

CISCO *Live!*



#CiscoLive



The bridge to possible

Building a Cyber Defense Center to Protect a Nation

Yasser Alghamdi – Cyber Defense Center Director
Saudi Telecom Co (stc)
@Yasser_J_Gh
CSSSEC-1202



#CiscoLive



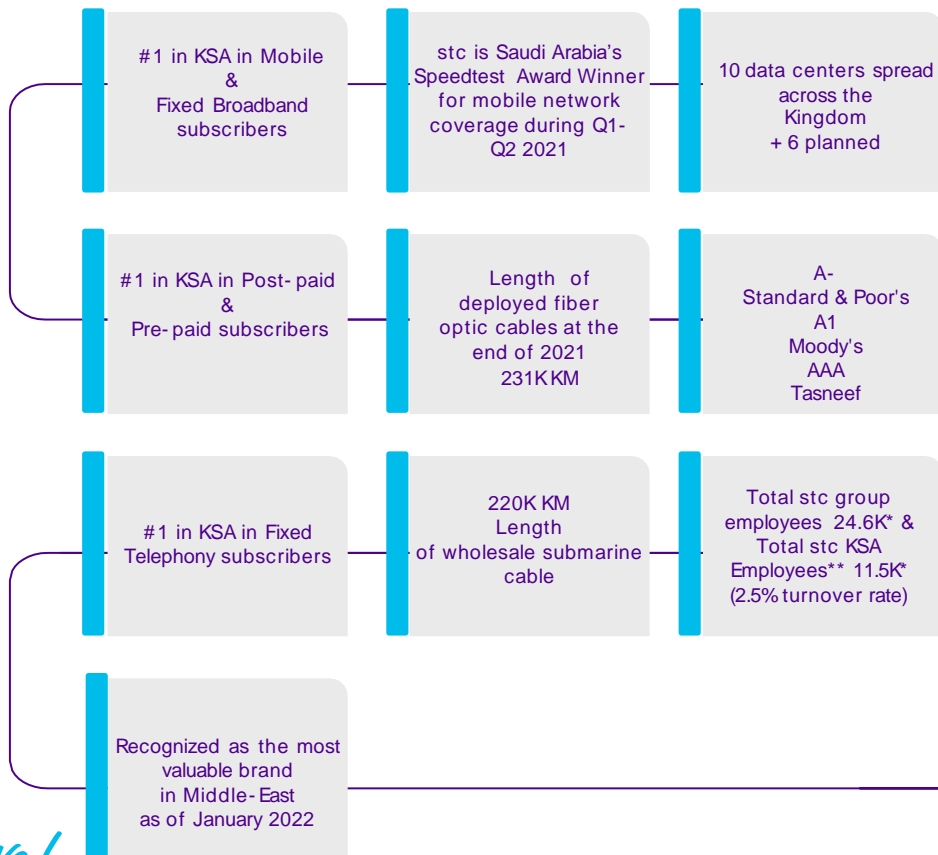
Agenda

- stc and CDC
- Overcoming Challenges
- Enhancing Core Capabilities
- Toward Innovation
- Lessons Learnt

stc and CDC

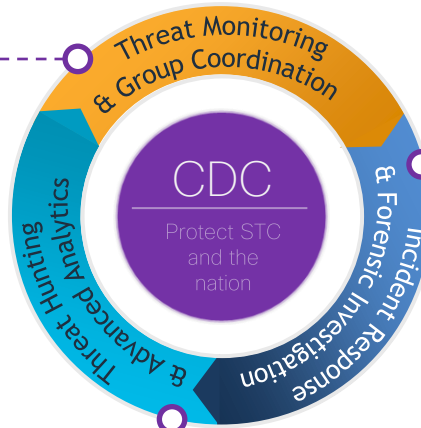


stc – Major Digital Transformation Partner



The Role of the CDC

Perform, improve and maintain threat detection
Perform triage to determine criticality and scope of impact of threat execution
Threat Monitoring, Content Management, Platform Management, L1 & L2 Incident Management Management, Delivery Management



Design, deploy and operate advanced analytics
Design and execute threat hunting expeditions
Enhance threat monitoring and hunting capabilities
Threat Hunting, Data Analytics

Manage incidents
Collect, investigate, document and preserve evidence Perform root cause analysis
Present key findings and insights
Perform reverse engineering and malware analysis
L3 Incident Response, Digital Forensics, Malware Analysis & reverse Engineering

CDC SERVICES

50+
SERVICE

CDC Workforce

40+
PEOPLE

Overcoming Challenges



A Large Footprint to Defend

Top Challenges

1 Reactive in nature

2 Centered around monitoring IT systems

3 Limited detection and response capabilities

4 Limited automation capabilities

Very large users across the world

30,000+
endpoints

Large number of non-actionable alerts to triage and investigate (manually)

1000+
Events to response per day

Very large network footprint

100,000+
Network Nodes

Large volume of events to store and process

14TB
Per day of events

Large number of assets across multiple geographical locations

10,000+
servers

Large number of applications to monitor but with minimal business

250+
Critical applications

Driving Values out of CDC Investments

Achieve better
visibility

Achieve better
detection

Achieve better
investigation

Achieve better
reporting

Optimize resource
usage

Reduce cyber
threats impact on stc
business

Planning for Success



Plan

CDC Service Strategy

- Business alignment
- Enterprise Strategy
- Drivers
- Services -> Subcomponents
- Operating model
- HL Organizational design
- Core Processes
- High Level Technology
- Align expectation to budget

Establish

Core Capabilities

- CDC roles & Mandate
- Visibility
- Detection
- Incident Mgmt
- Threat Hunting
- KPI Reporting
- Platform Mgmt

Drive Maturity

Continuous Development

- Advanced Detection
- Proactive Defense
- IT & Telecom Coverage
- Process development
- Playbooks & Use Case

Advanced

Functions

- Automation
- Analytics (AI/ML)

Success & Measurement

- Process and framework improvement
- Measure / Report
- Explore System Environment
- Optimize (Tech, Process, etc)
- Analyse (SLA / OLA / KPI)

Future

- Business Integration
- Emerging Technologies Adoption
- Regional & Global Leader
- Innovation

Spending time to Plan a Strategy

Challenge

CDC took a technology-centric approach to address the threat landscape. It was not easy to demonstrate the value that CDC brings. It was not easy to establish clear relationships between teams.



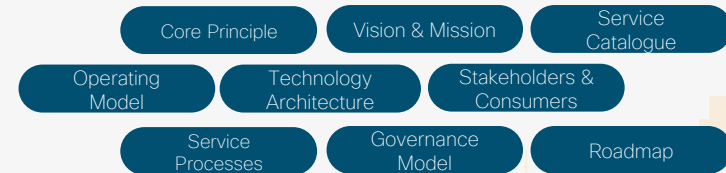
Solution

Work with Cisco CX to develop a strategy, service design, a governance model.

Outcome

Structuring a solid model for the CDC and positioning it as a center of excellence in the region

Clear roadmap of services and maturity to drive the technical architecture and security controls



Enhancing Core Capabilities



Establish and Enhance Core Capabilities – Detection

Challenge

Gap in the number of IT and telecom systems monitored by CDC.

Shortage in relevant detection use cases

Gap in having solid operation playbooks

Solution

Increase integration to cover all critical systems and nodes

Aligned with MITRE ATT@CK framework to cover most of TTPs

Enhance operation playbooks to conduct proper and mature response

Cover telecom usecases and integrate with all cyber technologies



Outcome

Systems & Nodes
Visibility

100,000+
Systems

MITRE ATT@CK
Alignment

1000+
Usecases & Rules

Technology
Integration

200+
Usecases

Telecom Specific
SS7, Diameter, etc.

20+
Usecases

Establish and Enhance Core Capabilities – Digital Forensics & Incident Response

Challenge

Relaying on external partners to conduct incident response.

Gap in having all needed capabilities and toolkits in field of digital forensics and malware analysis
unmatured MTTD & MTTR averages

Solution

Enhance incident response operation processes and reporting

Acquire missing forensics and malware analysis toolkits

Enhancing team capabilities toward advanced practices

Enhance MTTD & MTTR averages



Outcome

Time to Response

8H to 1H

Significant Improvement

Time to Contain

48H to 4H

Significant Improvement

Digital Forensics
Cases

200+

Reports

Establish and Enhance Core Capabilities – Hunting and Threat Intelligence

Challenge

Reactive approach to the detection of threat and responding to incidents
Low integration with threat intelligence operation
Lack of visibility on cyber technologies spikes

Solution

Adopted proactive approach to CDC operation
Build complete threat hunting operation
Establish solid threat intelligence alignment
Establish “Sayyad” as a threat hunting bounty platform



Outcome

Threat hunt
Campaigns

70+
Hunt

Threat intelligence
research

200+
Reports

Hunting Bounty
Platform

20+
Challenges

Establish and Enhance Core Capabilities – Measuring Performance SLAs/KPIs

Challenge

Only 4 SLAs/KPIs to measure the whole operation of CDC.

No proper automation in calculation the SLAs/KPIs frequently. Poor maturity in most of them

Poor CMMI measurement on CDC

Solution

3 years of SLAs/KPIs maturity plan and cover most of CDC operation day to day tasks

Automate the calculation of SLAs/KPIs actual numbers without human intervention

Increase the CMMI maturity score



Outcome

SLAs/KPIs

20+

Metrics

CMMI
Maturity

Level 4+

Integrated

SLAs/KPIs
Types

Incident, platform,
content, workforce,
hunting

Establish and Enhance Core Capabilities – Reporting

Challenge

Poor technical and executive reporting which caused ambiguity to take clear decision based on the shared data

Poor technical and executive dashboards

Solution

Enhance operation reporting/dashboard data

Enhance executive management reporting/dashboard data

Enhance external reporting/dashboard data (RMC, PMC, KPIs, etc)

Develop real-time dashboards reporting the security details of the top 10 critical applications



Outcome

Reporting Dashboard

70+
Dashboards

Reporting Schema

10+
Reports

External Reports

5+
Reports

Application Dashboards

10+
Dashboards

Toward Innovation



Establishing Innovation - Automation

Challenge

Triaging, investigating, containing, and reporting security incidents were manual, consuming time, and impacting SLAs and quality.

Massive operation time consuming to deal with all internal tasks and external requests



Solution

Establish automation as a service

Create a security automation framework and process

Design, test and operate integrations and playbooks on a SOAR platform

Outcome

Technology
Integration

20+

integrations

Automation
Workflows

40+

workflows

Automation
Activities

Collection, Actions,
and
Communication

Establishing Innovation - Data Analytics

Challenge

Thousand of assets, massive log size, complicated and custom technologies
shortage in experts in the market and fast changes in threat landscape are impact the quality of detection



Solution

Establish various machine learning models to baseline the behaviour and support the investigation with bigger scale through acquiring data analytics platform

Enabling machine learning across CDC technologies

Monitoring dashboards to provide analytics view on the attack volume

Outcome

Technologies Adaption

UEBA, Hadoop, Tableau, SIEM

Analytics Usecases

50+
usecases

Analytics Domains

Access Misuse,
Cyber Tech.
Attributes, Telecom
Cases, Network
Cases

Establishing Innovation – Future Strategy

Challenge

Poor integration with business operation
lack of heavily contribute to security community
Poor adaption of emerging technologies



Solution

Best-in-class cyber security experience to enable stc's business
Position stc as regional and global cyber security leader
Secure evolving digital and technology footprint

Outcome

Business
Integration

10+
Dashboards
and reports

Reginal & Global
Leader

10+
Contribution
and Publication

Evolving
Technology

5+
Technology

Lessons Learnt



Lessons Learnt

- 1 Start with structured strategy, clear key objectives, specific measurement, and periodical performance review to avoid ad-hoc mentality
- 2 Build solid operating model that help you to provide comprehensive services to CDC customers
- 3 Ensure full visibility to all entity assets, understand the business operation, and build detection capabilities by integrating with international practices and based on business logic
- 4 Build strong incident response capabilities to cover gaps in detection/protection and ensure to limit the impact to business



Lessons Learnt

5

Invest in automation and machine learning to reduce the overhead and deal better with huge size of data and logs

6

Adopt proactive approach and don't rely on reactive approach. The threat landscape is changing frequently

7

A hybrid delivery model, working with leading cyber security service providers helped us accelerate our maturity journey. Choose a "partner" that is willing to share knowledge and good practices.

8

Show value to executives and business owners by sharing cyber security insights for business services and threat landscape



Lessons Learnt

- 9 Listen to your *actionable* KPIs to drive actions. Adjust them if needed, and enhance them if available
- 10 It is not only about a SIEM. Deploy your use cases across your detection landscape (e.g., EDR, NDR, etc.), aggregate and correlate with your SIEM and then automate using a SOAR.
- 11 Optimize data ingestion and run optimization exercises regularly. They will save you money (lots) and ensure optimal platform operation.
- 12 Build attractive environment where people have fun at work. Fun at work is a key element of employee happiness in very exhausted domain



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 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

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Threat Protection | Secure Access Control | Managed Remote Access

Reliable | Scalable | Flexible



SDWAN



On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security



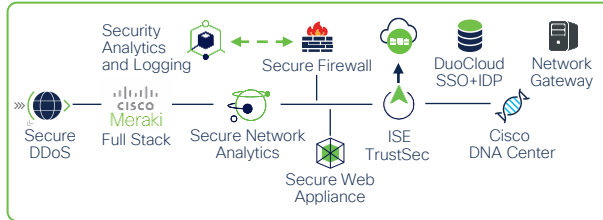
IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT



ZERO TRUST

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



Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack



App Observability | Detection | Response



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

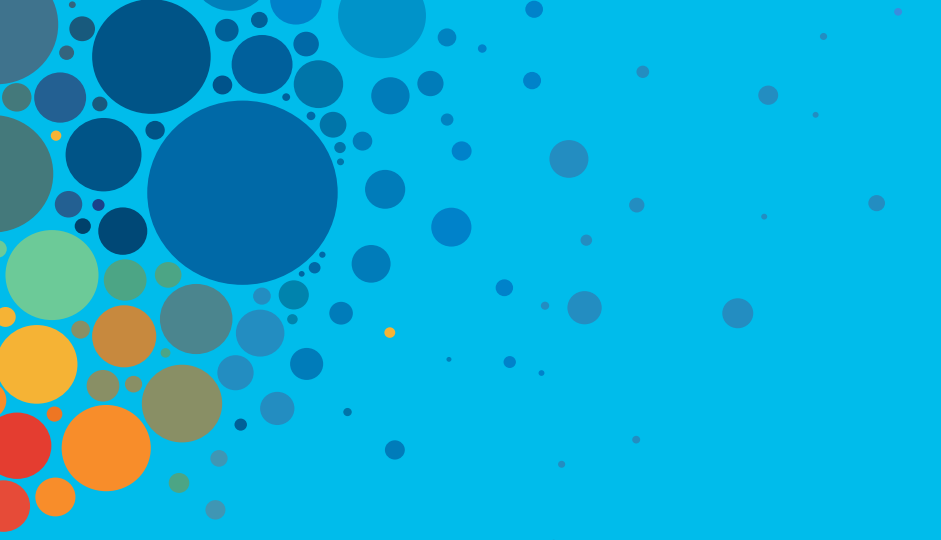
Cisco Guided Study Groups

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



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive