SMCCCD Cyber Security Initiatives

Department of the CTO - Information Security Office

* Required multifactor authentication for accessing critical services (OneLogin).
* District hosted sites require at least TLS 1.2 with 2048 bit AES encryption (dept of CTO).
* Mandatory Cybersecurity Training for all employees (KnowBe4).
* Malware detection and prevention on all District owned devices (Sophos & Cortex XDR).
* Patching of all District owned devices on weekly basis (JAMF and Quest Kace).
* MDM for MacOS and Windows laptops (JAMF & Absolute).
* 24x7 Security Operations Center (CI Security).
* Continuous online vulnerability scanning (Tenable.IO)
* Continuous security information and event management (Splunk)
* Continuous data loss prevention (Varonis)
* Daily backups with long-term retention, time-lock, and off-site replication (Veeam & ExaGrid)
* Current and evolving disaster preparedness plan for various scenarios (dept of CTO).
* Scanning of all attachments in Outlook (Office 365).
* Scanning of online cloud storage (Cloudlock).
* External email notice and suspicious email alerting tool (Office 365 & Phish Alert).
* Suspicious online behavior reporting process (HR dept).
* 24/7 video surveillance and keycard access of all datacenter locations (dept of Public Safety).
* Environmental monitoring of all datacenter locations (FPO dept).

Graphical user interface, application

Description automatically generated

KnowBe4 training platform showing current progress of 2023 training.

A picture containing graphical user interface

Description automatically generated

Quest Kace patch management showing current patch progress.

Table

Description automatically generated

Quest Kace showing Cortex XDR antivirus installed on Servers.

Graphical user interface, application

Description automatically generated

ExaGrid backup appliance showing data stored and time lock policy.

Graphical user interface, application

Description automatically generated

Users licensed for Office 365 A5 license which includes email security.

Graphical user interface, text, application, email

Description automatically generated

Sample email with warnings regarding external sender and the “Phish Alert” button.

Graphical user interface, application, table

Description automatically generated

Sample Tenable.IO report showing at risk systems

Sample alert from CI Security

From: MS-ISAC SOC <SOC@msisac.org>  
Date: Wednesday, January 18, 2023 at 9:12 AM  
To: Wu, Jiajun <wuj@smccd.edu>, West, Adam C. <westa@smccd.edu>, Jorgensen, David <jorgensend@smccd.edu>, Demissie, Yoseph <demissiey@smccd.edu>, Soo, Aaron <sooa@smccd.edu>, Grewal, Daman <grewald@smccd.edu>  
Cc: SOC\_Supervisor.dl <SOC\_Supervisor.dl@cisecurity.org>, MS-ISAC SOC <SOC@msisac.org>  
Subject: [EXTERNAL]CA - SMCCCD - Multiple Albert Incidents Generated - MS-ISAC Tickets 15860593, 15860592, 15860594

Albert Incident #: 15860593  
Severity: Warning  
MS-ISAC SOC Ticket: 15860593  
Description: Win32/LingyunNet.A CnC Checkin  
Status: NEW  
  
Albert Incident #: 15860592  
Severity: Warning  
MS-ISAC SOC Ticket: 15860592  
Description: Win32/LingyunNet.A Heartbeat  
Status: NEW  
  
Albert Incident #: 15860594  
Severity: Warning  
MS-ISAC SOC Ticket: 15860594  
Description: Win32/LingyunNet.A Heartbeat Response  
Status: NEW  
  
Analysis  
This is a bulk Albert alert notification for affected IP. The logs from each alert have been attached to this email for your review and investigation. Each alert generated will be tracked by its own Ticket ID. A history of each ticket has been included below in the Supporting Details section.  
  
Source IP was logged communicating with destination IP over destination port 801/UDP (source port 65344/TCP). This traffic matches a signature for Win32/LingyunNet.A Heartbeat. The source IP has been seen communicating with malicious files recently per VirusTotal. As this traffic is abnormal and we cannot confirm if it is malicious, we are escalating this for your awareness.

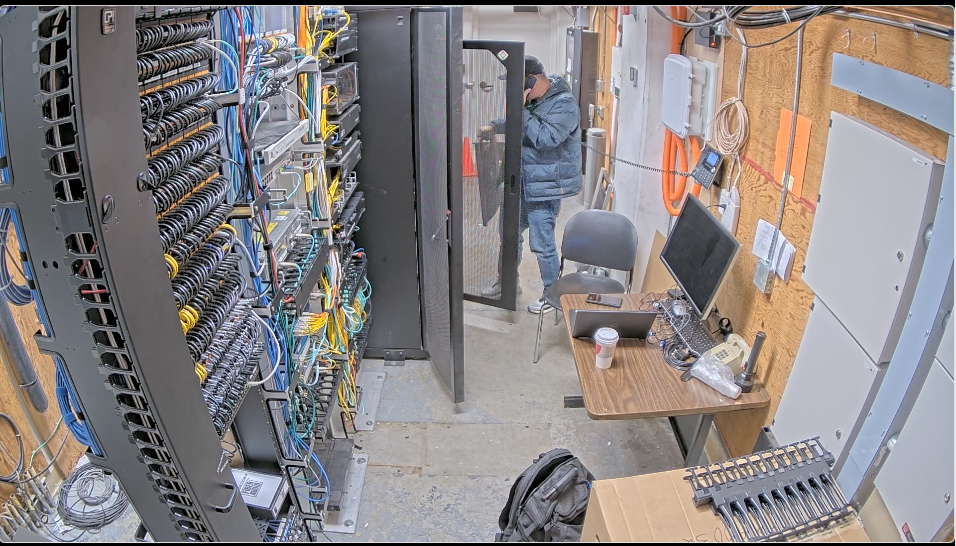


Image of a technician working in Cañada datacenter captured from video