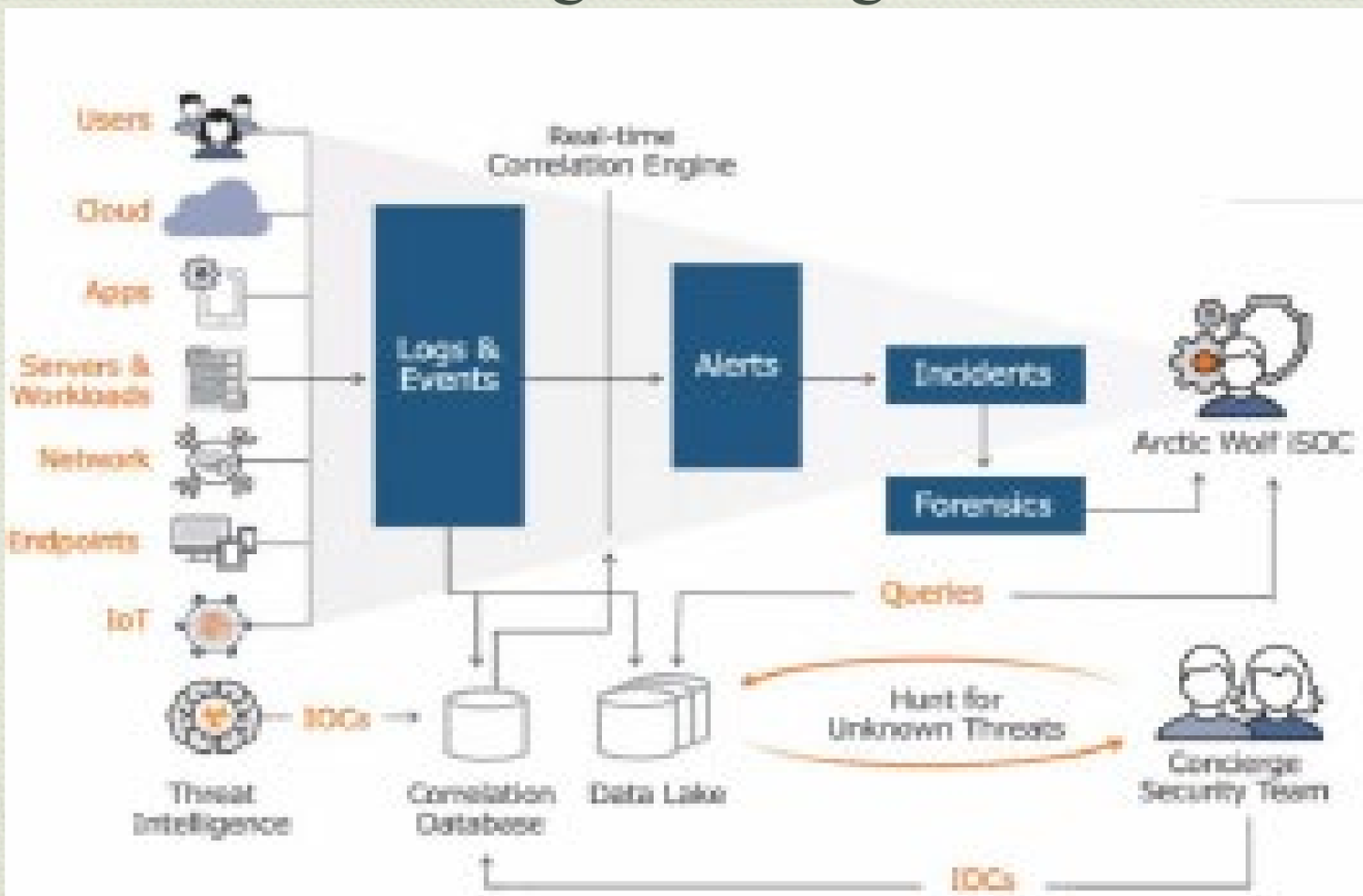
- Regular, automated backups
- 3-2-1 model



Protective Measures

Managed detection and response (MDR)

- Threat searching and mitigation



~100B Raw Observations/day
~35B Parsed and Analyzed/day
~50K Incident Investigations/day
~400-700 Escalated Incidents/day

Real-time Correlation

- Analyze billions of events
- Real-time correlation against IOCs
- Reduced false positives

Forensics

- Search and research quickly
- Construct blast zone analysis and remediate

Hunt

- Hunt for unknown threats with deep analytics and human expertise
- Identify new IOCs to improve monitoring

Additional Considerations

- Expanded Cybersecurity awareness training
- Continued adoption of Cloud
- Stronger collaboration on technology selection
- Explore enhanced cybersecurity policies and standards
- Leverage expert partners

Questions

Mohammad Ahmed, IT Manager (Contract via Interwest)

mahmed@interwestgrp.com

Joe Keegan, Senior Systems Analyst (Contract via Interwest)

jkeegan@interwestgrp.com

Atherton IT Helpdesk

iwsupport@ci.atherton.ca.us