State of Cyber Security

2021

Supporting the OCTA mission by protecting OCTA networks, systems, and the confidentiality of data.

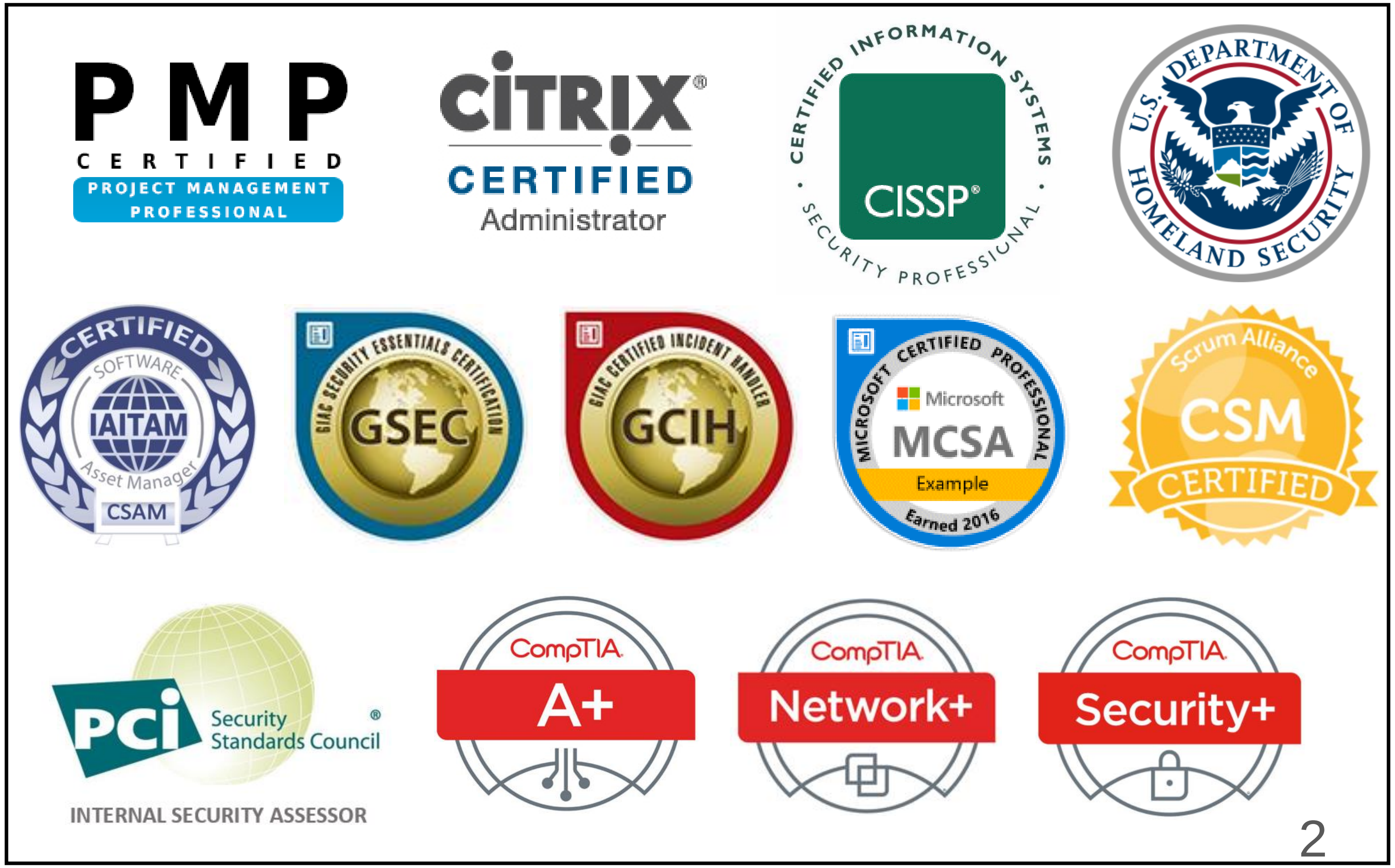
OCTA

Cyber Security Team Members

- **Michael Cardoza**
  - Cyber Security Manager
    - DHS held Security Clearance (SECRET)
- **Phil Moncada**
  - Cyber Security Analyst, Sr
- **Sean Slaven**
  - Cyber Security Analyst, Sr
- **Samantha Robert**
  - Cyber Risk Manager

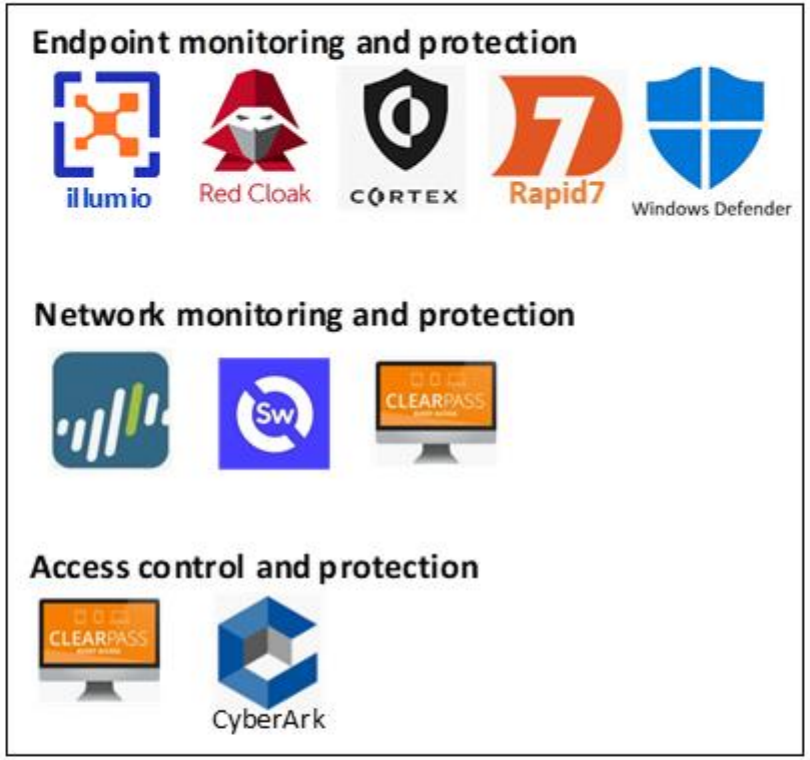
Government / Private / Department of Defense

Cyber Security: 40 YRS **IT**: 32 YRS

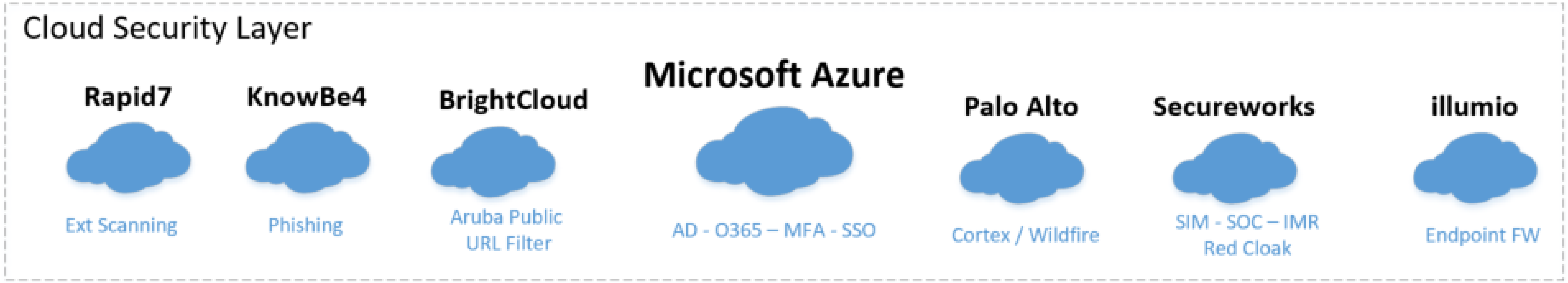

PMP CERTIFIED PROJECT MANAGEMENT PROFESSIONAL
CITRIX® CERTIFIED Administrator
CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL CISSP®
U.S. DEPARTMENT OF HOMELAND SECURITY
CERTIFIED SOFTWARE IAITAM Asset Manager CSAM
GIAC SECURITY ESSENTIALS CERTIFICATION GSEC
GIAC CERTIFIED INCIDENT HANDLER GCIH
MICROSOFT CERTIFIED PROFESSIONAL Microsoft MCSA Example Earned 2016
Scrum Alliance CSM CERTIFIED
PCI Security Standards Council® INTERNAL SECURITY ASSESSOR
CompTIA A+
CompTIA Network+
CompTIA Security+

Cybersecurity Overview

- Cloud / Network / Endpoint
- Monitor, Detect, Alert, and Protect
- SIEM* / 24-hr Security Operations Center
- Vulnerability Scanning and Remediation
- Machine Learning / Behavior Analysis
- Access Management
- Multi-Factor authentication /Single Sign-on
- Network Segmentation
- Email / Phishing Protection & Training


Endpoint monitoring and protection
illumio
Red Cloak
CORTEX
Rapid7
Windows Defender
Network monitoring and protection
Sw
CLEARPASS
Access control and protection
CLEARPASS
CyberArk

- *Security information and event management



2020 Accomplishments

Cyber Security Accomplishments

1. Remote work security reviews and enhancements
2. Cybersecurity integrations
3. Completion of multiple vulnerability programs
4. Completion of 1st year mandatory security training
5. Automated processes
6. 300 percent increase in AI* monitored networked devices
7. Integration of Cloud, perimeter, and endpoint monitoring and protection.
8. Third-party & Internal audits, risk assessments, and testing
9. Data security best practices

MDR IMPLEMENTATION

RAPID7 IMPLEMENTATION

VULNERABILITY REMEDIATION

USER TRAINING & AWARENESS

AUDIT SUPPORT & RESPONSE

DATA CENTER SECURITY

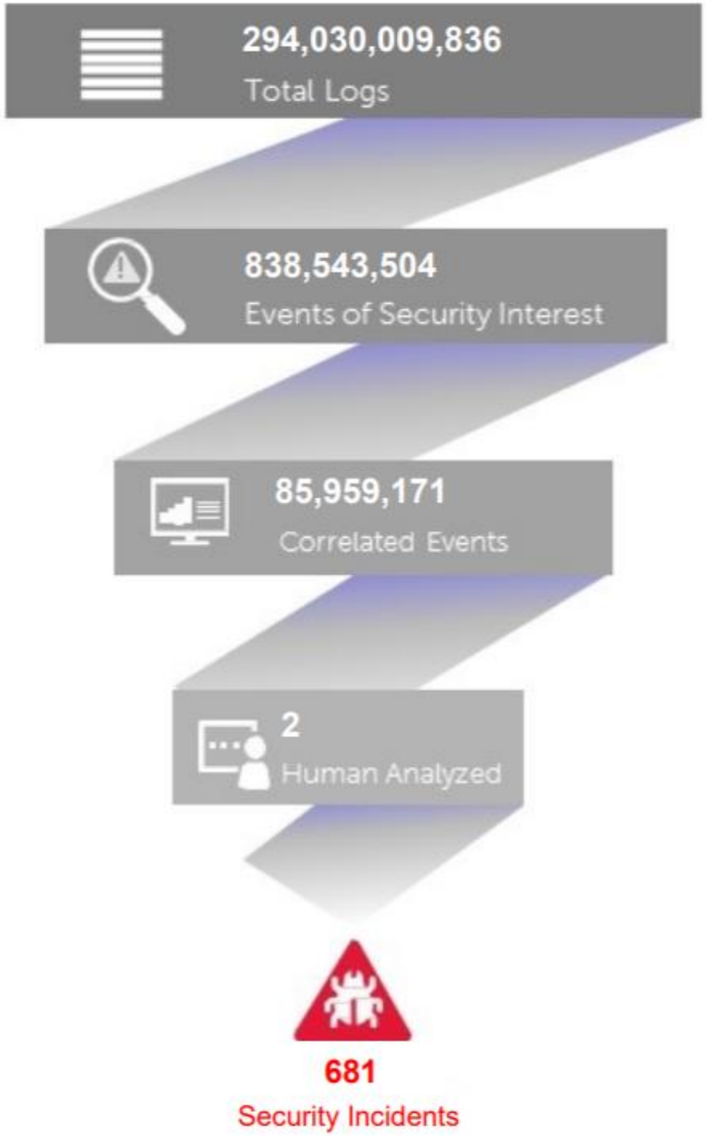
*Artificial Intelligence

Monitor, Detect, and Respond

Over 294 billion logs reviewed in 2020

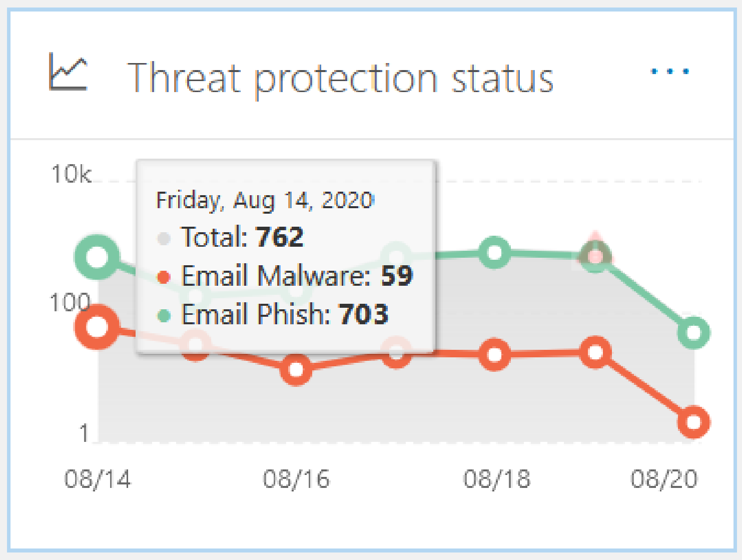
- AI powered Security Solutions
- Cloud, Perimeter, & Endpoint monitoring
- 24/7 Security Operations Center
- Threat Hunting and Intelligence
- Incident Response and Support

Zero Loss of Data



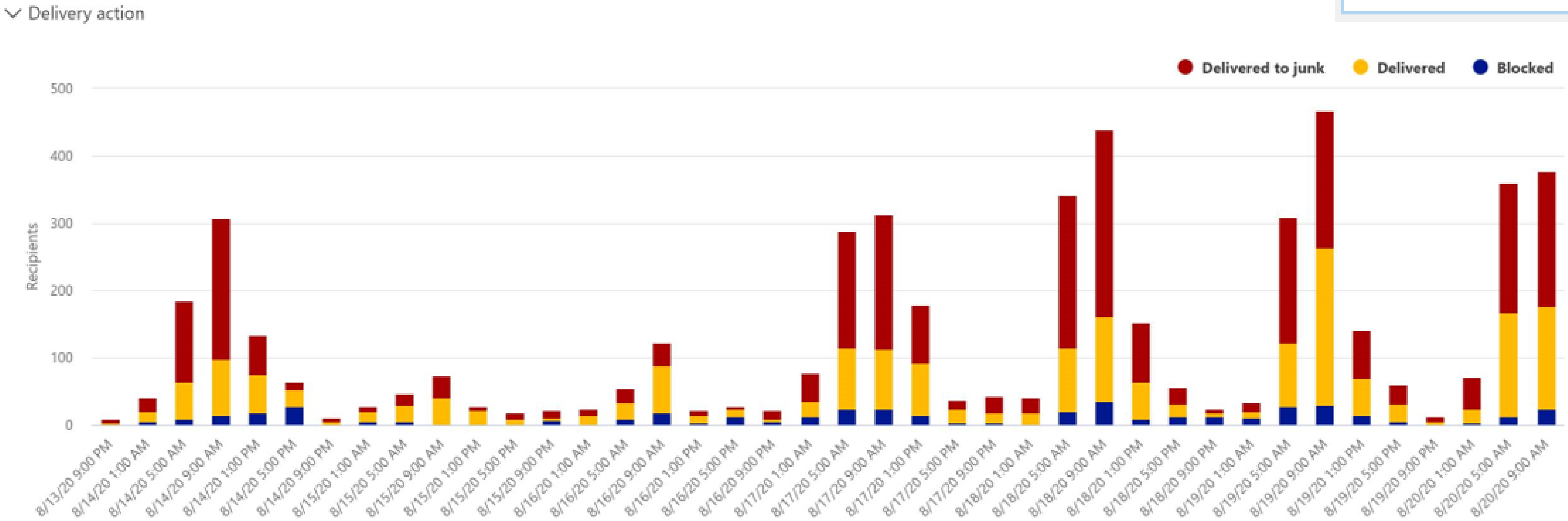
Cloud Security

- AI based automation
- Monitoring of logins and risky behavior in Microsoft 365
- Advanced threat protection for email
- Anti-phishing, impersonation, and malware protection
- Multi-factor authentication and Single Sign-on
- Conditional Access



Threat protection status

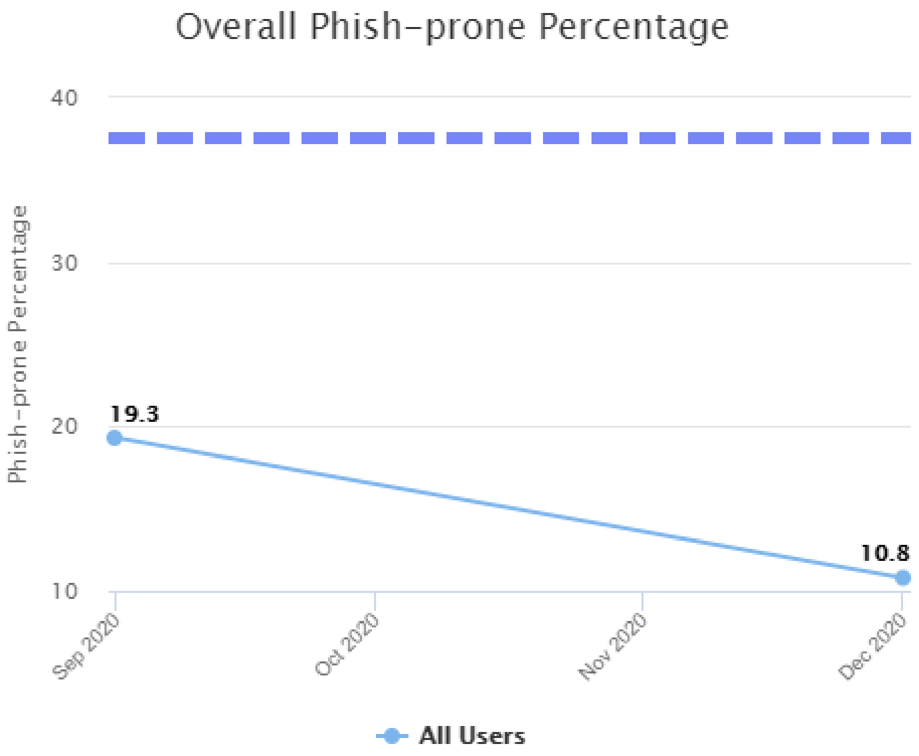
Friday, Aug 14, 2020
- Total: **762**
- Email Malware: **59**
- Email Phish: **703**

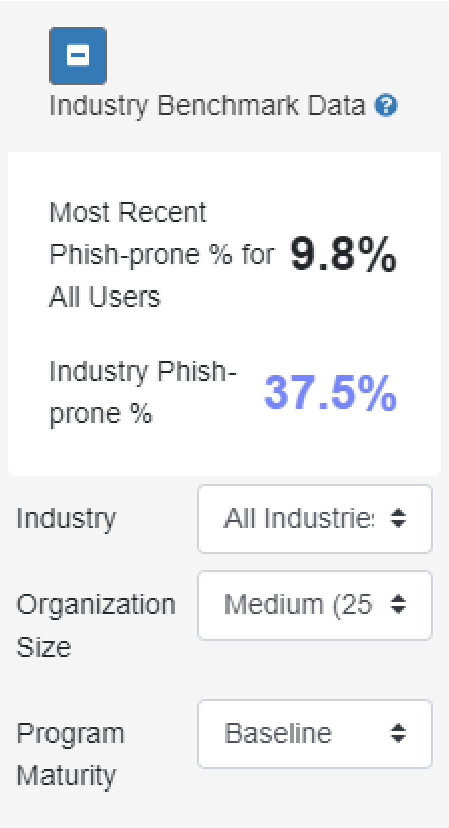


Security Awareness Program

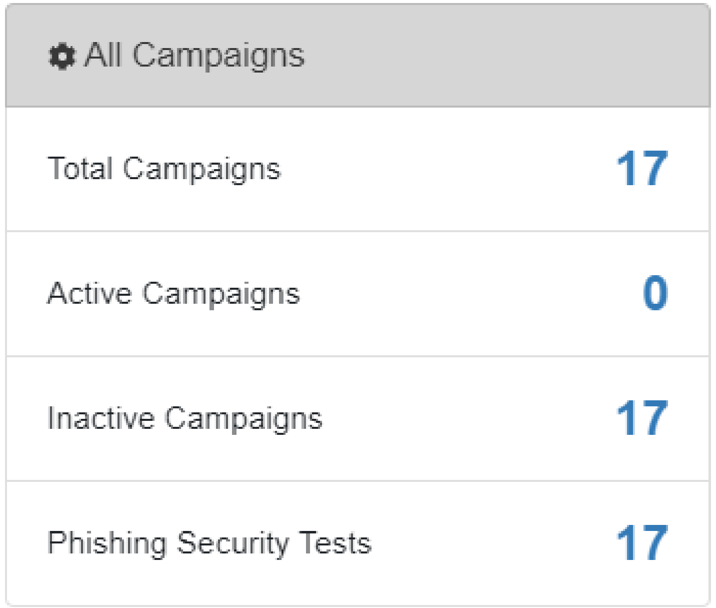
- OCTA employees are an important part of our security program
- Phishing is an important part of an attacker's process
- Training remains a focus of our Security Awareness Program

91 percent of cyberattacks begin with a spear phishing email (KnowBe4 2020)




Industry Benchmark Data

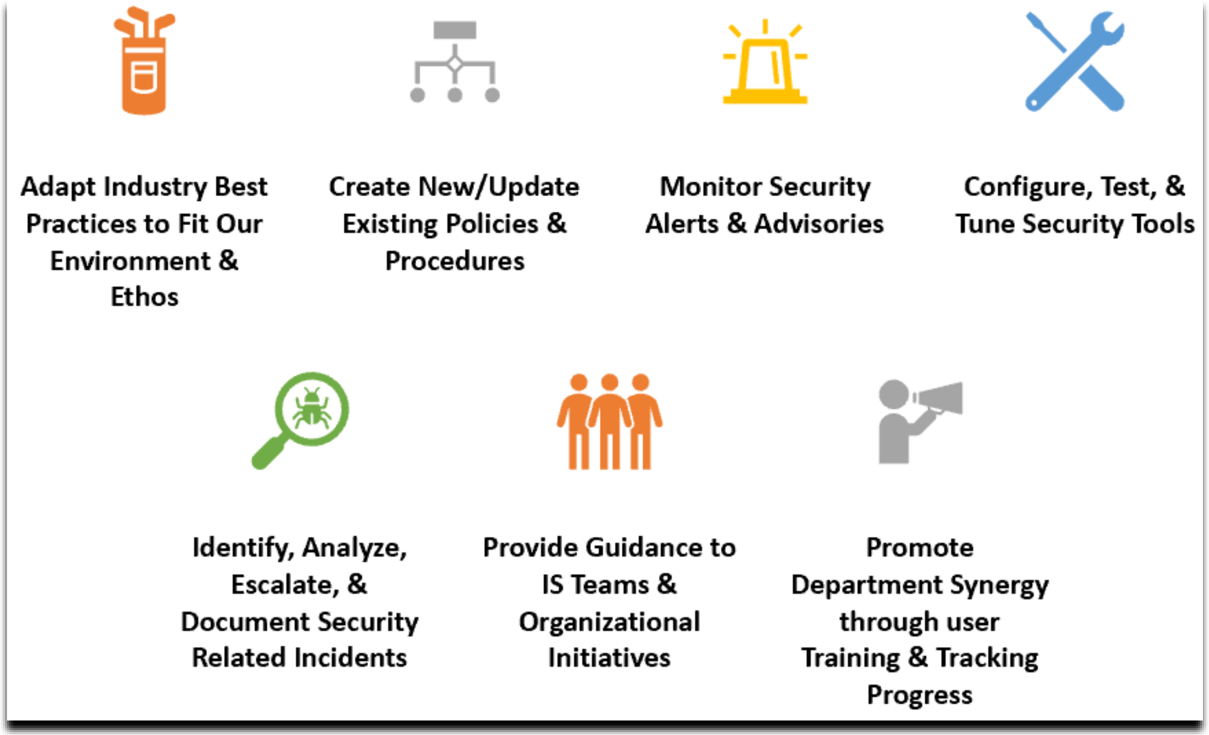
Most Recent Phish-prone % for All Users	9.8%
Industry Phish-prone %	37.5%
Industry	All Industrie:
Organization Size	Medium (25
Program Maturity	Baseline


All Campaigns	
Total Campaigns	17
Active Campaigns	0
Inactive Campaigns	17
Phishing Security Tests	17

2021 Cybersecurity Goals

Cyber Security Goals

1. Identify and remediate vulnerabilities and threats
2. Review and update policies and procedures
3. Maintain scanning, monitoring, and auditing responsibilities
4. Provide regular OCTA cybersecurity training and awareness
5. Continue Third-party & internal risk assessments
6. Determine and implement security enhancements
7. Test and tune security tools



Adapt Industry Best Practices to Fit Our Environment & Ethos

Create New/Update Existing Policies & Procedures

Monitor Security Alerts & Advisories

Configure, Test, & Tune Security Tools

Identify, Analyze, Escalate, & Document Security Related Incidents

Provide Guidance to IS Teams & Organizational Initiatives

Promote Department Synergy through user Training & Tracking Progress