
cisco Live!
ALL IN

The bridge to possible

From ship to shore... Integrations, collaboration, and (securely) taking control beyond the Cisco Secure Email Gateway

Cisco Secure Email

Robert Sherwin, Technical Marketing Engineer, Technical Leader
@igo232

BRKSEC-2288

Cisco Webex App

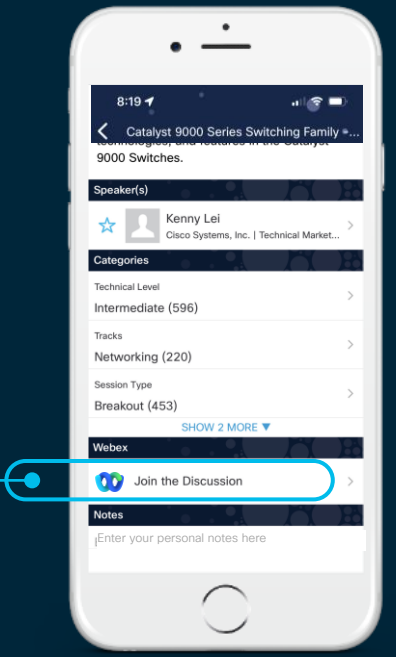
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

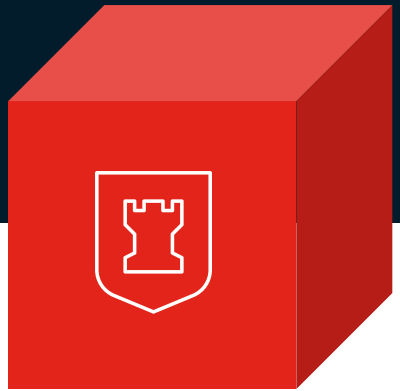
Webex spaces will be moderated by the speaker until June 17, 2022.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2288

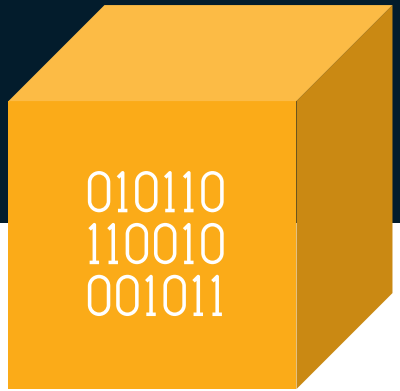
Agenda

1. Fundamental Protections



Drop the obvious attack before the malicious email is delivered.

2. Definition based URL Filtering

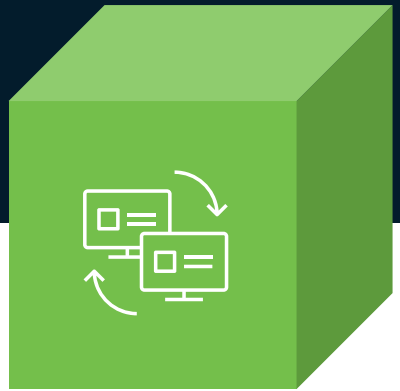


Pragmatically filter unwanted URLs via Talos threat intelligence integration.

3. URL Rewrite & Analysis

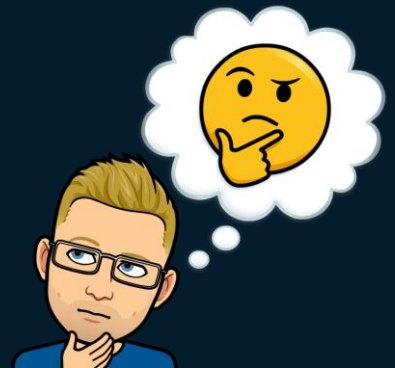
Seamless analysis of URLs that are newly observed or deemed suspicious.

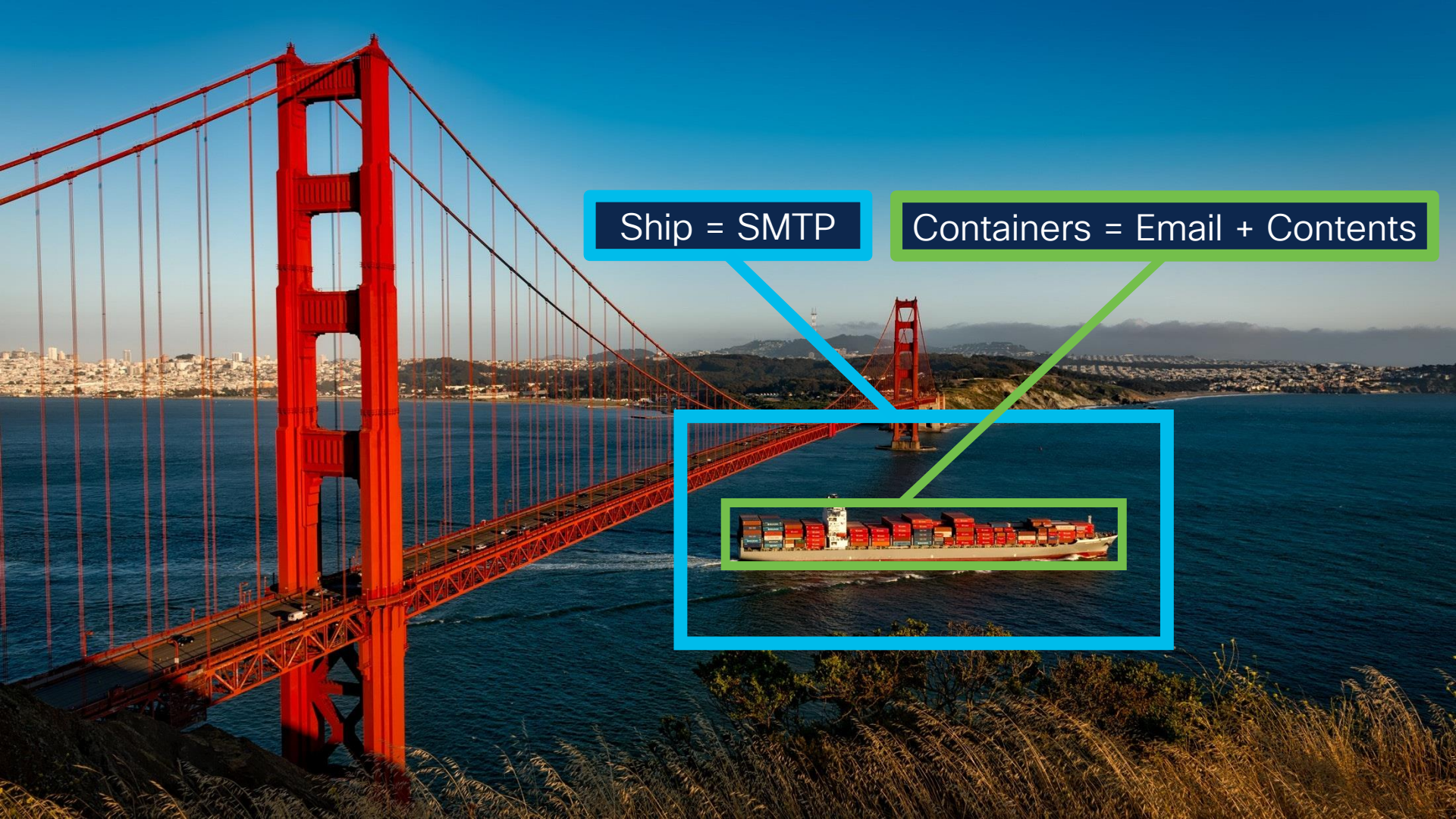
4. Next-level Integrations

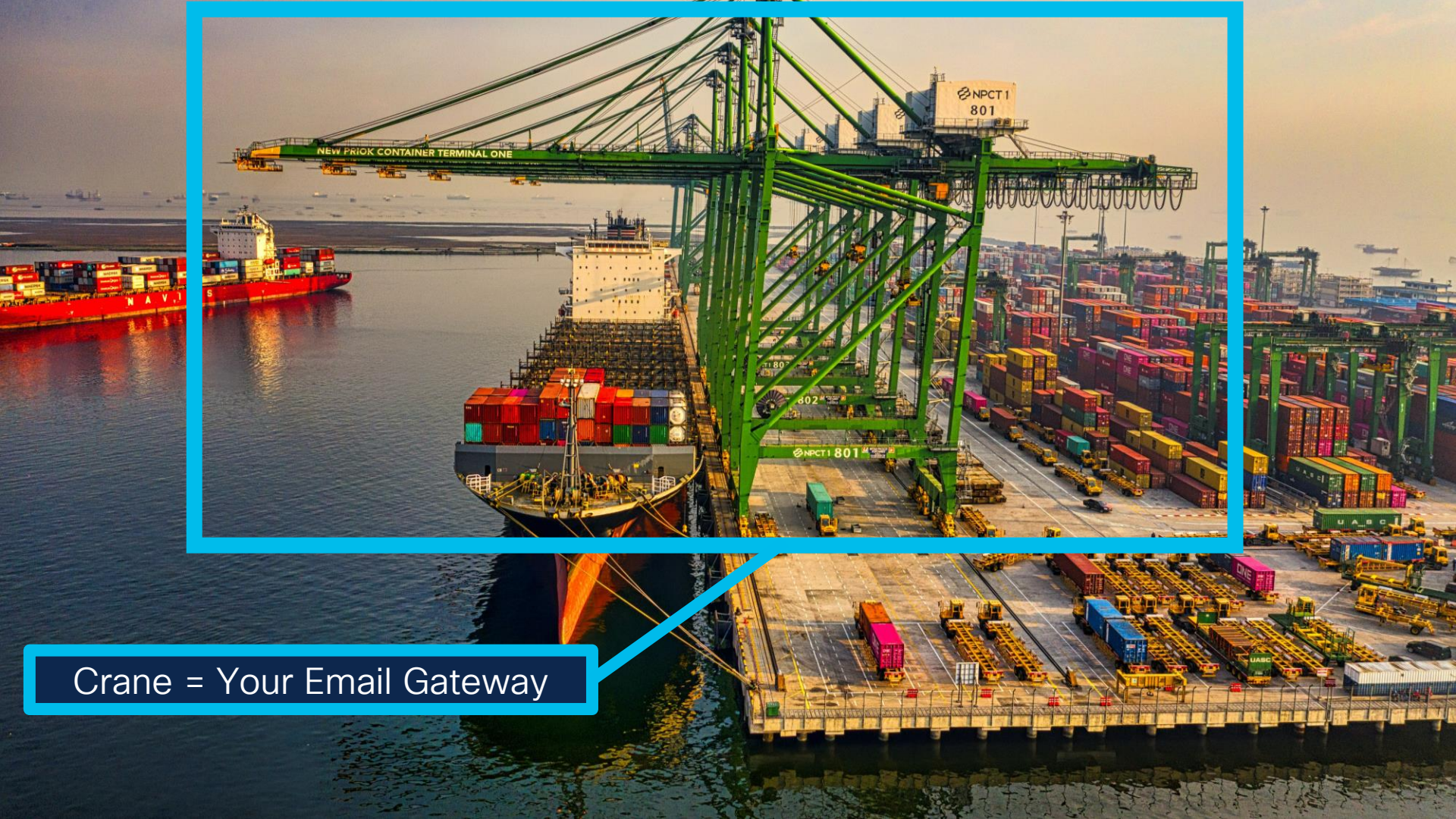


Expand email security defense beyond the Gateway through collaboration.

Ship to shore?




Ship = SMTP
Containers = Email + Contents


NEW PRIOK CONTAINER TERMINAL ONE
NPCT 1
801
802
NPCT 1 801
Crane = Your Email Gateway


Shore (Port) = Your Destination

Cisco Secure Email Gateway/Cloud Gateway Pipeline

Fundamental Protections

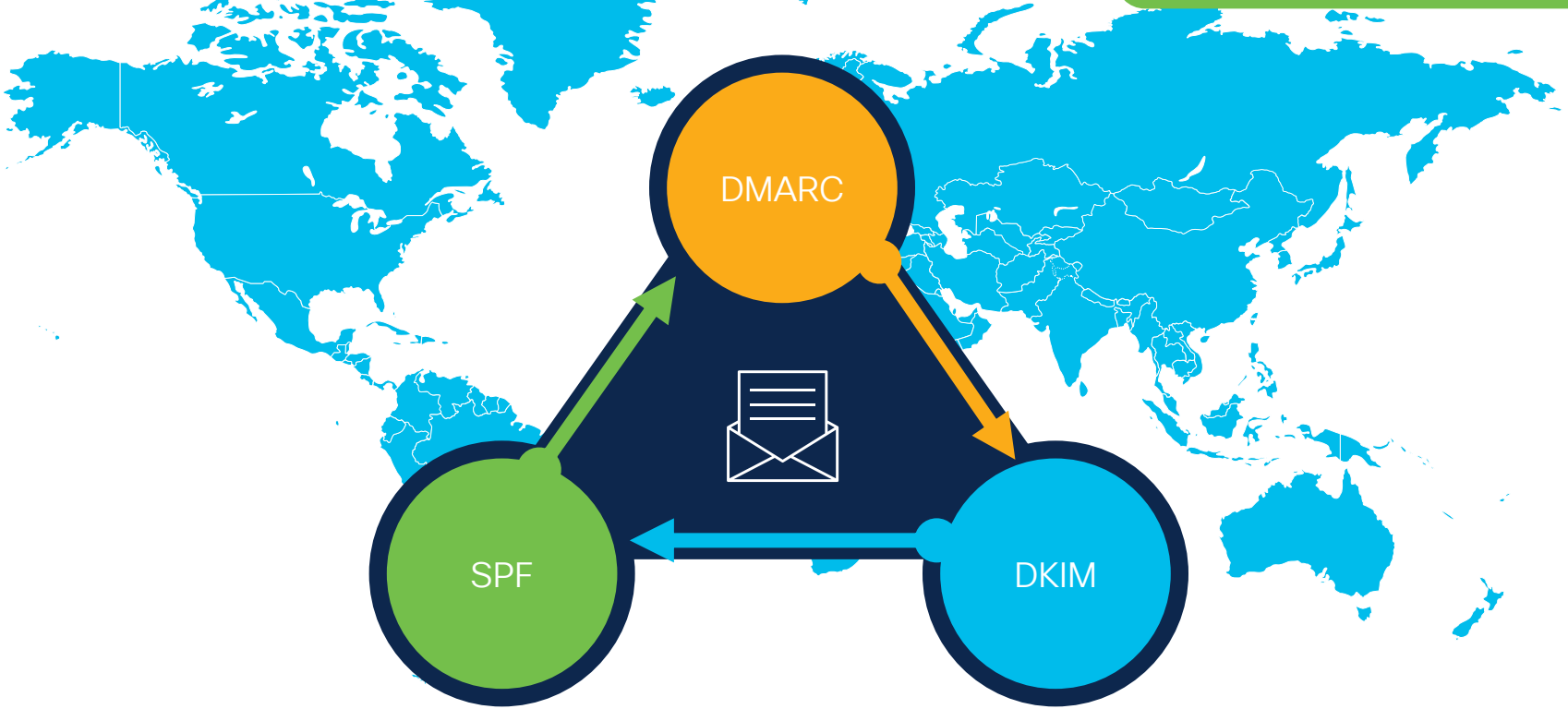
The Force of Talos Intelligence

- IP Reputation
- Host Reputation
- Sender Domain Reputation

Sender Authentication Trifecta

Breakout Tip:

cs.co/brksec-2327



Example of check_domain.py

Breakout Tip:

cs.co/check_domain

```
┌──(kali㉿kali)-[~/scripts/check_domain]
└─$ python3 check_domain.py -d nhl.com
================================================
[+] A Record : 8.20.73.150
[.] Record not found AAAA in domain 'nhl.com'.
[+] MX Record : 10 esa1.hc3405-36.iphmx.com.
[+] MX Record : 10 esa2.hc3405-36.iphmx.com.
[+] TXT Record : "google-site-verification=_yup8HiUiA_uo4bg2hQoij63dP4oSvmtRcNE6q7i6NQ"
[+] TXT Record : "jon7qv7to8b2vkf0733c5mob78"
[+] TXT Record : "adobe-idp-site-verification=b1a9bddb8ba893901680eb1190803ff68ea897d8f363d2b7fd166a0d16297e13"
[+] TXT Record : "apple-domain-verification=DfS0kKbWaeVQrWTW"
[+] SPF Record:  "v=spf1 mx ip4:8.11.3.51 ip4:8.20.73.51 ip4:69.72.18.20 ip4:69.72.16.20 ip4:108.166.45.120 ip4:50.31.43.169
ip4:139.138.57.24 ip4:216.71.146.234 include:spf.protection.outlook.com -all"
[+] TXT Record : "ca3-34d17a6da1f244f098f22d4d518be004"
[+] TXT Record : "facebook-domain-verification=auaz3u8n1q4spli5cgbwadmfcehaym"
[+] TXT Record : "gnIzEWRy2xVqYXGoscbcm8VBBBC4LVLWqJWNfU650lhMwMnHJ7Rmdk9rUTNTKHYJP0sPvq+UfZhZXwD9cWAO1A=="
[.] DKIM Record : Selector 'nhl' or 'selector1' is not found in the DNS records. Check DKIM configuration or choose the manual
selector option.
[+] DMARC Record :  "v=DMARC1;p=none;fo=1;rua=mailto:dmarc@nhl.com;ruf=mailto:dmarc@nhl.com"
[.] BIMI Record :  [illegible] figuration or choose the manual
selector option.
```

Let’s send mail!

```
┌──(kali㉿kali)-[~/scripts/check_domain]
└─$ swaks -f test@nhl.com -t robsherw@bce-demo.com --server myesa.iphmx.com --attach-type text/html
…
Sun Jun 12 16:28:22 2022 Info: Start MID 340722 ICID 1589839
Sun Jun 12 16:28:22 2022 Info: MID 340722 ICID 1589839 From: <test@nhl.com>
Sun Jun 12 16:28:22 2022 Info: MID 340722 SDR: Domains for which SDR is requested: reverse DNS host: ec2-3-136-210-164.us-east-
2.compute.amazonaws.com, helo: ip-172-31-43-120.us-east-2.compute.internal, env-from: nhl.com, header-from: Not Present, reply-
to: Not Present
Sun Jun 12 16:28:23 2022 Info: MID 340722 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/A, Suspected
Domain(s) : N/A (other reasons for verdict). Sender Maturity: 29 days for domain: nhl.com
Sun Jun 12 16:28:23 2022 Info: MID 340722 ICID 1589839 RID 0 To: <robsherw@bce-demo.com>
Sun Jun 12 16:28:23 2022 Info: MID 340722 SPF: mailfrom identity test@nhl.com Fail (v=spf1)
Sun Jun 12 16:28:23 2022 Info: MID 340722 DMARC: Message from domain nhl.com, DMARC fail, (SPF aligned False, DKIM aligned
False) DMARC policy is none, applied policy is none
Sun Jun 12 16:28:23 2022 Info: MID 340722 DMARC: Verification failed.
Sun Jun 12 16:28:23 2022 Info: MID 340722 DMARC: No action taken by DMARC policy.
Sun Jun 12 16:28:23 2022 Info: MID 340722 Message-ID '<20220612162651.4050900@ip-172-31-43-120.us-east-2.compute.internal>'
Sun Jun 12 16:28:23 2022 Info: MID 340722 Subject "test Sun, 12 Jun 2022 16:26:51 +0000”
…
Sun Jun 12 16:28:23 2022 Inf : Message finished MID 340722 done
Sun Jun 12 16:28:23 2022 Inf : MID 340723 queued for delivery
```

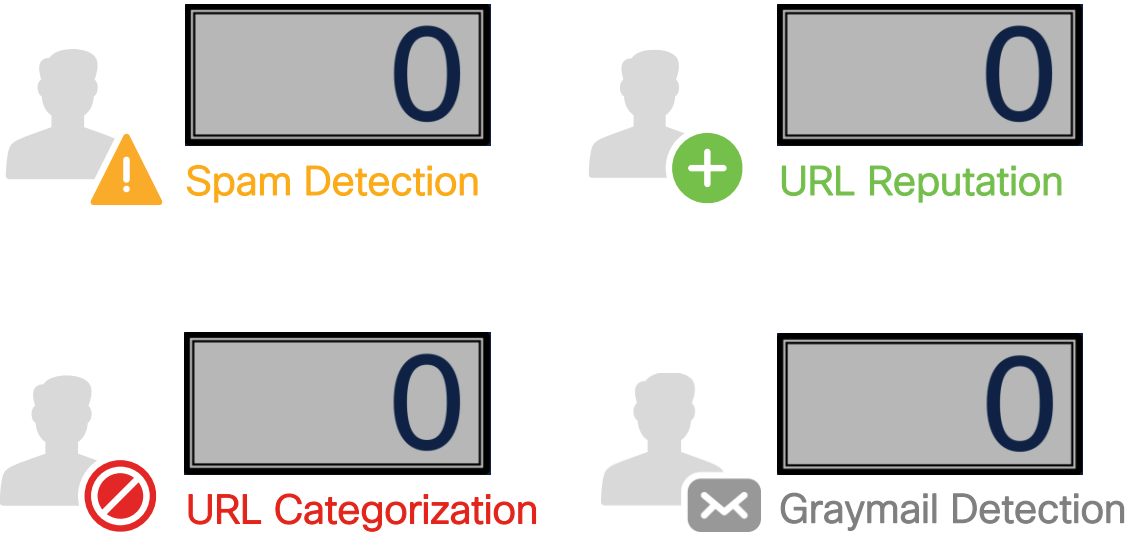
If SPF did fail and DMARC was reject

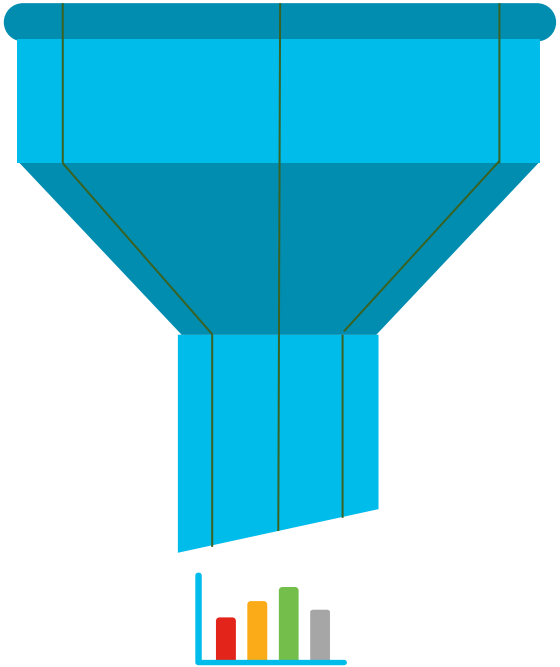
```
┌──(kali㉿kali)-[~/scripts/check_domain]
└─$ swaks -f robsherw@igo232.com -t robsherw@bce-demo.com --server myesa.iphmx.com --attach-type text/html

…
Sun Jun 12 16:26:23 2022 Info: Start MID 340721 ICID 1589835
Sun Jun 12 16:26:23 2022 Info: MID 340721 ICID 1589835 From: <robsherw@igo232.com>
Sun Jun 12 16:26:23 2022 Info: MID 340721 SDR: Domains for which SDR is requested: reverse DNS host: ec2-3-136-210-164.us-east-
2.compute.amazonaws.com, helo: ip-172-31-43-120.us-east-2.compute.internal, env-from: igo232.com, header-from: Not Present,
reply-to: Not Present
Sun Jun 12 16:26:23 2022 Info: MID 340721 SDR: Consolidated Sender Threat Level: Neutral, Threat Category: N/A, Suspected
Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain: igo232.com
Sun Jun 12 16:26:23 2022 Info: MID 340721 ICID 1589835 RID 0 To: <robsherw@bce-demo.com>
Sun Jun 12 16:26:23 2022 Info: MID 340721 SPF: mailfrom identity robsherw@igo232.com Fail (v=spf1)
Sun Jun 12 16:26:23 2022 Info: MID 340721 DMARC: Message from domain igo232.com, DMARC fail, (SPF aligned False, DKIM aligned
False) DMARC policy is reject, applied policy is reject
Sun Jun 12 16:26:23 2022 Info: MID 340721 DMARC: Verification failed.
Sun Jun 12 16:26:23 2022 Info: MID 340721 DMARC: Message rejected by DMARC policy.
Sun Jun 12 16:26:23 2022 Info: MID 340721 rejected by DMARC policy
Sun Jun 12 16:26:23 2022 Info                                                    4:52 +0000"
Sun Jun 12 16:26:23 2022 Info: Message aborted MID 340721 Receiving aborted
Sun Jun 12 16:26:23 2022 Info: Message finished MID 340721 aborted
```

Definition based URL Filtering

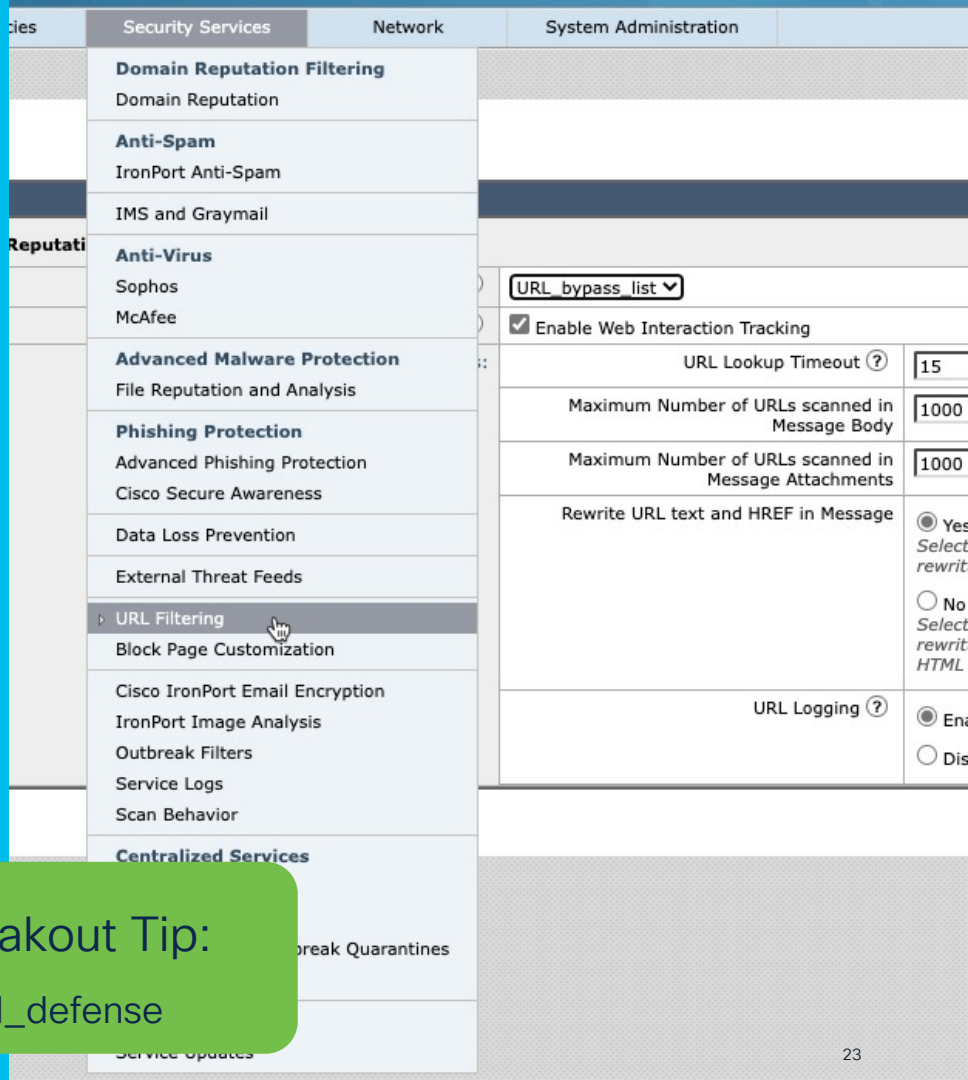
Trap the unwanted URLs





Reputation and Categorization

URL Filtering Demo

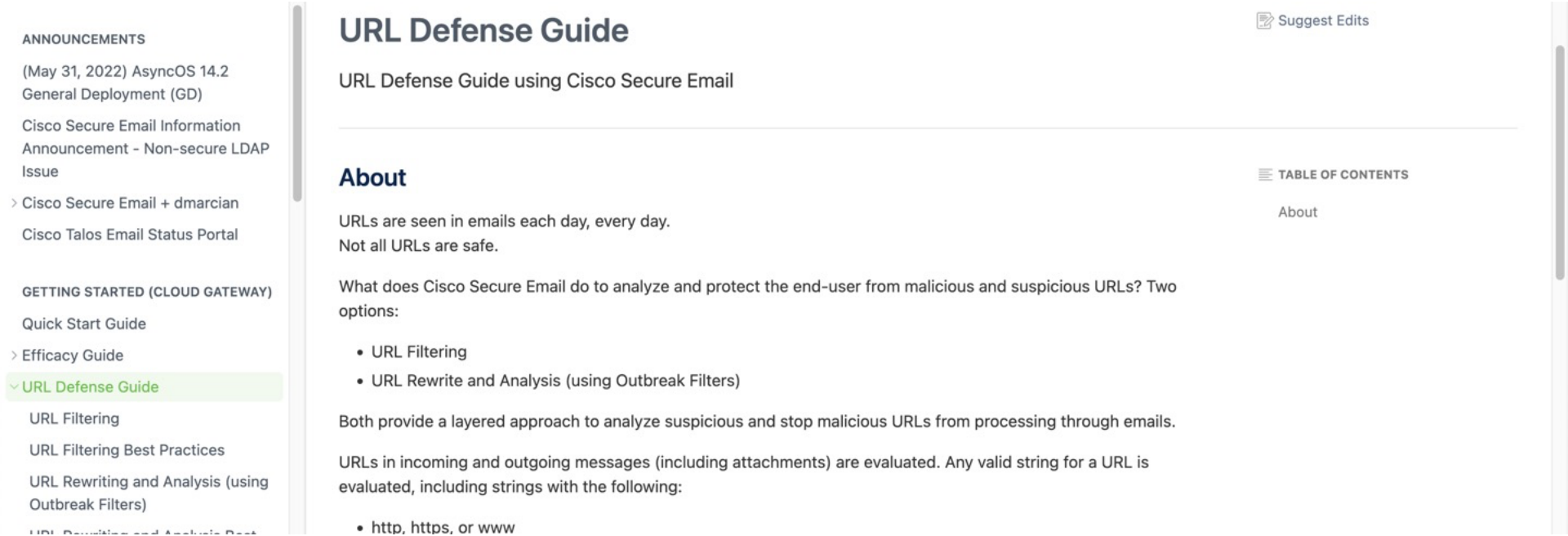


Breakout Tip:

cs.co/url_defense

Demo was in the BRKSEC only...
Please refer to docs.ces for URL Filtering...

- URL Defense Guide (cisco.com)



URL Rewrite & Analysis

Outbreak Filtering

Collect

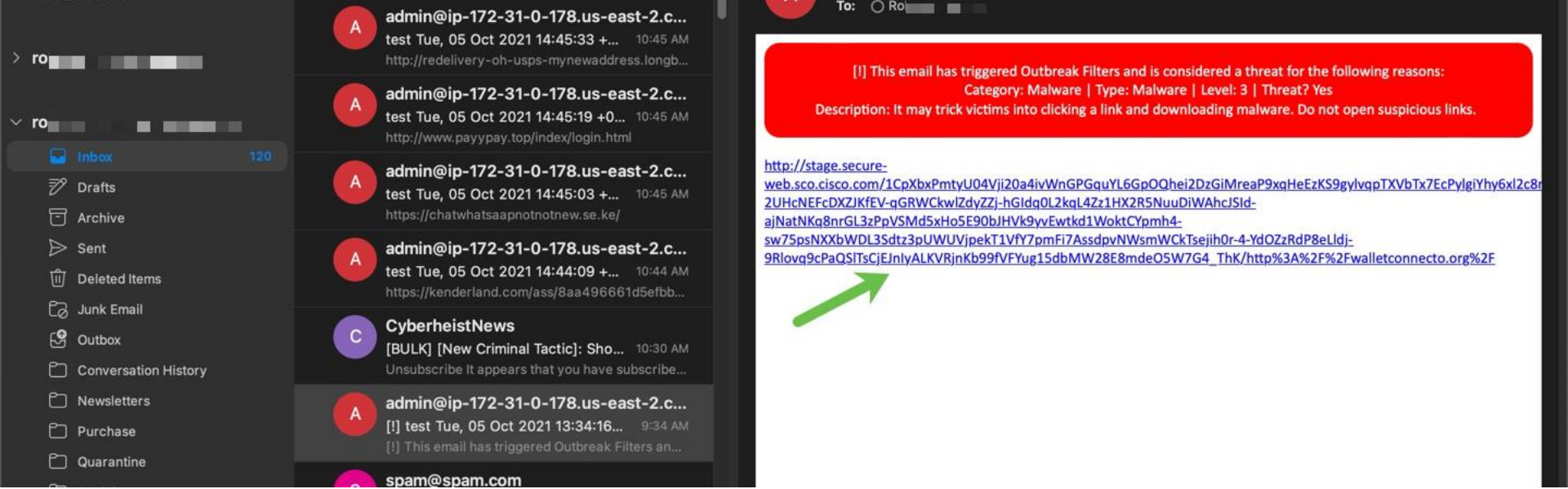
Captures data from over 100,000 contributing organizations and 35% of email traffic globally

Verify

Human curation to verify anomalies and approve automatically generated outbreak and adaptive rules

Automate

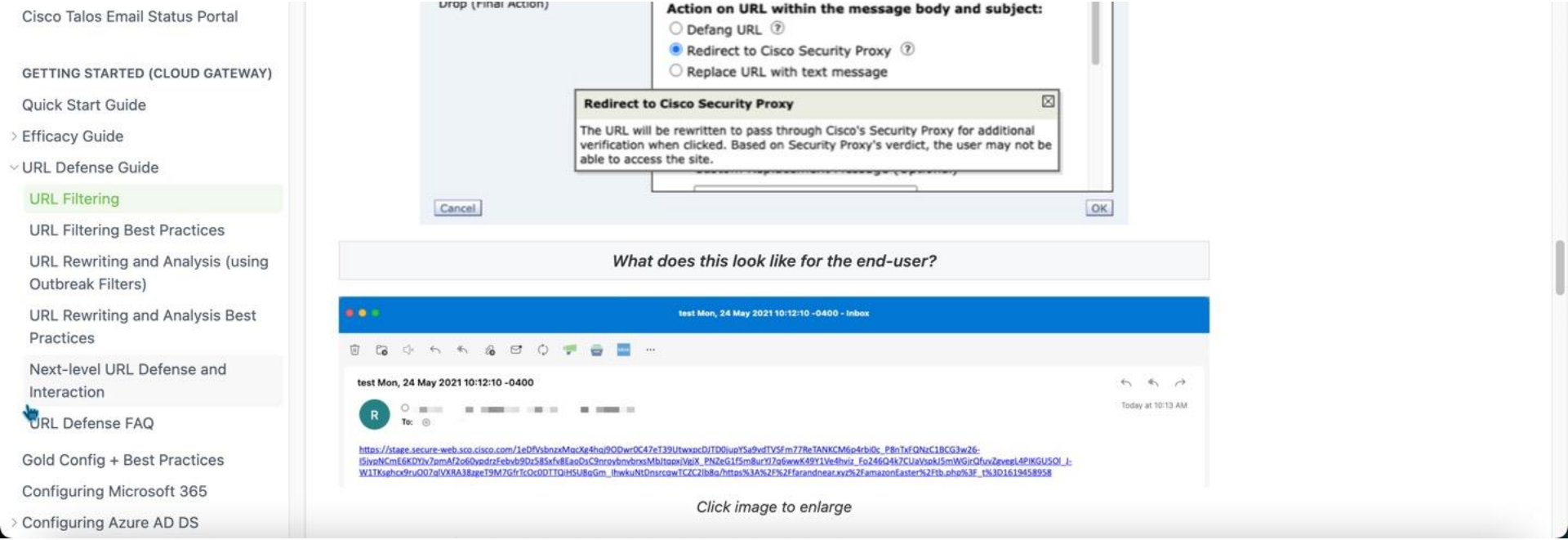
Dynamically quarantine or rewrite suspicious URL for deeper inspection via fine-grained rules



URL Rewrite (Outbreak Filters) Demo

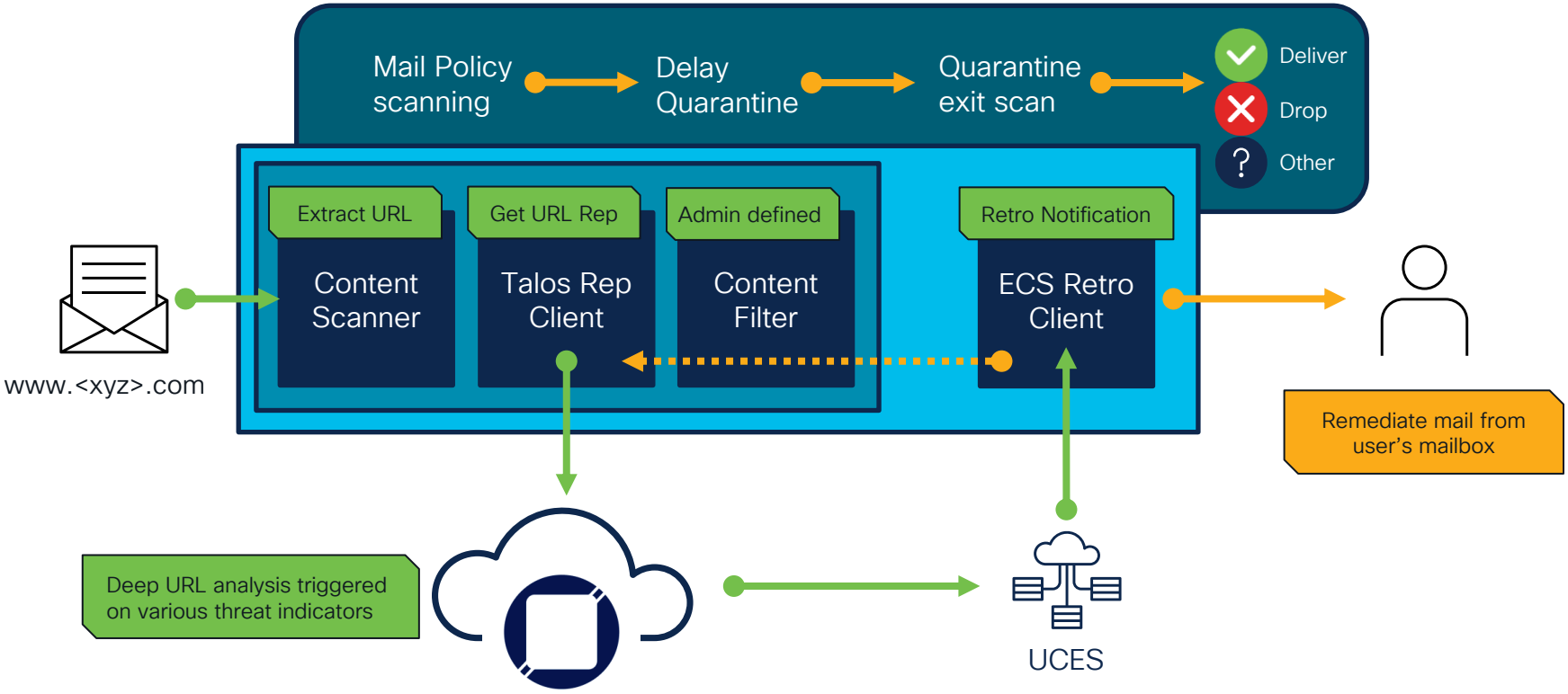
Demo was in the BRKSEC only...
Please refer to the recording or docs.ces...

- URL Defense Guide (cisco.com)



*New w/14.2 for Cloud customers

URL Protection + Remediation Workflow



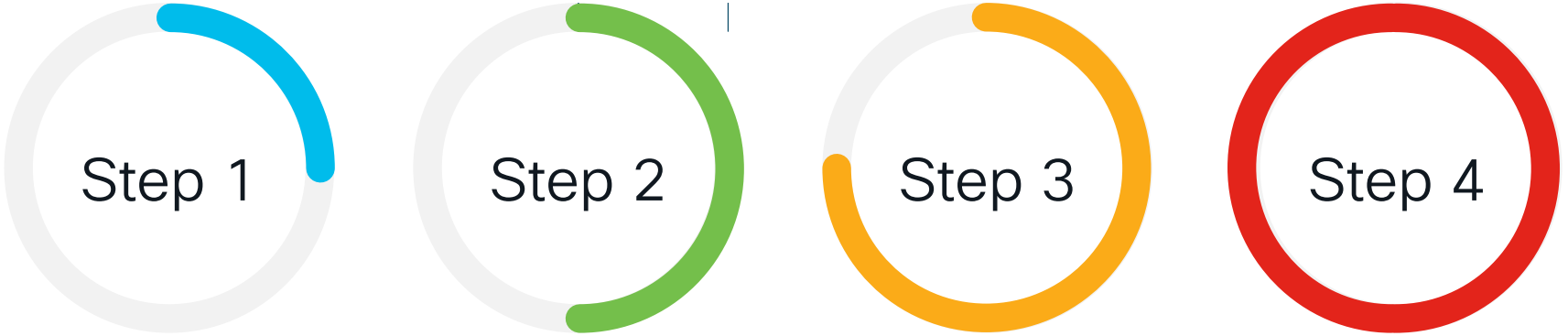
How URL Protection is triggered

Next-level Integrations

What are the challenges?

1. Too many IoCs to sift through
2. IoC from different types and scopes
3. Different teams need to work together
4. Need a tool to fuse all IoC together
5. Rely on big data analytics and correlation

How SecureX helps...



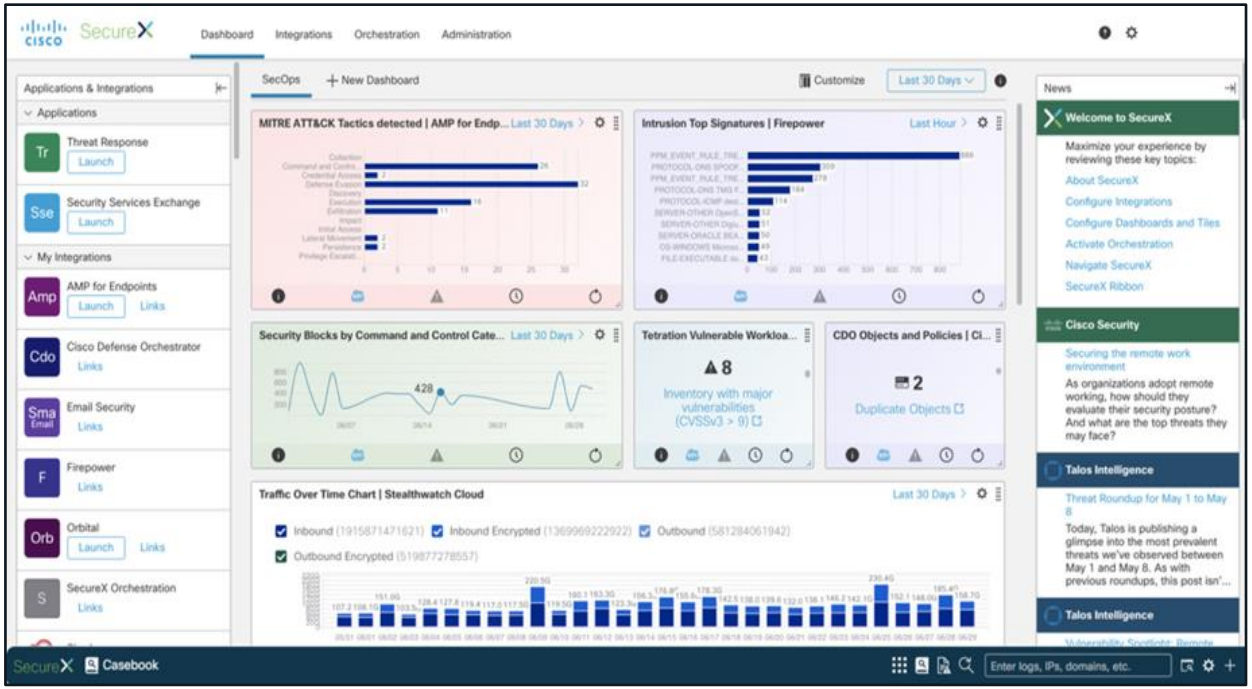
Collect data from Cisco and other threat feeds

Correlate with big data analytics

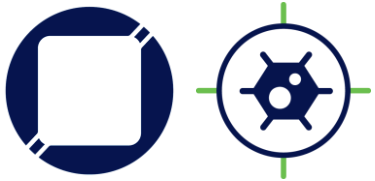
Reactive and proactive actions

Predictive action before attack happens

Step 1: Collect Data



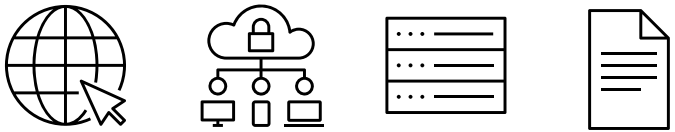
Step 2: Intel Collaboration



Cisco Talos, Cisco Malware Analytics, Third-party advisories

cisco SECURE X

Indication of Compromise (IoC)



URL IP Host SHA

Cisco Secure Email Cloud or Gateway

External Threat Feed Sources

Add Source

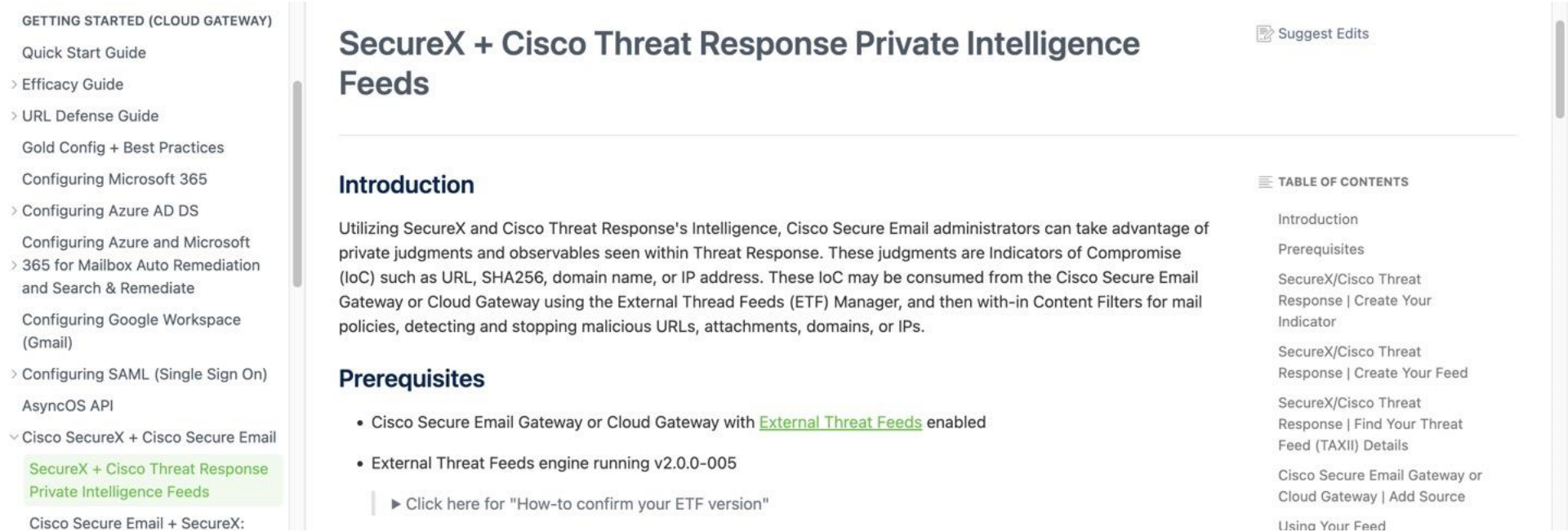
Source Name	Source Details	Polling Interval	Last Successful Poll	Status	Suspend/ Resume Polling	Delete	Poll Now
hailataxii	*Hostname* hailataxii.com *Collection Name* guest.phishtank_com	15m	22 Sep 2021 18:42:25	Idle	⏸	🗑	Poll Now
robsherw_CTR	*Hostname* private.intel.amp.cisco.com *Collection Name* ee77f78a-45e7-4321-8c6d-1ce016689728	15m	17 Sep 2021 12:43:31	Idle	⏸	🗑	Poll Now

** You can configure up to 8 external threat feed sources only.*

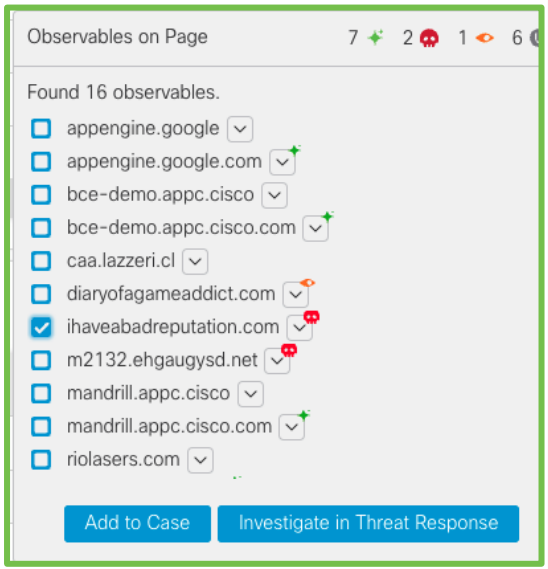
External Threat Feeds Demo

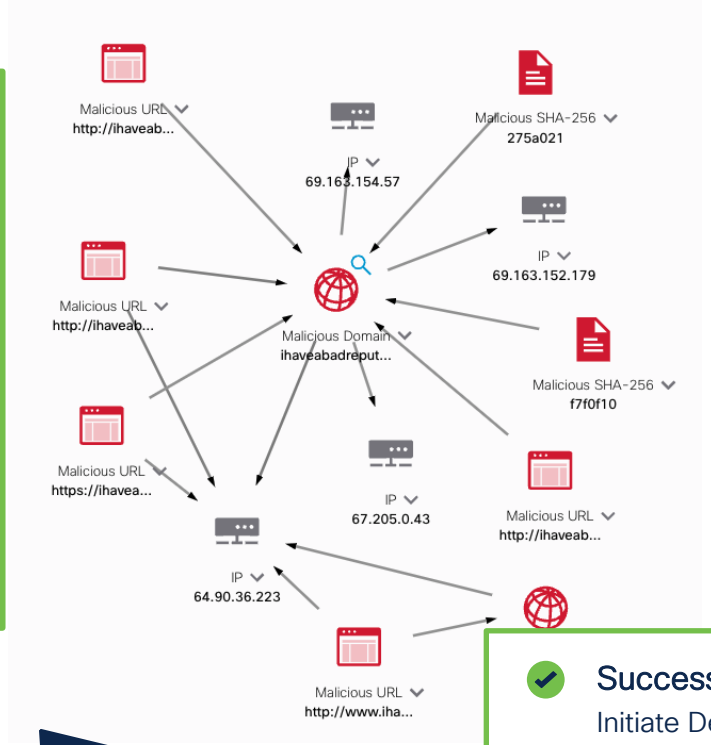
Demo was in the BRKSEC only...
Please refer to docs.ces for the ETF steps...

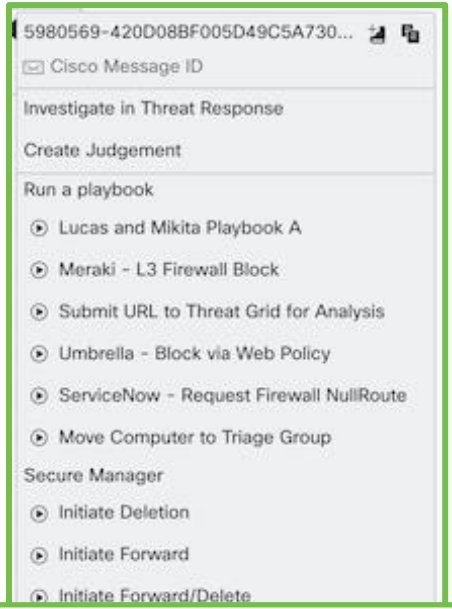
- SecureX + Cisco Threat Response Private Intelligence Feeds



Step 3: Reactive and Proactive actions







Success
Initiate Deletion

Partner Security Tools

(Cisco Hosted) APIVoid

Threat Analysis APIs for Threat Detection & Prevention

+ New Module Learn More

(Cisco Hosted) AbuseIPDB ...

Check IP addresses against AbuseIPDB's abusive IP database.

+ New Module Learn More

(Cisco Hosted) Akamai

Security Center provides answers to essential questions in the most intuitive and simple way

+ New Module Learn More

(Cisco Hosted) AlienVault O...

The AlienVault Open Threat Exchange (OTX) is the world's most authoritative open threat information sharing and analysis network.

+ New Module Learn More

(Cisco Hosted) CyberCrim...

Featuring FIFTY message echos covering ALL computer scenes: Art, Warez, Hacking, Phreaking, Technology, BBS Support, Demos, Coding, Sound, Gaming, as well a...

+ New Module Learn More

(Cisco Hosted) Farsight Se...

Farsight Security DNSDB® is the world's largest DNS intelligence database that provides a unique, fact-based, multifaceted view of the configuration of the global...

+ New Module Learn More

(Cisco Hosted) Gigamon T...

Accelerate network detection and response with Gigamon ThreatINSIGHT - a cloud-native, high-velocity NDR solution.

+ New Module Learn More

(Cisco Hosted) Google Ch...

Chronicle is a cloud service, built as a specialized layer on top of core Google infrastructure, designed so that enterprises can privately retain, analyze and search th...

+ New Module Learn More

(Cisco Hosted) Google Saf...

Safe Browsing is a Google service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources. Examples of unsafe web...

+ New Module Learn More

(Cisco Hosted) Have I Bee...

Have I Been Pwned allows you to search across multiple data breaches to see if your email address has been compromised.

+ New Module Learn More

(Cisco Hosted) IBM X-Forc...

IBM X-Force Exchange is a threat intelligence sharing platform enabling research on security threats, aggregation of intelligence, and collaboration with peers.

+ New Module Learn More

(Cisco Hosted) IsItPhishing

The IsItPhishing Threat Detection Rest API allows to check in real time and in a fully automated process whether an URL is a phishing or a spam website.

+ New Module Learn More

(Cisco Hosted) MISP

MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing.

+ New Module Learn More

(Cisco Hosted) Microsoft Gr...

The Microsoft Graph Security API is an intermediary service that provides a single programmatic interface to connect multiple Microsoft Graph Security providers....

+ New Module Learn More

(Cisco Hosted) Palo Alto Ne...

AutoFocus is a cloud-based threat intelligence service that enables you to easily identify critical attacks, based on intelligence from Unit 42, the Palo Alto...

+ New Module Learn More

(Cisco Hosted) Pulsedive

Pulsedive threat intelligence enriches any domain, URL, or IP. Scan new indicators, pivot to search on any data point, and investigate threats.

+ New Module Learn More

(Cisco Hosted) Qualys IOC

Qualys IOC enables threat hunting, detection of suspicious activity, and detection of malware for devices both on / off the network.

+ New Module Learn More

(Cisco Hosted) SecurityTr...

SecurityTrails can enrich your data with passive and historical data.

+ New Module Learn More

(Cisco Hosted) Shodan

Shodan is the world's first search engine for Internet-connected devices.

+ New Module Learn More

(Cisco Hosted) SpyCloud Ac...

SpyCloud helps enterprises prevent corporate account takeover by detecting stolen passwords early, before criminals have a chance to use them.

+ New Module Learn More

(Cisco Hosted) Threatscore...

Threatscore gives a computed score about a level of threat for any (known) observables.

+ New Module Learn More

(Cisco Hosted) urlscan.io

urlscan is a sandbox for websites which allows you to inspect suspicious and malicious websites

+ New Module Learn More

Bastille Networks

RF monitoring for wireless intrusion detection and policy enforcement.

+ New Module Learn More

CyberCrime Tracker

Featuring FIFTY message echos covering ALL computer scenes: Art, Warez, Hacking, Phreaking, Technology, BBS Support, Demos, Coding, Sound, Gaming, as well a...

+ New Module Learn More

Generic Serverless Relay

Generic Serverless Relay module that can be used when developing new integrations

+ New Module Learn More

Microsoft Graph Security ...

The Microsoft Graph Security API is an intermediary service that provides a single programmatic interface to connect multiple Microsoft Graph Security providers....

+ New Module Learn More

Radware Cloud DDoS Prote...

Radware's Cloud DDoS Protection Services deliver the most accurate and rapid protection from today's constantly evolving DDoS threats.

+ New Module Learn More

Radware Cloud WAF Serv...

Radware's Cloud WAF Service provides adaptive web security protection in an easy to use, hassle free service.

+ New Module Learn More

SecureX CESA Relay

SecureX CESA Relay is a Splunk Technical Add-on which queries CESA/NVM Datasources logs within Splunk.

+ New Module Learn More

ServiceNow Security Incident...

ServiceNow® SecOps (Security Operations) connects your existing security tools to prioritize and respond to vulnerabilities and security incidents faster.

Signal Sciences Next-Gen...

Protect apps running on your network from OWASP attacks with no tuning. Signal Sciences next-gen WAF deploys anywhere in your technology stack.

Sixgill Darkfeed

Sixgill's premium underground intelligence collection capabilities, real-time collection and advanced warning about IOCs to help you keep your edge against unknown...

Splunk Relay module

This Relay module is a Splunk Technical Add-on which queries Datasources logs within Splunk.

VirusTotal

VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

+ New Module Learn More

Partner Security Tools

(Cisco Hosted) APIVoid
Threat Analysis APIs for Threat Detection & Prevention
+ New Module Learn More

(Cisco Hosted) AbuseIPDB ...
Check IP addresses against AbuseIPDB's abusive IP database.
+ New Module Learn More

(Cisco Hosted) Akamai
Security Center provides answers to essential questions in the most intuitive and simple way
+ New Module Learn More

(Cisco Hosted) AlienVault O...
The AlienVault Open Threat Exchange (OTX) is the world's most authoritative open threat information sharing and analysis network.
+ New Module Learn More

(Cisco Hosted) CyberCrim...
Featuring FIFTY message echos covering ALL computer scenes: Art, Warez, Hacking, Phreaking, Technology, BBS Support, Demos, Coding, Sound, Gaming, as well a...
+ New Module Learn More

(Cisco Hosted) Farsight Se...
Farsight Security DNSDB® is the world's largest DNS intelligence database that provides a unique, fact-based, multifaceted view of the configuration of the global...
+ New Module Learn More

(Cisco Hosted) Gigamon T...
Accelerate network detection and response with Gigamon ThreatINSIGHT - a cloud-native, high-velocity NDR solution.
+ New Module Learn More

(Cisco Hosted) Google Ch...
Chronicle is a cloud service, built as a specialized layer on top of core Google infrastructure, designed so that enterprises can privately retain, analyze and search th...
+ New Module Learn More

(Cisco Hosted) Google Saf...
Safe Browsing is a Google service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources. Examples of unsafe web...
+ New Module Learn More

(Cisco Hosted) Have I Bee...
Have I Been Pwned allows you to search across multiple data breaches to see if your email address has been compromised.
+ New Module Learn More

(Cisco Hosted) IBM X-Forc...
IBM X-Force Exchange is a threat intelligence sharing platform enabling research on security threats, aggregation of intelligence, and collaboration with peers.
+ New Module Learn More

(Cisco Hosted) IsItPhishing
The IsItPhishing Threat Detection Rest API allows to check in real time and in a fully automated process whether an URL is a phishing or a spam website.
+ New Module Learn More

(Cisco Hosted) MISP
MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing.
+ New Module Learn More

(Cisco Hosted) Microsoft Gr...
The Microsoft Graph Security API is an intermediary service that provides a single programmatic interface to connect multiple Microsoft Graph Security providers....
+ New Module Learn More

(Cisco Hosted) Palo Alto Ne...
AutoFocus is a cloud-based threat intelligence service that enables you to easily identify critical attacks, based on intelligence from Unit 42, the Palo Alto...
+ New Module Learn More

(Cisco Hosted) Pulsedive
Pulsedive threat intelligence enriches any domain, URL, or IP. Scan new indicators, pivot to search on any data point, and investigate threats.
+ New Module Learn More

(Cisco Hosted) Qualys IOC
Qualys IOC enables threat hunting, detection of suspicious activity, and detection of malware for devices both on / off the network.
+ New Module Learn More

(Cisco Hosted) SecurityTr...
SecurityTrails can enrich your data with passive and historical data.
+ New Module Learn More

(Cisco Hosted) Shodan
Shodan is the world's first search engine for Internet-connected devices.
+ New Module Learn More

(Cisco Hosted) SpyCloud Ac...
SpyCloud helps enterprises prevent corporate account takeover by detecting stolen passwords early, before criminals have a chance to use them.
+ New Module Learn More

(Cisco Hosted) Threatscore...
Threatscore gives a computed score about a level of threat for any (known) observables.
+ New Module Learn More

(Cisco Hosted) urlscan.io
urlscan is a sandbox for websites which allows you to inspect suspicious and malicious websites
+ New Module Learn More

Bastille Networks
RF monitoring for wireless intrusion detection and policy enforcement.
+ New Module Learn More

CyberCrime Tracker
Featuring FIFTY message echos covering ALL computer scenes: Art, Warez, Hacking, Phreaking, Technology, BBS Support, Demos, Coding, Sound, Gaming, as well a...
+ New Module Learn More

Generic Serverless Relay
Generic Serverless Relay module that can be used when developing new integrations
+ New Module Learn More

Microsoft Graph Security ...
The Microsoft Graph Security API is an intermediary service that provides a single programmatic interface to connect multiple Microsoft Graph Security providers....
+ New Module Learn More

Radware Cloud DDoS Prote...
Radware's Cloud DDoS Protection Services deliver the most accurate and rapid protection from today's constantly evolving DDoS threats.
+ New Module Learn More

Radware Cloud WAF Serv...
Radware's Cloud WAF Service provides adaptive web security protection in an easy to use, hassle free service.
+ New Module Learn More

SecureX CESA Relay
SecureX CESA Relay is a Splunk Technical Add-on which queries CESA/NVM Datasources logs within Splunk.
+ New Module Learn More

ServiceNow Security Incident...
ServiceNow® SecOps (Security Operations) connects your existing security tools to prioritize and respond to vulnerabilities and security incidents faster.

Signal Sciences Next-Gen...
Protect apps running on your network from OWASP attacks with no tuning. Signal Sciences next-gen WAF deploys anywhere in your technology stack.

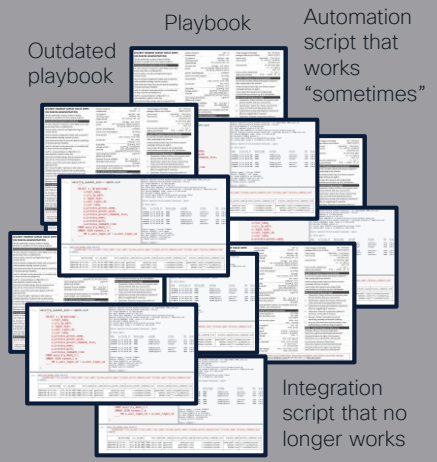
Sixgill Darkfeed
Sixgill's premium underground intelligence collection capabilities, real-time collection and advanced warning about IOCs to help you keep your edge against unknown...

Splunk Relay module
This Relay module is a Splunk Technical Add-on which queries Datasources logs within Splunk.

VirusTotal
VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.
+ New Module Learn More

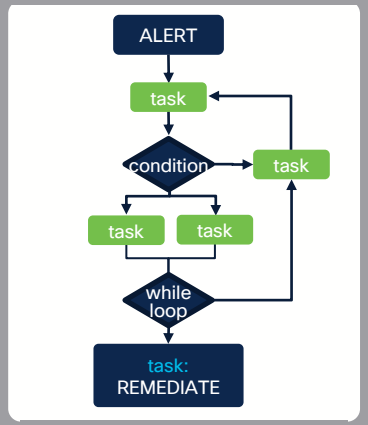
Step 4: Predictive actions

BEFORE:
Repetitive, human-powered tasks



SOLUTION:
Orchestrating security across the full lifecycle

Pre-built or customizable workflows



Cisco or non-Cisco infrastructure

AFTER:

"We have never communicated faster: Our approvals are automated."

"I combined 9 tasks across 3 security tools, 2 infrastructure systems, and 3 teams in **one keystroke**!"

"I make automated playbook changes in minutes with a drag-drop interface."

"My top 5 most frustrating tasks have all be automated."

Sessions on Orchestration

Crash Course: Automating with SecureX Orchestration - HOLSEC-2001.a

Oxana Sannikova, Technical Solutions Architect
Matt Vander Horst, Technical Leader

Wed
Thur

Increase Visibility and Response to Email Threats Using Cisco SecureX Orchestration - DEVNET-2107

Alexandre Argeris, Cybersecurity Technical Solutions Architect

Thur

SecureX Orchestration

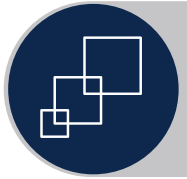
Process automation made simple with a no/low-code drag-drop interface

Investigate

Reduce research and response times with workflows and playbooks that execute at machine speed

Automate

Eliminate repetitive tasks and reduce MTTR to increase productivity and focus on mission-critical projects



Integrate

Unique turnkey approach to quickly integrate with other systems and solutions to expand your toolbox

Scale

Automation that scales infinitely and never takes a day off, delivering the same SLA around the clock

Key Takeaways

1. Re-evaluate your containers!
2. Re-educate yourself! (You may be doing it wrong.)
3. URL attacks are more prevalent
4. Cisco Secure Email has worked to improve URL defense seamlessly
5. Expand what your security posture is beyond your email gateway

If you don't... please don't let this happen to your ship...

Keep up-to-date! For more info:

cisco.com/go/emailsecurity

ask-secure-email@cisco.com

docs.ces.cico.com

- URL Defense Guide
- Efficacy Guide

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Security Reference Architecture

CISCO SECURE

TALOS — Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt

Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE) | ZERO TRUST

Threat Protection | Secure Access Control | Managed Remote Access

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

SDWAN

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes
- Cloud DDoS,WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- Meraki Full Stack
- Secure Network Analytics
- Secure Web Appliance
- ISE TrustSec
- Cisco DNA Center

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

- Cloud Native Security
- APIC
- Secure Workload
- Secure Application by AppDynamics

App Observability | Detection | Response

- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

cisco Live!

Thank you


cisco Live!
ALL IN

Appendix

Cisco Live On-Demand Library

- Don't Send, Deliver! - BRKSEC-2337
- Fixing Email! - Cisco Email Security Advanced Troubleshooting - BRKSEC-3265
- SPF is not an acronym for "Spoof"! Let's utilize the most out of the next layer in Email Security! - BRKSEC-2327

Talos

- Cisco Talos Intelligence Group - Comprehensive Threat Intelligence
- Reputation Center - A Real Time Threat Detection Service
- Requires CCO ID log-in:
  - Web and Email Reputation Tickets
  - Email Submissions
  - Cisco Talos Sender Domain Reputation (SDR)
    - The attached white paper provides an overview of Cisco Talos SDR.
    - The 'SDR Whitepaper AsyncOS 14.2' version published on June 2nd, 2022, is specific to release AsyncOS 14.2 and later (verdict updates & maximum value for Domain Maturity).

SPF, DKIM, DMARC

- Cisco Secure Email + dmarcian (docs.ces.cisco.com)
- dmarcian for Cisco customers – dmarcian (dmarcian Log-in portal)
  - DMARC Testing & Reporting Tools - Test DMARC Online (dmarcian)

Useful SPF, DKIM, DMARC Scripts:

- cs.co/check_domain
- cs.co/spoofthatmail

URL Protection (+more!)

- cs.co/url_defense (URL Defense Guide)
- Gold Config + Best Practices
- Efficacy Guide

SecureX

- Cisco SecureX + Cisco Secure Email
- SecureX + Cisco Threat Response Private Intelligence Feeds
- Cisco Secure Email + SecureX: Extending email protection and integrations beyond the gateway