

# Quarterly Cybersecurity Review (QCR)

---

Q2 2018

Manny Landron



# Agenda

- ✓ Q2 Accomplishments
- ✓ Cybersecurity Roadmap (2018/19)
- ✓ Vulnerability Management
- ✓ Network Security Monitoring
- ✓ Threat Monitoring – Phishing
- ✓ Threat Monitoring – Malware
- ✓ Threat Monitoring – Command and Control
- ✓ Website Filtering
- ✓ Endpoint Protection
- ✓ AS400 Password Resets



# Key Q2 Accomplishments

- ✓ Successfully responded to a targeted phishing campaign that attempted to harvest IAT user IDs and passwords.
- ✓ Published and communicated the End User Cybersecurity Policy and achieved 100 percent acknowledgment within 45 days.
- ✓ Completed planning phase for cybersecurity project, Phase II – IV.
- ✓ Upgraded end point protection solution to address security and performance issues.
- ✓ Upgraded network security monitoring solution to address performance issues and further tuned configuration and rule set.
- ✓ Upgraded vulnerability management solution to address security and performance issues and added an additional scan engines.
- ✓ Completed IFIC cybersecurity due diligence review.



- ✓ Completed external web site and infrastructure inventory. Participated in ISC2 panel discussion discussing ransomware and attended RSA Security conference.
- ✓ Drafted comprehensive AS400 operations run book.
- ✓ Drafted secure coding standards for .NET.

# Cybersecurity Roadmap

## 2018

Q4

- ✓ Implement ServiceNow Change Management
- ✓ Annual Risk Assessment–Encryption (Email)
- ✓ IFIC Limited Compliance Assessment
- ✓ Multifactor Authentication (O365)
- ✓ Deploy Internet gateway (Zscaler)
- ✓ Complete periodic applications access reviews
- ✓ Incident Response Plan

Q3

- ✓ Firewall Migration
- ✓ Deploy Intrusion Detection / Prevention System
- ✓ Data Retention Program
- ✓ Penetration Test

# Cybersecurity Roadmap

## 2019

Q1

- ✓ Multifactor Authentication (VPN)
- ✓ Implement O365 and Microsoft Azure Auditing
- ✓ Deploy Microsoft Intune Mobile Device Management
- ✓ Third Party Risk Management

Q2

- ✓ Encryption (Offsite Backups)
- ✓ Encryption (File Transfer)
- ✓ Application Security Vulnerability Management

Q3

- ✓ Encryption (Removable Media)
- ✓ Annual cybersecurity program assessment
- ✓ Privacy Policy
- ✓ Business Impact Assessment (BIA)

# Vulnerability Management

## Q1

- ✓ **Internal Vulnerabilities:** Reduced internal exploitable vulnerabilities from 2,355 in January 2018 to 900 as of March 29, 2018, a net reduction of 1,455 or 62 percent of exploitable vulnerabilities.
- ✓ **External Vulnerabilities:** Reduced external vulnerabilities by 53 percent from 129 on January 2018 to 61 as of March 29, 2018.
- ✓ Include total vulnerabilities next time

## Q2 (Trend )

- ✓ **Internal Vulnerabilities:** Increased internal exploitable vulnerabilities from 900 in March 2018 to 1,139 as of June 30, 2018, **a net increase of 239 or 26 percent** of exploitable vulnerabilities compared to Q1 2018.
- ✓ **External Vulnerabilities:** **Increased external vulnerabilities by 77 percent** from 61 on March 2018 to 108 as of June 30, 2018.

Our annual goal is to address 20 percent of exploitable internal security vulnerabilities by the end of CY 2018 using January 2018 security assessment results as a baseline.



# Network Security Monitoring

- ✓ Collected over **15 billion events**.
    - January: 6.7 billion events
    - February: 4.9 billion events
    - March: 3.8 billion events
  - ✓ Processed over **2,300 alerts**.
    - January: 853
    - February: 766
    - March: 696
  - ✓ Sample alerts
    - Unauthorized external vulnerability scans or probes
    - Accounts added to administrative groups
    - Accounts locked out
    - VPN connections from outside the country
    - Multiple VPN connections with two different IP addresses within a 2 hour period
  - ✓ Responded to one security incident.
- ✓ Collected over 18.5 billion events.
    - April: 6.6 billion events
    - May: 6.2 billion events
    - June: 5 billion events
  - ✓ Processed over 2,400 alerts.
    - April: 1,366
    - May: 716
    - June: 334
  - ✓ Sample alerts – Include counts next time
    - Unauthorized external vulnerability scans or probes
    - Accounts added to administrative groups
    - Accounts locked out
    - Internal accounts failing to login to a common host (mostly related to scripts failing for developer)
    - Internal accounts successfully authenticating to multiple hosts in a short time.

**Note:** One analyst processes about 40 security alerts per day on average, 2 – 4 hours per day.

# Threat Monitoring - Phishing

## Q1/Q2 - Automated

- ✓ Prevented **469** potential phishing attacks YTD.

January: 42  
February: 10  
March: 160  
April: 160  
May: 67  
June: 30

Q1: **8 emails** contained malicious content

## Q1/Q2 - Manual (Trend )

- ✓ Analyzed **1238** suspicious email messages YTD.

January: 147  
February: 99  
March: 125  
April: 514  
May: 208  
June: 145

Q2: **612 emails** contained malicious content.

Note: One analyst processes about 40 security alerts per day on average,  
1 – 2 hours per day, unless there is an associated incident.

Phishing– Blocked connections to known fake, malicious sites that are intent on stealing passwords, credit card numbers, social security numbers or other personally identifiable information if we click on an associated link within an email and enter the information within web forms hosted on the site.



# Threat Monitoring - Malware

Prevented **8,207** potential Malware compromises YTD.

## Q1

JAN

664

FEB

1.3K

MAR

2.2K

**Total: 7.6K**

## Q2 (Trend ↓)

APR

2.2K

MAY

1.3K

JUN

543

**Total: 5.5K**

Malware – Blocked connections to known malicious sites that statically host or that redirect us to sites that may automatically install malware on our computers without our knowledge. In some cases, the malware installation does not require the end user to possess elevated privileges.

# Threat Monitoring – Command & Control

Q1

JAN

2


FEB



MAR



Total: 117

Q2 (Trend )

APR



MAY



JUN



Total: 140

**Command and Control** – Blocks connection attempts to sites known to deliver malware, in the event that a file on your computer attempts to connect to a known malicious site that hosts command and control malware typically associated with bots. A "bot" is a type of malware that allows an attacker to take control over an affected computer. Also known as "Web robots", bots are usually part of a network of infected machines, known as a "botnet", which is typically made up of victim machines that stretch across the globe.

# Website Filtering

**224.3  
MILLION**

Web requests made by IAT  
during Q2 2018 that passed  
through the web proxy.

## No Q1 Data

because proxy was not  
implemented until  
March 2018.

Blocked 11.2M requests during Q2 2018

April: **4.2M**

Blocked by category: 3.9M  
Block by reputation: 58.5K  
Blocked unauthorized software downloads: 201K

May: **5M**

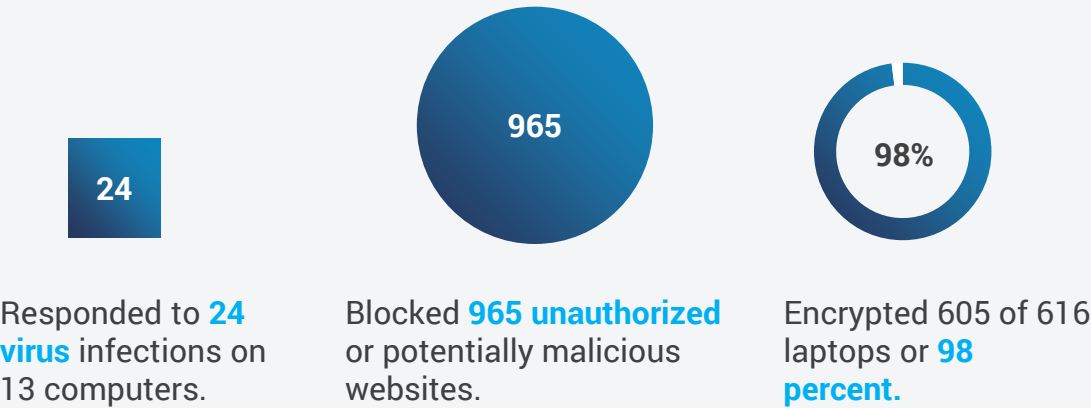
Blocked by category: 4.1M  
Block by reputation: 41K  
Blocked unauthorized software downloads: 754K

June: **2M**

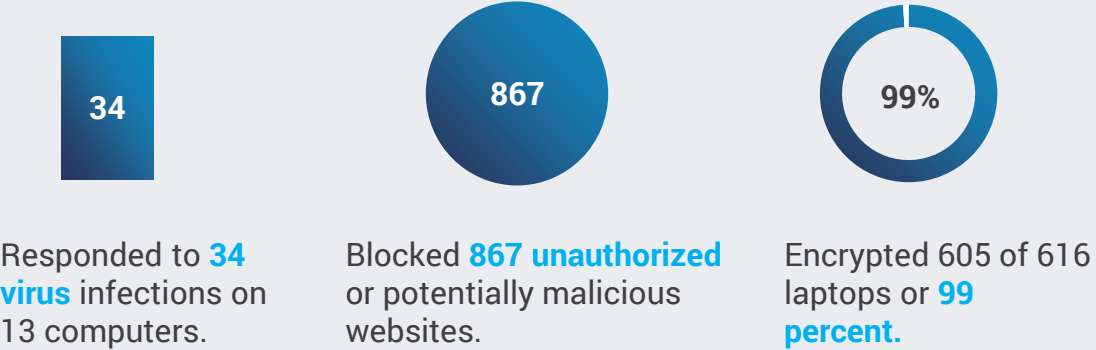
Blocked by category: 1.3M  
Block by reputation: 72K  
Blocked unauthorized software downloads: 667K

# Endpoint Protection

## Q1 2018



## Q2 2018 (Trend ↑)

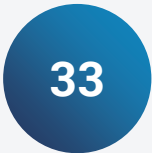


# AS400 Password Resets


**Q1 2018** (Total: 144)



Agents / Broker Resets



Agents / Broker Resets

**Q2 2018** (Total: 108) (Trend )



Agents / Broker Resets



Agents / Broker Resets

Total Resets : 252

Total Agent/Broker Resets: 204

Total IAT Internal: 48

# Thank You!

---

Questions? | Discussion

