5 Security Building Blocks with SOAR Architect & Author Joey Muniz

Real-World Deployment Advice from UDC and NFF

Welcome!

AGENDA

- Speaker Introductions and NFF Overview
- Security Building Blocks and SOAR
- Security Transformation: University of the District of Columbia
- Cybersecurity Solutions
- Questions and Answers – Submit via Chat

SPEAKERS

- Chris Peabody – Chief Strategy Officer, Networking For Future
- Joey Muniz – Senior Cybersecurity Architect , Cisco Systems
- Mike Rogers – Executive Director, Information Services and Management, University of the District of Columbia
- Jonathan Topping – Principal Architect / Director of Solutions Architecture, Networking For Future

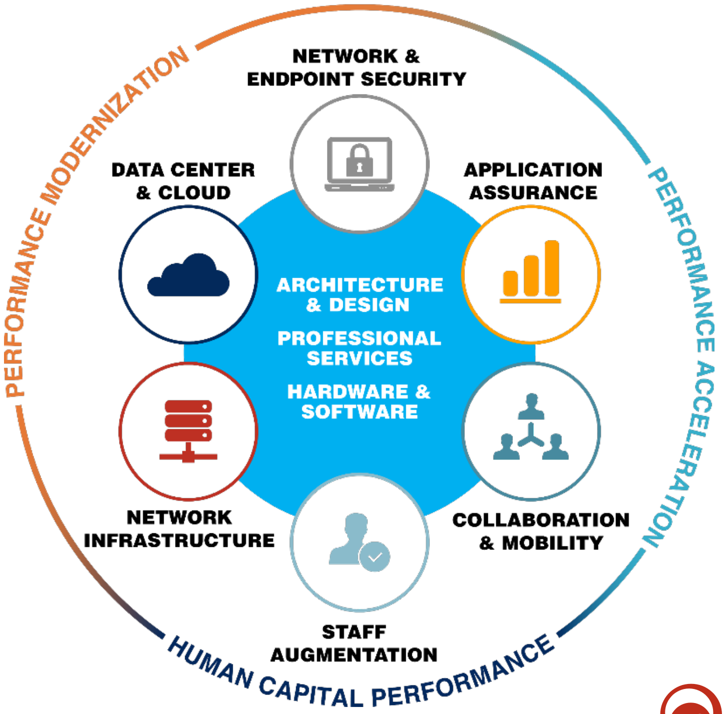
OVERVIEW

Networking For Future, Inc. (NFF)

- Founded in 1996
- Headquartered in Washington, DC
- 130+ Employees
- ISO 9001:2015 Certified
- 77% of workforce hold industry certifications

Offering a performance-focused approach to delivering transformational IT business solutions.

IT Business Solutions



OVERVIEW

Strategic Partners

- Cisco Gold Integrator Partner
- NetApp Gold Partner
- VMware Enterprise Partner
- Splunk Partner
- Microsoft Partner
- Gigamon Partner
- Riverbed Premier Partner
- Aternity Partner
- IET Corporation Partner
- F5 Networks Partner
- Citrix Silver Solution Advisor
- CoreSite Partner
- TRAXyL Partner

Strategic Contract Vehicles

- GSA Schedule 47QTCA21D0047
- District of Columbia Supply Schedule
  - MOBIS and ITES
- Maryland Education Enterprise Consortium (MEEC)
- Maryland Consulting and Technical Services (CATS+)
- Fairfax County Public Schools
- Maryland Department of Information Technology (DoIT) Hardware Master Contract
- Cisco Virginia Association of State College and University Purchasing Professionals (VASCUPP)
- Federal Reserve Board 202000834

CISCO TOP-FIVE MID-ATLANTIC SLED PARTNER 2019 & 2020

CISCO OUTSTANDING SOLUTIONS PARTNER OF THE YEAR 2016

SARA Standards American Registrations Authority REGISTERED ISO 9001:2015

CBE Certified Business Enterprise Program

Inc. 500 | 5000

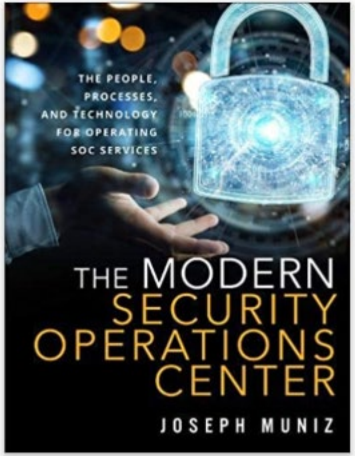
2016 INNER CITY 100 ICIC

HALL OF FAME AWARD

NFF

Security Building Blocks and SOAR

Joey Muniz
Senior Cybersecurity Architect
Cisco Systems


THE PEOPLE, PROCESSES, AND TECHNOLOGY FOR OPERATING SOC SERVICES
THE MODERN SECURITY OPERATIONS CENTER
JOSEPH MUNIZ

CISCO
SECURE

The bridge to possible

Building Blocks for SOAR

Security Orchestration, Automation and Response

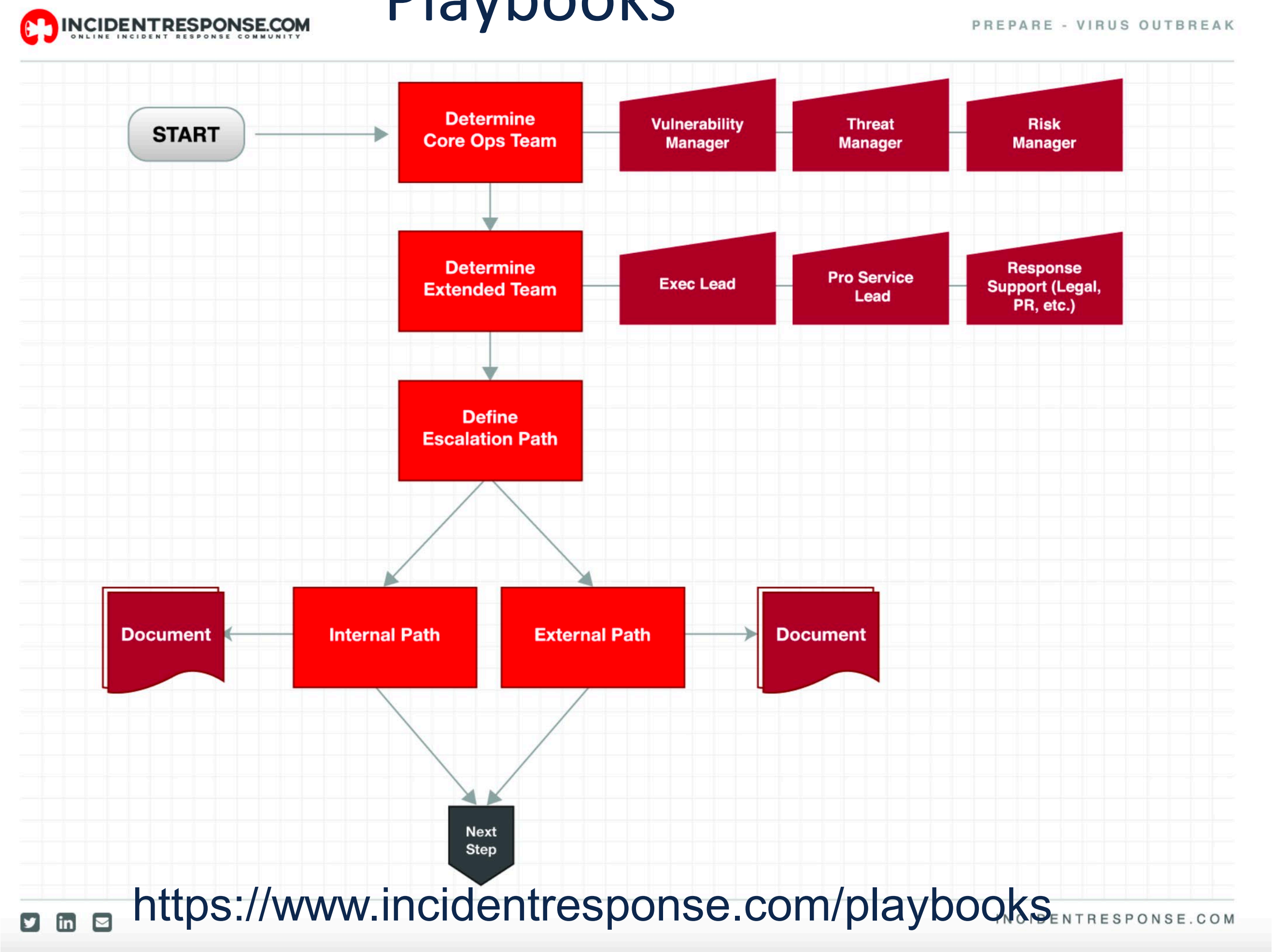
SOC Services

- **Risk Management** – Addressing all forms of organizational risk
- **Compliance** – Addressing compliance requirements
- **Vulnerability Management –** Addressing **t**echnical vulnerabilities
- **Analysis –** Analyzing artifacts and event data
- **Incident Response** – Responding to cyber attacks
- **Digital Forensics** – Post event forensics and preparation for legal action
- **Situational and Security Awareness –** Training organization about security programs
- **Research and Development** – Understanding threat landscape and technologies

ISACA COBIT Maturity Levels

Grade	
0 – No Program	No Capabilities or Processes
1 – Ad Hoc	Recognized problems. Ad hoc Approach
2 – Repeatable but intuitive	Some process but no formal training or procedures. Self ran
3 - Defined Process	Documented process but up to individual to follow
4. – Managed and Measurable	Monitor and manage compliance. Action can be taken to improve

Playbooks



INCIDENTRESPONSE.COM
ONLINE INCIDENT RESPONSE COMMUNITY

PREPARE - VIRUS OUTBREAK

START

Determine Core Ops Team

Vulnerability Manager

Threat Manager

Risk Manager

Determine Extended Team

Exec Lead

Pro Service Lead

Response Support (Legal, PR, etc.)

Define Escalation Path

Document

Internal Path

External Path

Document

Next Step

INCIDENTRESPONSE.COM

https://www.incidentresponse.com/playbooks

SIEM

Security Information and Event Management – Centralized log collection from various tools to mine data and respond to events

SOAR

Security Orchestration, Automation and Response – Collects data from a range of sources and automates response when possible

XDR

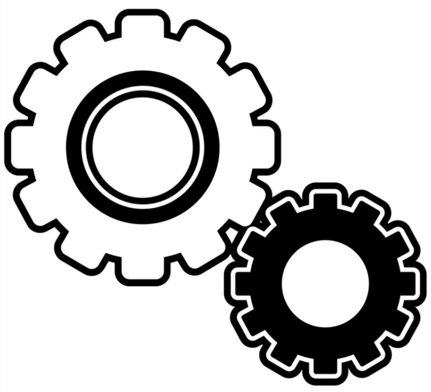
Endpoint Detection and Response (EDR)– Uses local detection and cloud capabilities to detect threats on endpoints

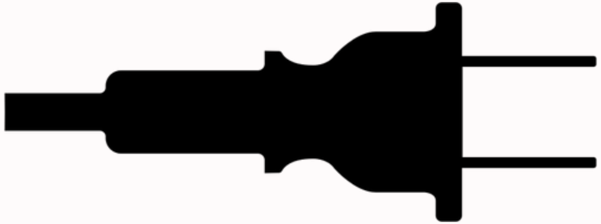
(XDR) – X represents multiple data sources to expand EDR. XDR is the future of EDR allowing for network, endpoint and cloud data.

Does SOAR or XDR Require a SIEM?

SOAR Vendors

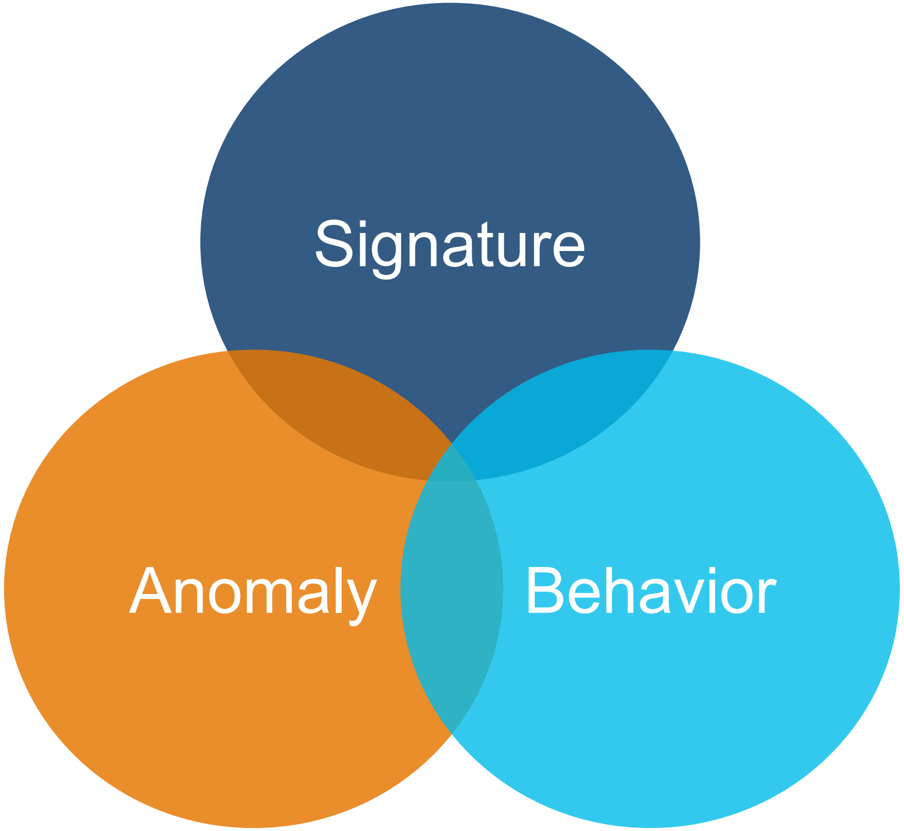
Need a SIEM to get Data



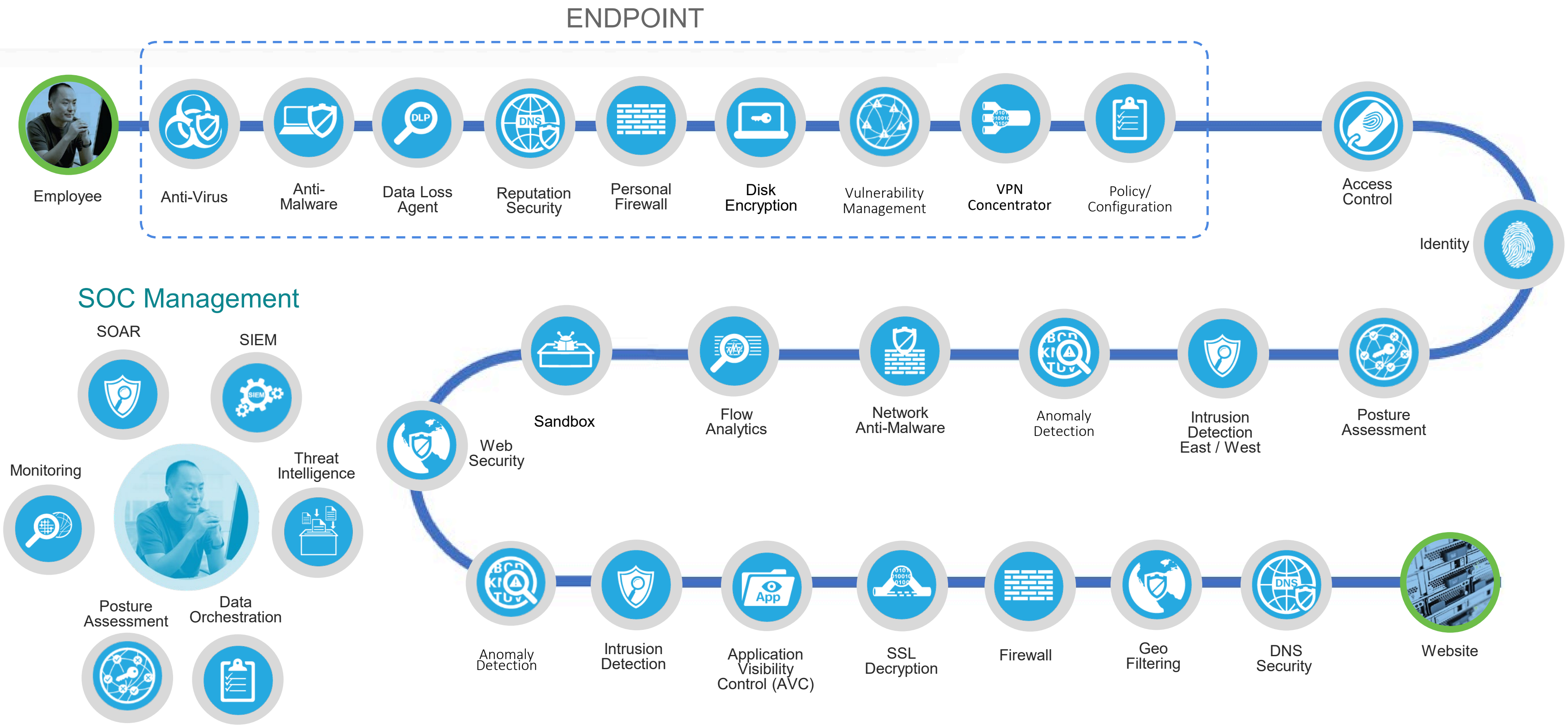


SecureX Does Not … **But Can Make Your SIEM Better**

Security Capabilities



Average Security Tools for Defense in Depth



ENDPOINT

Employee

Anti-Virus

Anti-Malware

Data Loss Agent

Reputation Security

Personal Firewall

Disk Encryption

Vulnerability Management

VPN Concentrator

Policy/ Configuration

Access Control

Identity

Posture Assessment

Intrusion Detection East / West

Anomaly Detection

Network Anti-Malware

Flow Analytics

Sandbox

Web Security

Anomaly Detection

Intrusion Detection

Application Visibility Control (AVC)

SSL Decryption

Firewall

Geo Filtering

DNS Security

Website

SOC Management

SOAR

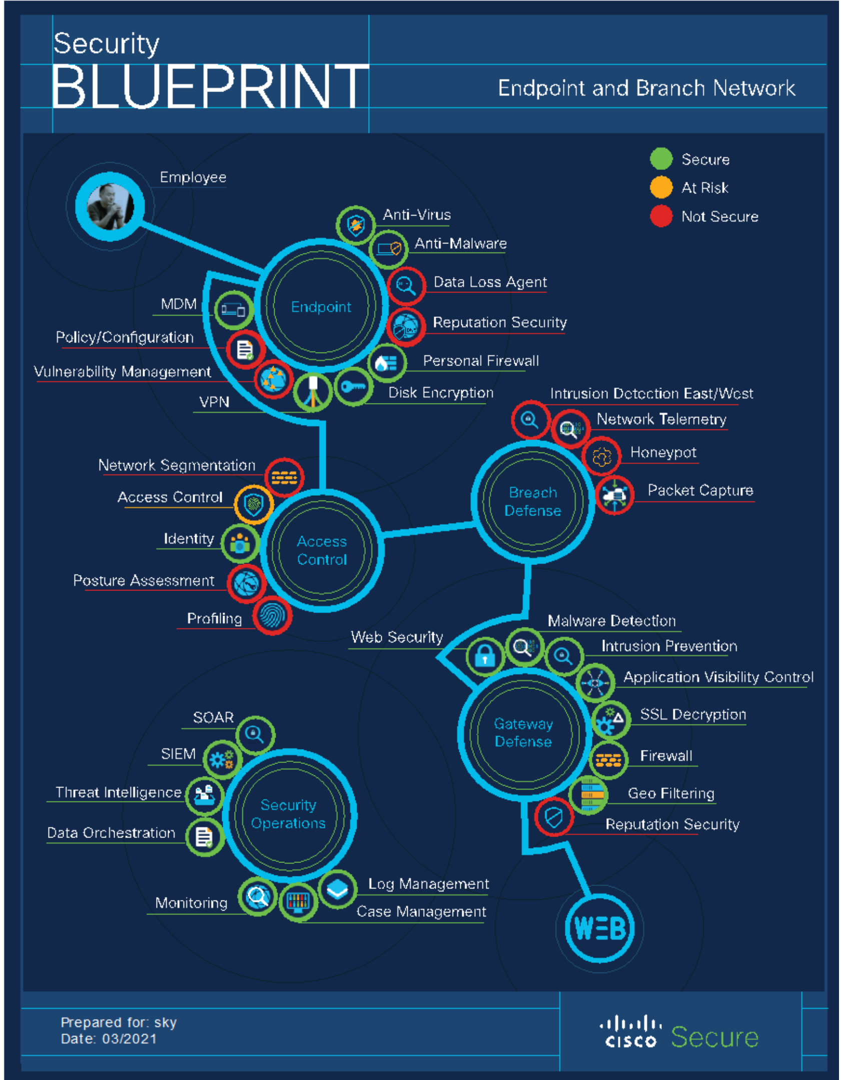
SIEM

Monitoring

Threat Intelligence

Posture Assessment

Data Orchestration



Security
BLUEPRINT

Endpoint and Branch Network

🟢 Secure
🟠 At Risk
🔴 Not Secure

Employee

Endpoint
Anti-Virus
Anti-Malware
Data Loss Agent
Reputation Security
Personal Firewall
Disk Encryption
VPN
Vulnerability Management
Policy/Configuration
MDM

Breach Defense
Intrusion Detection East/West
Network Telemetry
Honeypot
Packet Capture

Access Control
Network Segmentation
Access Control
Identity
Posture Assessment
Profiling

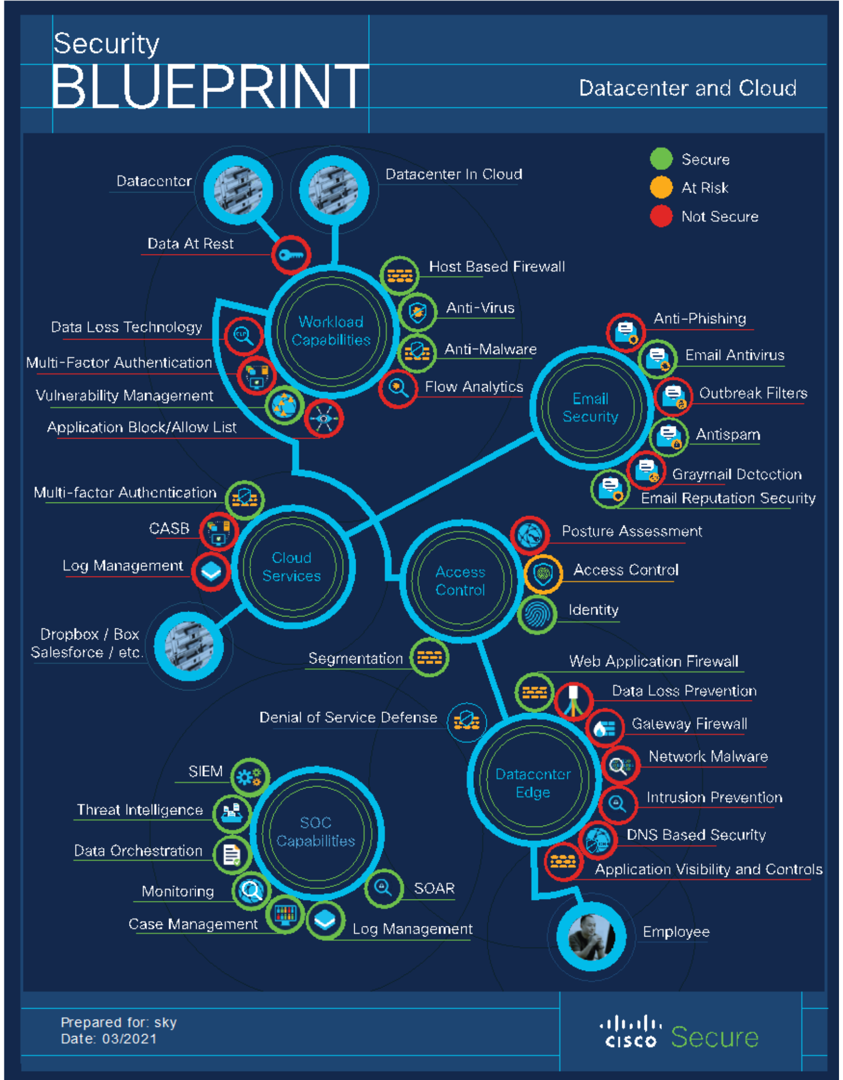
Gateway Defense
Web Security
Malware Detection
Intrusion Prevention
Application Visibility Control
SSL Decryption
Firewall
Geo Filtering
Reputation Security

WEB

Security Operations
SOAR
SIEM
Threat Intelligence
Data Orchestration
Monitoring
Log Management
Case Management

Prepared for: sky
Date: 03/2021

cisco Secure



Security
BLUEPRINT

Datacenter and Cloud

🟢 Secure
🟠 At Risk
🔴 Not Secure

Datacenter
Datacenter In Cloud
Data At Rest

Workload Capabilities
Host Based Firewall
Anti-Virus
Anti-Malware
Flow Analytics
Data Loss Technology
Multi-Factor Authentication
Vulnerability Management
Application Block/Allow List

Email Security
Anti-Phishing
Email Antivirus
Outbreak Filters
Antispam
Graymail Detection
Email Reputation Security

Cloud Services
Multi-factor Authentication
CASB
Log Management
Dropbox / Box
Salesforce / etc.

Access Control
Posture Assessment
Access Control
Identity
Segmentation

Datacenter Edge
Web Application Firewall
Data Loss Prevention
Gateway Firewall
Network Malware
Intrusion Prevention
DNS Based Security
Application Visibility and Controls
Denial of Service Defense

SOC Capabilities
SIEM
Threat Intelligence
Data Orchestration
Monitoring
Case Management
Log Management
SOAR

Employee

Prepared for: sky
Date: 03/2021

cisco Secure

Can’t Answer: What Happened?????

Can’t Answer: What Happened?????

Vulnerabilities

Malicious Sources

Key For SOAR - DevOps

Making things work with things

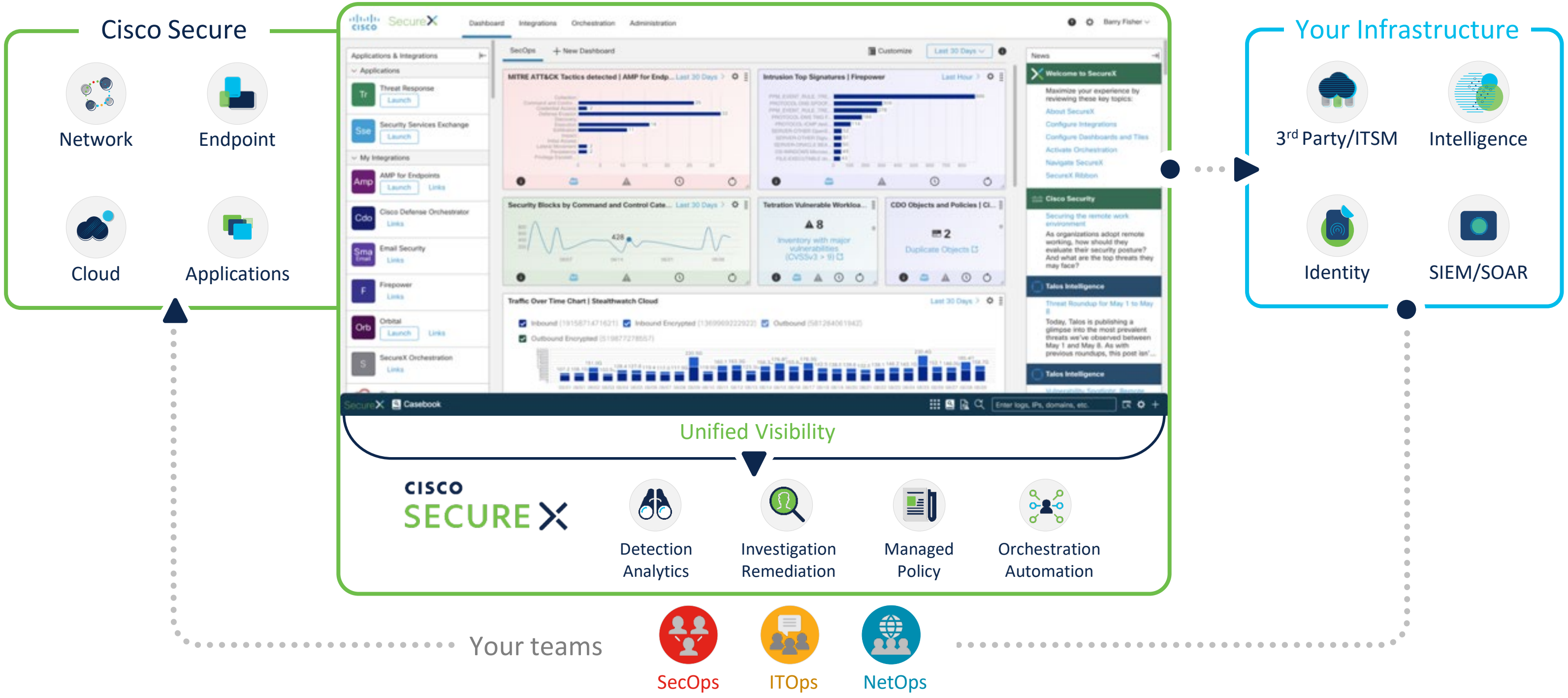
Developer.cisco.com

Jenkins
CHEF
ANSIBLE
puppet

Industry: *Make This Easier!*

Introducing SecureX

A cloud-native, built-in platform experience within our portfolio



Intro to 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

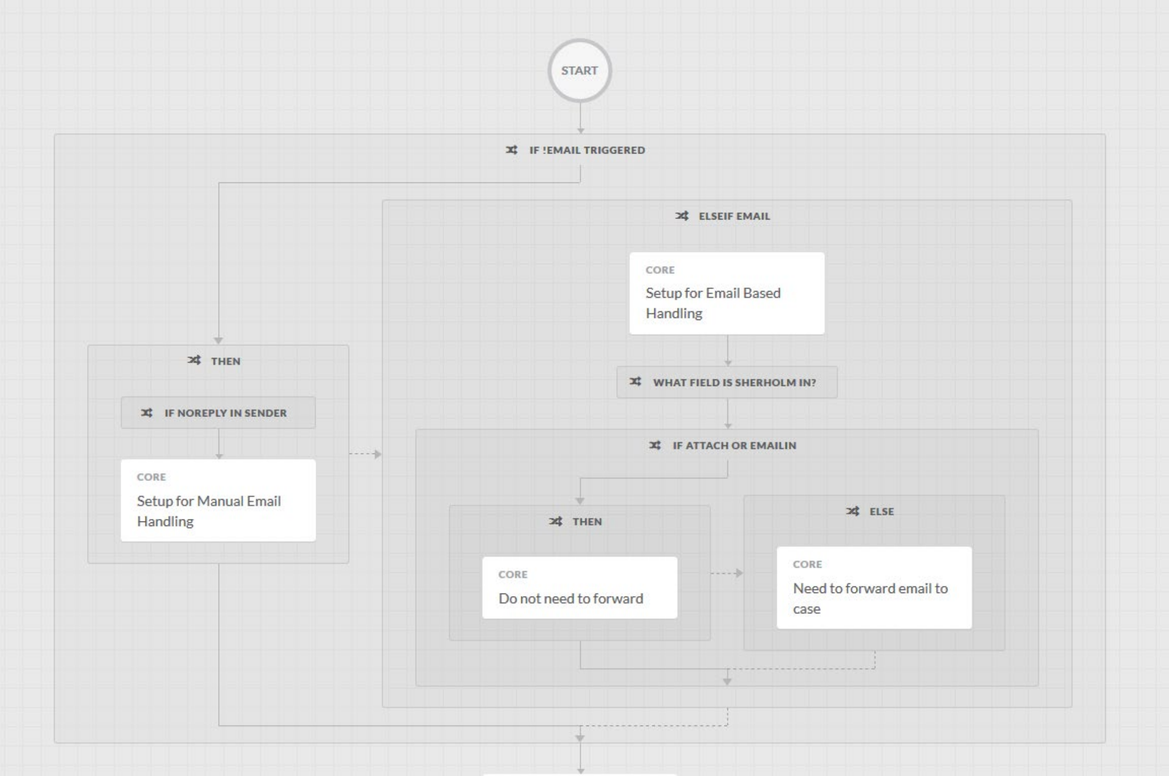
Unique turnkey approach to quickly integrate with other systems and solutions to expand your toolbox

Scale

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

Workflows

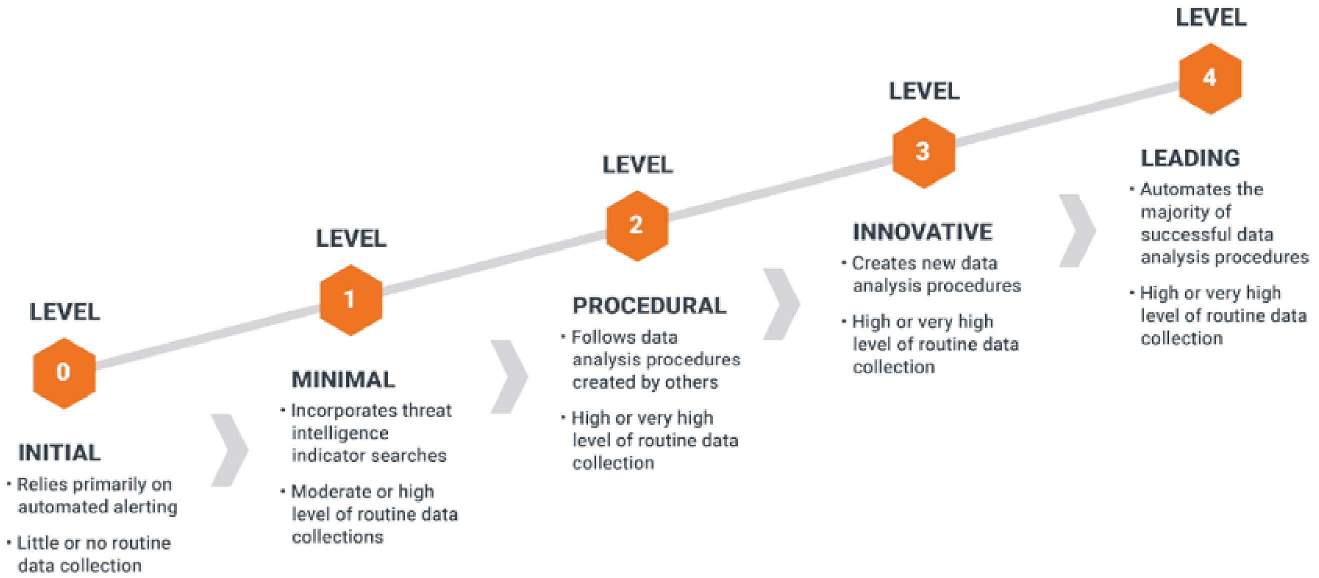
- A simple or complex series of activities that accomplish a task or series of tasks
- Built using the drag and drop workflow editor



Threat Hunting

Proactive – Hunting for a Hypotheses

Reactive – Responding security events



LEVEL 0

INITIAL

- Relies primarily on automated alerting
- Little or no routine data collection

LEVEL 1

MINIMAL

- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collections

LEVEL 2

PROCEDURAL

- Follows data analysis procedures created by others
- High or very high level of routine data collection

LEVEL 3

INNOVATIVE

- Creates new data analysis procedures
- High or very high level of routine data collection

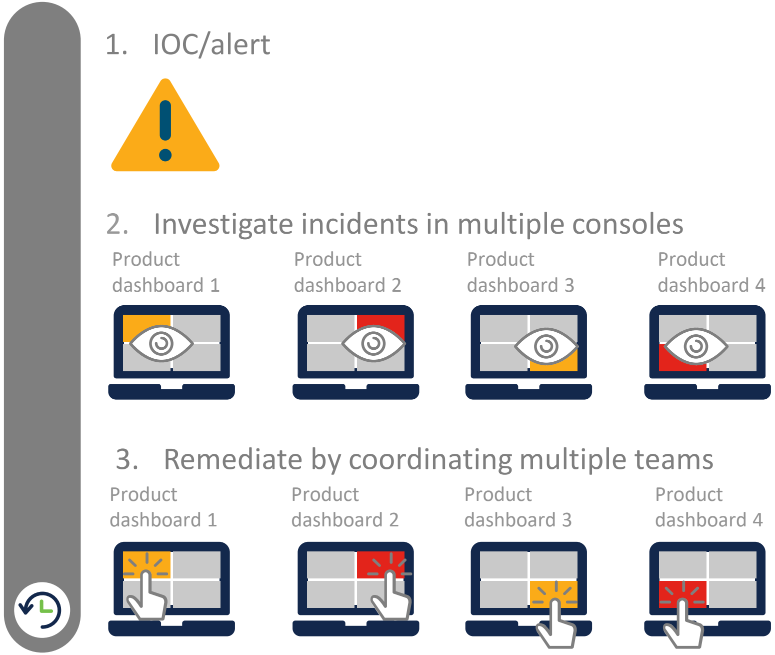
LEVEL 4

LEADING

- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

Threat Hunting Simplified

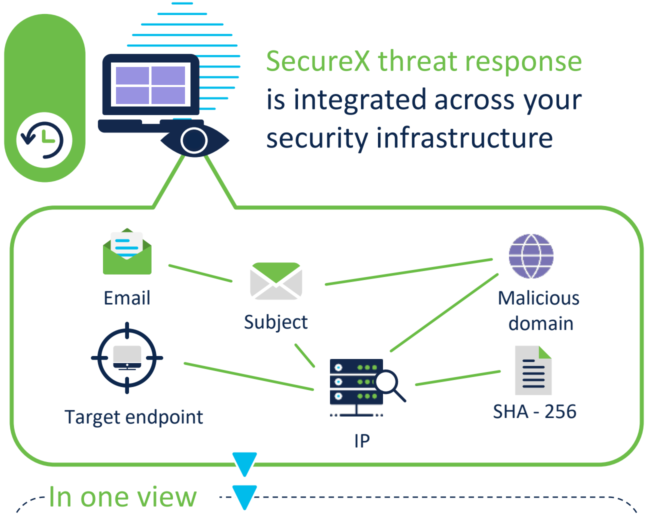
Before: 32 minutes



1. IOC/alert
2. Investigate incidents in multiple consoles

3. Remediate by coordinating multiple teams

After: 5 minutes



SecureX threat response is integrated across your security infrastructure

In one view

Query intel and telemetry from multiple integrated products

Quickly visualize the Threat impact in your environment

Remediate directly from one UI

Go To:
SecureX threat response deep dive

Next Steps

- Learn DevOps Concepts: developer.cisco.com
- Build Playbooks: www.incidentresponse.com/playbooks
- dCloud Labs: dCloud.cisco.com
- Security Blueprint: ciscosecurityblueprint.com

  (use jomuniz@cisco.com as your point of contact)

THANK YOU

cisco SECURE

Security Transformation: University of the District of Columbia

Mike Rogers
Executive Director,
Information Services and Management
University of the District of Columbia

Jonathan Topping
Principal Architect /
Director of Solutions Architecture
Networking For Future

Security Transformation: University of the District of Columbia

University of the District of Columbia 1851

University of the District of Columbia Overview

- Established by Abolitionist Myrtilla Miner in 1851
- Only Public University in the Nation's Capital
- Committed to a Mission of Education, Research, and Community Service

Where We Started Our Security Journey

- "Flat" Network – Little to no separation of network users / devices
- No Threat Inspection – Unable to see / address bad actors
- No Identity – Unable to determine who / what is on the network

Where We Are Today On Our Security Journey

- Macro and Micro Segmentation
- Threats Mitigated at Multiple Layers (IPS / Malware / DNS)
- End-to-End Visibility of Who and What is on the Network

What's Left On Our Security Journey

- Utilize Segmentation to Further Restrict Access
- Endpoint Security Management
- Multi-Factor Authentication
- Automation – Turn the data to quick action

Advice:

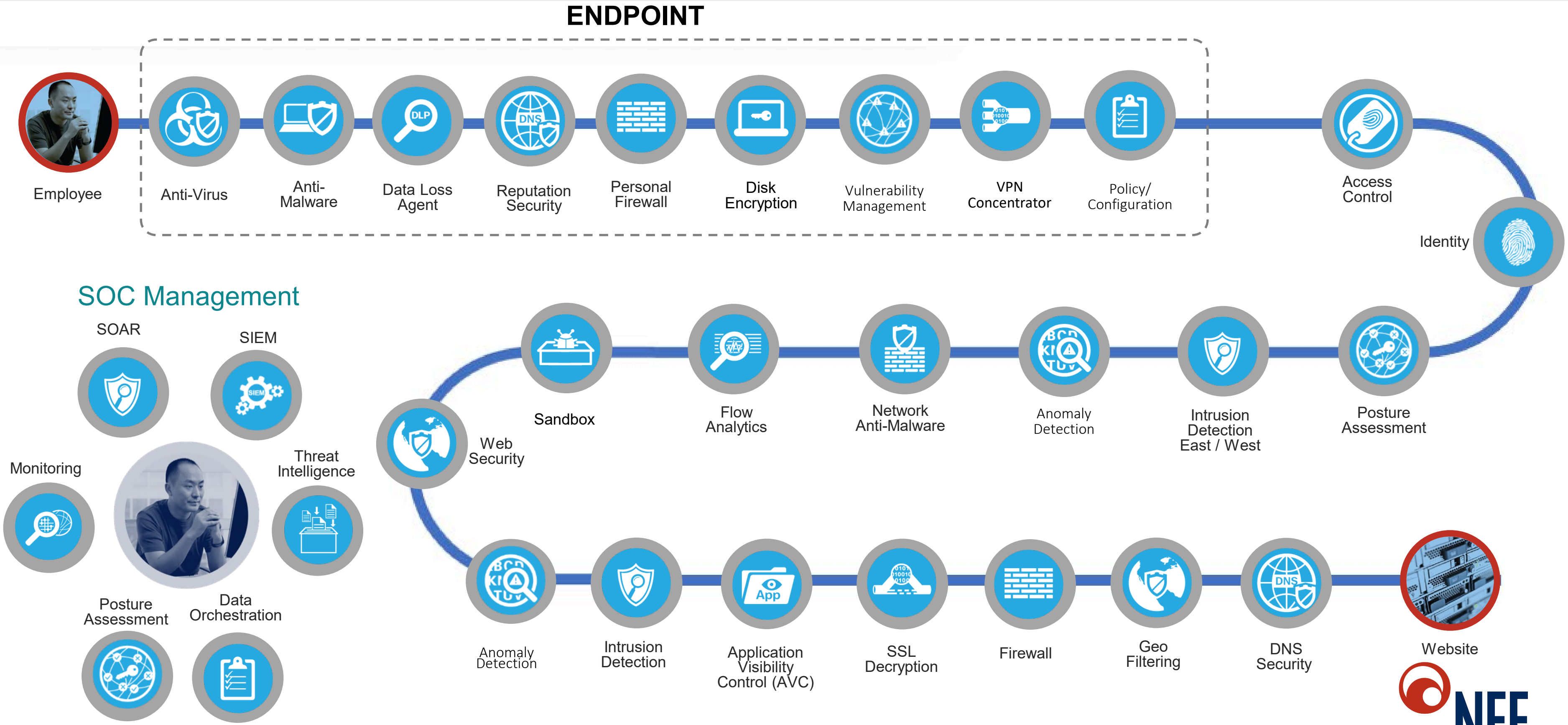
- Triage Weak Points
- Get Data First
- Intelligence and Response Come Next
- Make It Easy on Your Users
- Inform, But Don't Spam
- Prevent "Hurdles"

NFF

Cybersecurity Solutions

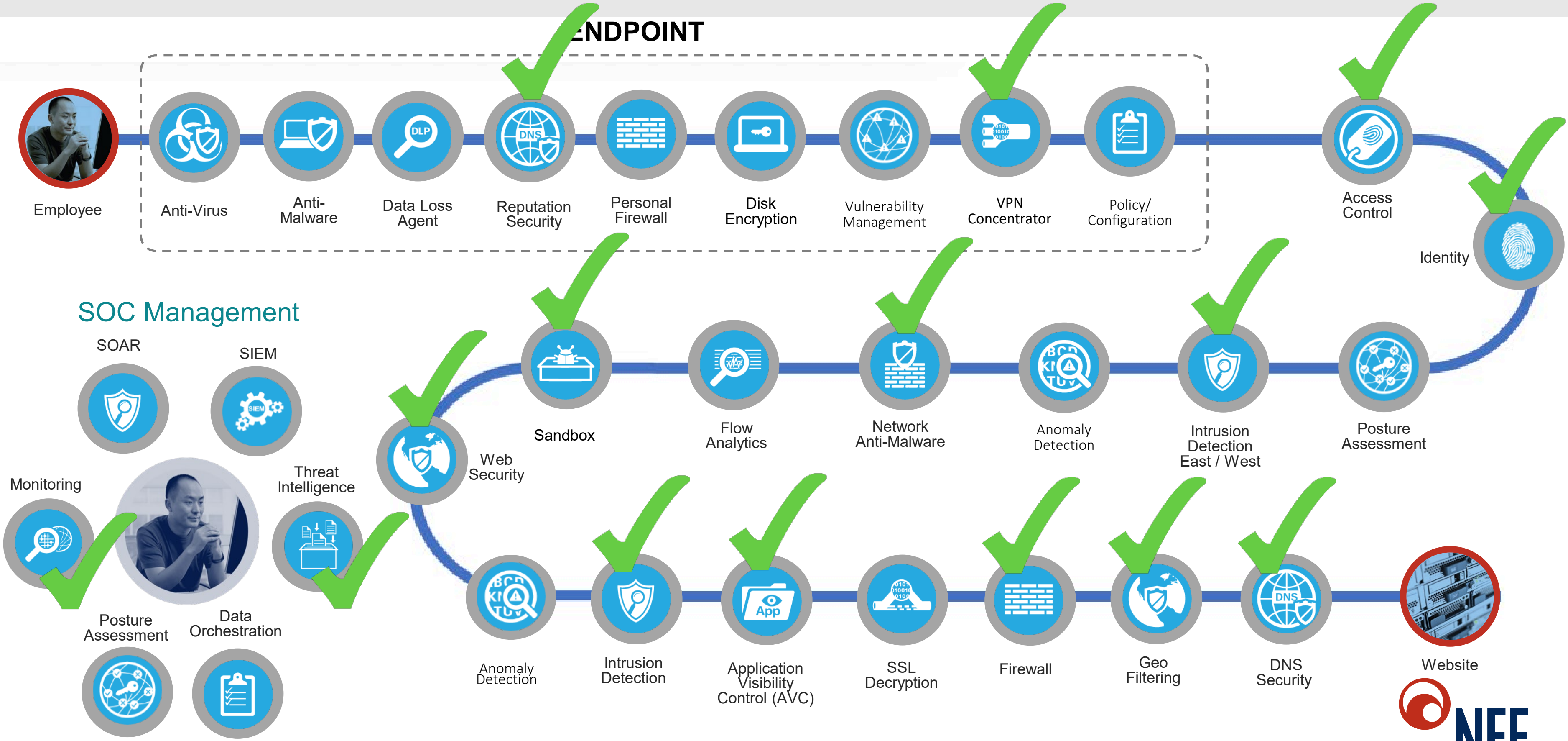
Jonathan Topping
Principal Architect / Director of Solutions Architecture
Networking For Future

UDC CASE STUDY MAPPED TO DEFENSE IN DEPTH



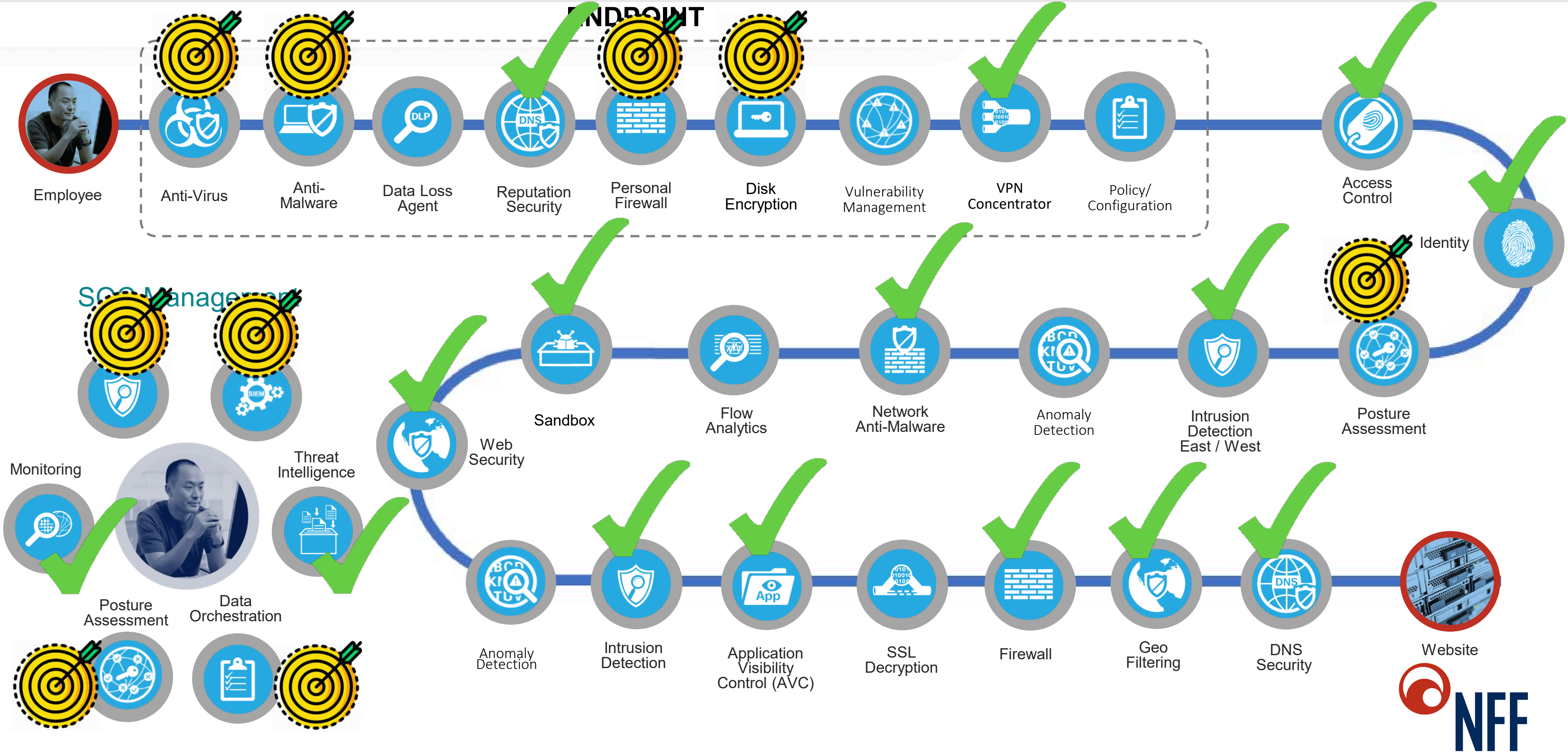
NFF

UDC CASE STUDY MAPPED TO DEFENSE IN DEPTH



NFF

UDC CASE STUDY MAPPED TO DEFENSE IN DEPTH



ENDPOINT

Employee

Anti-Virus

Anti-Malware

Data Loss Agent

Reputation Security

Personal Firewall

Disk Encryption

Vulnerability Management

VPN Concentrator

Policy/ Configuration

Access Control

Identity

Posture Assessment

Intrusion Detection East / West

Anomaly Detection

Network Anti-Malware

Flow Analytics

Sandbox

Web Security

Anomaly Detection

Intrusion Detection

Application Visibility Control (AVC)

SSL Decryption

Firewall

Geo Filtering

DNS Security

Website

SOC Management

Monitoring

Threat Intelligence

Posture Assessment

Data Orchestration

Final Thoughts

Questions and Answers

(submit via chat)

Your performance improvement is our measure of success.

Thank You!