Security Operations in real life

Marek Kumpošt

It takes 20 years to build a reputation and few minutes of a cyber-incident to ruin it.

~ Stephane Nappo

Small company

- Typically no security team at all
- One man show
  - Sometimes not even that
- Security is a function of IT team or IT admin
- Security is perceived as not much important domain
  - It is mostly about backup and authentication services
- Pros/Cons
  - + at least one person, who spells Security right ☺
  - - lack of knowledge/experience of just one person

Taking security (more) seriously

- Typically after a major security incident
- Or audit

- Before these two happen
  - Minimal budget
  - Minimal human resources
  - Minimal respect for Security (aka “why we should be a target”)

Medium-sized company

- Small all-purpose team
  - Dealing with operational/infrastructure/application layers
  - Still “nobody knows everything aspect”
- Security is perceived as unnecessary evil
  - Maybe after a data breach.
- Pros/Cons
  - + Dedicated security team
  - - Budget aspect
  - - Limited experience with various aspects of Security

Big company or large enterprises

- Big dedicated team or teams
  - Not all of them necessarily focused on security
  - Privacy team, for instance
- Focused on different areas of security
- Pros/Cons
  - + Dedicated teams
  - + Detailed experience in various security domains
  - + Might have a dedicated budget
  - - Security costs a lot
  - - Slower speed of innovation

Example of focused Security (sub)teams

- Security Engineering
- Security Architecture
- Security Operations Center
- Application Security
- Pentesting Team
- Security Consulting Team
- CISO

Security Architecture

- Ensures that security best practices are addressed
- Defines overall security policies/standards/procedures
- Makes sure that new technologies fits withing existing ones
- Performs risk assessments
- Prevent bad designs
- May focus on Operations/Application/Product

Security Engineering

- “Build tools, techniques and methods to support the development and maintenance of systems that can resist malicious attacks that are intended to damage a computer-based system or its data.”
- Example of tools for:
  - SIEM (Security Information and Event Management)
    - Build with ELK, Splunk, OSSEC, etc.
  - FIM (File Integrity Monitoring)
    - Technologies like Qualys, Tanium, LogRythm
  - Network segmentation
    - PaloAlto, CISCO, Illumio
  - (Micro)Services management (or container security)

Istio

Linkerd v2

Consul

Security Operations Centre

- Breaches in 2020: 3950
- Large business victims: 72%
- Sm./Med. business victims: 28%
- Targeting web apps: 43%
- Avg cost of a large breach: $392 million

Security Operations Centre – Key objectives

- Manages and Coordinates the response to Cyber Threats and Incidents
- Monitors the Cyber Security posture and reports deficiencies
- Ability to correlate system, application, network, server, security logs in a consistent way
- Performs Threat and Vulnerability Analysis
- Performs Analysis of Cyber Security Events
- Maintains an Internal Database of Cyber Security Incidents
- Provide Alerts and Notifications to General and Specific Threats
- Provide regular reporting to Management and Cyber Incident Responders

Security Operations Centre – Some more key objectives

Ability to automate the requirement to meet compliance – vulnerability assessment and risk management

Ensure change control function is integrated into the SOC process

Identification for all security attack vectors and classification of incidents

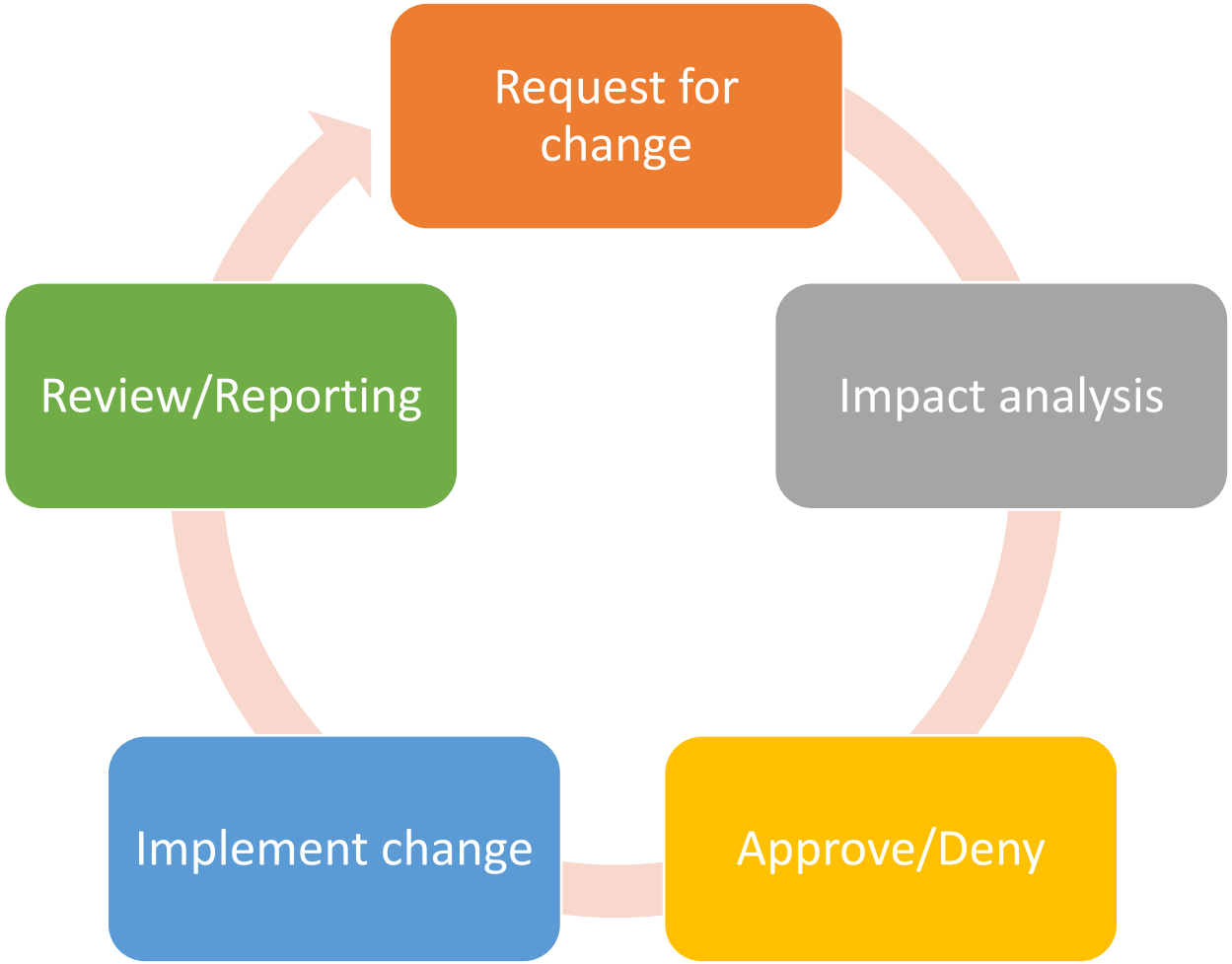
Define disaster recovery plans for ICE (in-case of emergency).

Build a comprehensive reporting dashboard that is aligned to security metrics

Proactive Security Monitoring based on predefined security metrics / KPI

Examples of SecOps processes

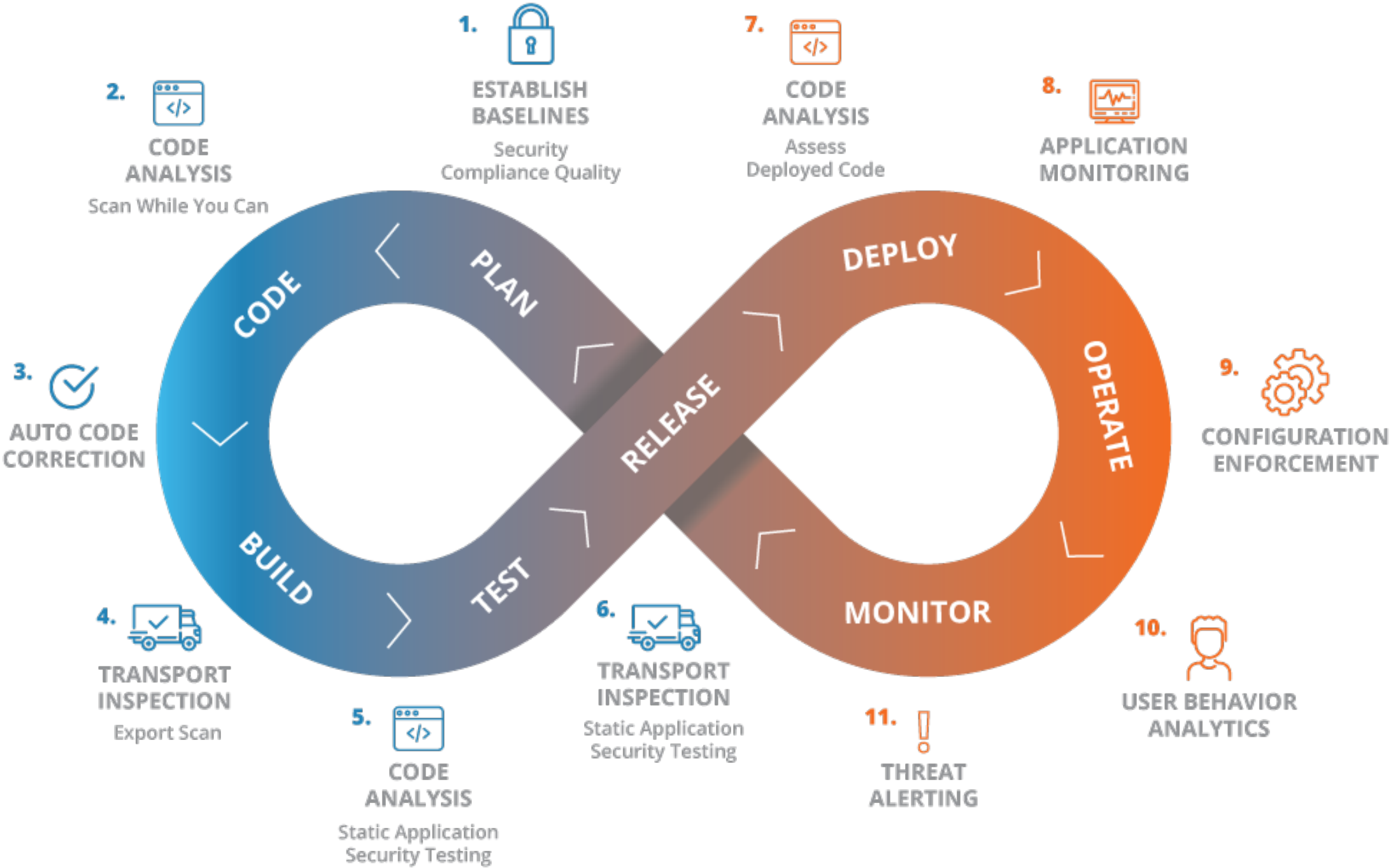
Secure change management lifecycle



Security Design Review – Operations view

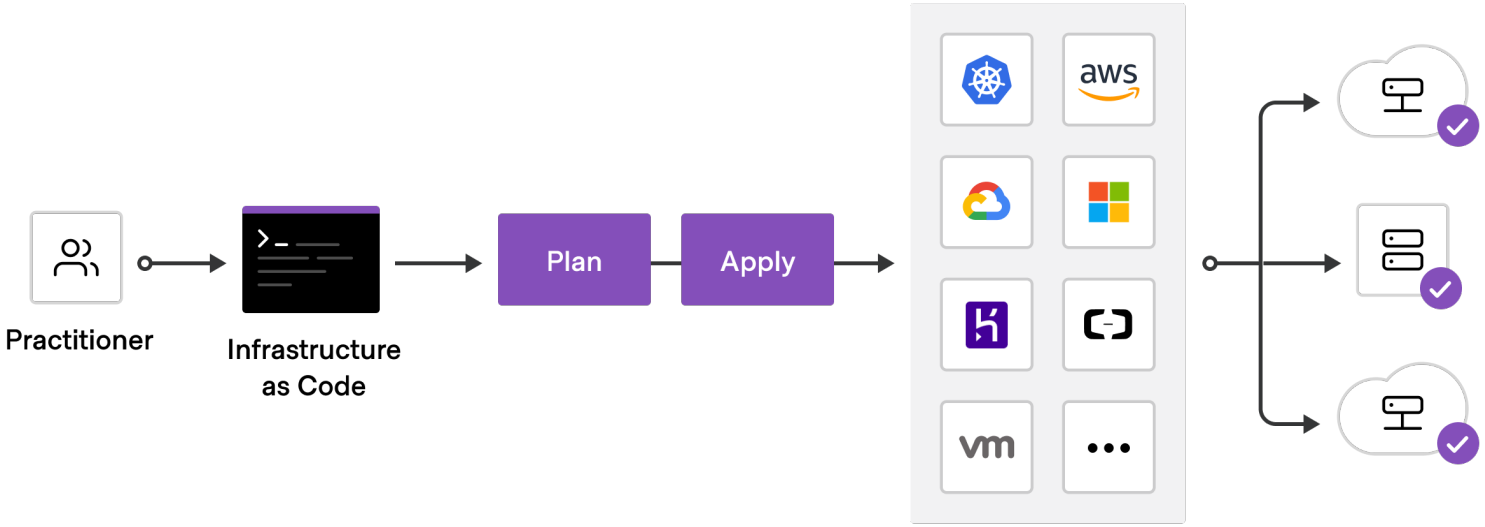
Justification for change	Use-cases	Environments in scope	Logical network diagrams
Network access control	User access control	Data sensitivity and data encryption	Logging, monitoring auditing
Vulnerability management	Business continuity and disaster recovery	Secrets management	…

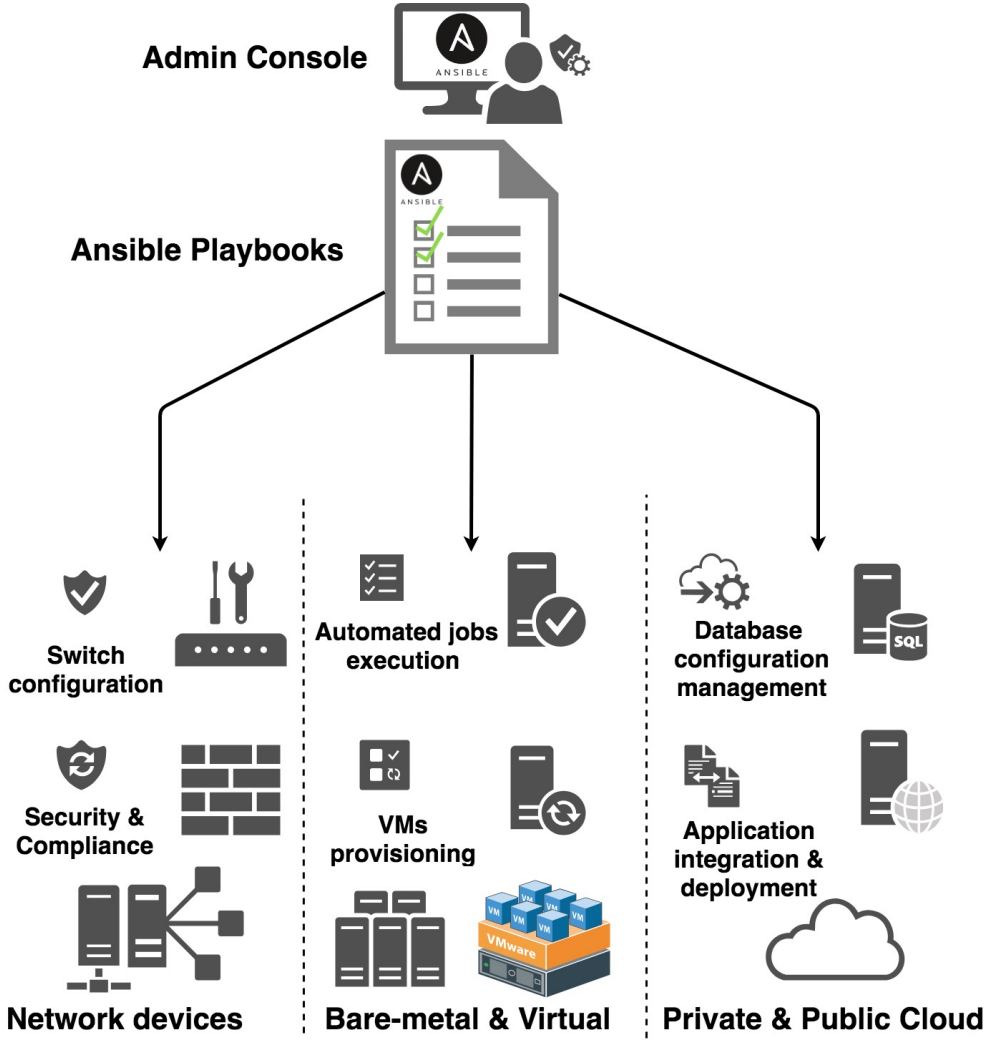
DevSecOps concept


1.
ESTABLISH BASELINES
Security
Compliance Quality
2.
CODE ANALYSIS
Scan While You Can
3.
AUTO CODE CORRECTION
4.
TRANSPORT INSPECTION
Export Scan
5.
CODE ANALYSIS
Static Application Security Testing
6.
TRANSPORT INSPECTION
Static Application Security Testing
7.
CODE ANALYSIS
Assess Deployed Code
8.
APPLICATION MONITORING
9.
CONFIGURATION ENFORCEMENT
10.
USER BEHAVIOR ANALYTICS
11.
THREAT ALERTING
CODE
PLAN
BUILD
TEST
RELEASE
DEPLOY
OPERATE
MONITOR

DevSecOps in the light of SecOps

- Software defined Data Centers
  - AWS, Azure, Google Cloud, OCI
- Security driven by code (Ansible, Terraform,..)





Examples of Security Frameworks

CIS controls v8 (formerly SANS top 20)

- Focuses on activities, rather than who manages the devices
- Consists of 18 controls
  - Aims to cover critical processes/activities in a company
- Contains 153 safeguards
  - Grouped to implementation groups (IG1/2/3)
- Provides mapping to well known frameworks
  - CSF, ATT&CK, CSA, PCI, SOC2, …

CONTROL 01 Inventory and Control of Enterprise Assets

5 Safeguards — IG1 2/5 — IG2 4/5 — IG3 5/5

CONTROL 02 Inventory and Control of Software Assets

7 Safeguards — IG1 3/7 — IG2 6/7 — IG3 7/7

CONTROL 03 Data Protection

14 Safeguards — IG1 6/14 — IG2 12/14 — IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software

12 Safeguards — IG1 7/12 — IG2 11/12 — IG3 12/12

CONTROL 05 Account Management

6 Safeguards — IG1 4/6 — IG2 6/6 — IG3 6/6

CONTROL 06 Access Control Management

8 Safeguards — IG1 5/8 — IG2 7/8 — IG3 8/8

CONTROL 07 Continuous Vulnerability Management

7 Safeguards — IG1 4/7 — IG2 7/7 — IG3 7/7

CONTROL 08 Audit Log Management

12 Safeguards — IG1 3/12 — IG2 11/12 — IG3 12/12

CONTROL 09 Email and Web Browser Protections

7 Safeguards — IG1 2/7 — IG2 6/7 — IG3 7/7

CONTROL 10 Malware Defenses

7 Safeguards — IG1 3/7 — IG2 7/7 — IG3 7/7

CONTROL 11 Data Recovery

5 Safeguards — IG1 4/5 — IG2 5/5 — IG3 5/5

CONTROL 12 Network Infrastructure Management

8 Safeguards — IG1 1/8 — IG2 7/8 — IG3 8/8

CONTROL 13 Network Monitoring and Defense

11 Safeguards — IG1 0/11 — IG2 6/11 — IG3 11/11

CONTROL 14 Security Awareness and Skills Training

9 Safeguards — IG1 8/9 — IG2 9/9 — IG3 9/9

CONTROL 15 Service Provider Management

7 Safeguards — IG1 1/7 — IG2 4/7 — IG3 7/7

CONTROL 16 Applications Software Security

14 Safeguards — IG1 0/14 — IG2 11/14 — IG3 14/14

CONTROL 17 Incident Response Management

9 Safeguards — IG1 3/9 — IG2 8/9 — IG3 9/9

CONTROL 18 Penetration Testing

5 Safeguards — IG1 0/5 — IG2 3/5 — IG3 5/5

CIS Control 04: Secure Configuration of Enterprise Assets and Software

SAFEGUARDS				IMPLEMENTATION GROUPS			APPLICABILITY	
NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3	INCLUDED?	JUSTIFICATION
4.6	**Securely Manage Enterprise Assets and Software** Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet and HTTP, unless operationally essential.	Network	Protect	●	●	●	Yes	Organizations developing mobile applications and infrastructure should use modern, secure management protocols. Organizations should ensure that applications selected for management of the deployed devices utilize secure transport protocols.
4.7	**Manage Default Accounts on Enterprise Assets and Software** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	Users	Protect	●	●	●	No	This is typically not a concern with mobile devices, unless the device is rooted or jailbroken.
4.8	**Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.	Devices	Protect		●	●	Yes	Users should be educated on the implications of obtaining and installing mobile apps from insecure locations, or on iOS signed with developer or enterprise signatures.

Another Security Framework

The Cybersecurity Framework (NIST)

Three Primary Components

Core

Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

Profiles

Alignment of an organization's requirements and objectives, risk appetite and resources ***using*** the desired outcomes of the Framework Core

Implementation Tiers

A qualitative measure of organizational cybersecurity risk management practices

Key Framework Attributes

Principles of Current and Future Versions of the Framework

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector

The Framework Core

Establishes a Common Language

Function
Identify
Protect
Detect
Respond
Recover

- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

An Excerpt from the Framework Core

The Connected Path of Framework Outcomes

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5 Functions 23 Categories 108 Subcategories 6 Informative References

Implementation Tiers

The Cybersecurity Framework Version 1.1

	1	2	3	4
	Partial	**Risk Informed**	**Repeatable**	**Adaptive**
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization: • **monitors and manages supply chain risk**[1.1] • benefits my sharing or receiving information from outside parties			

https://facilitycyber.labworks.org/

0 of 108 Answered

0% COMPLETE

- **Identify**
  - **Asset Management**
  - Business Environment
  - Governance
  - Risk Assessment
  - Risk Management Strategy
  - Supply Chain Risk Management
- Protect
- Detect
- Respond
- Recover
- Results

Asset Management

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

	Fully Implemented	Largely Implemented	Partially Implemented	Not Implemented
1. Physical devices and systems within the organization are inventoried *Hardware inventory keeps a record of all the devices and allows administrators to discover what assets are on the network and to quickly locate information about these devices. It is important to know what exactly is on the network so that vulnerabilities can be identified.* *Implementation Notes* >	✓	✓	✓	✗
2. Software platforms and applications within the organization are inventoried *All programs installed on a computer should be tracked and managed by keeping an up-to-date inventory that tracks software versions and patch history. Vulnerabilities of a network can be better identified if all of the deployed software is known.* *Implementation Notes* >	✓	✓	✓	✗
3. Organizational communication and data flows are mapped *All communication between devices is defined to indicate how information should be transferred within and outside your facility network. During an incident, this information may be referred back to as to what normal network traffic should look like.*	✓	✓	✓	✗

And one more ☺

MITRE ATT&CK (attack.mitre.org)

- Adversarial Tactics, Techniques & Common Knowledge
- Aim is to
  - Categorise adversarial behaviours based on real-world observations
- Used for offensive and defensive activities, measurements, reporting, …
- Can be heavily customized
  - Enterprise, Mobile, PRE-ATT&CK

MITRE ATT&CK™

MITRE ATT&CK® Navigator

Defense Evasion 34 techniques	Credential Access 14 techniques	Discovery 24 techniques	Lateral Movement 9 techniques
Modify Authentication Process		System Service Discovery	Remote Services
	Network Sniffing		Software Deployment Tools
	OS Credential Dumping	Application Window Discovery	
Direct Volume Access	Input Capture		Replication Through Removable Media
Rootkit	Brute Force	System Network Configuration Discovery	
Obfuscated Files or Information	Two-Factor Authentication Interception		Internal Spearphishing
		System Owner/User Discovery	Use Alternate Authentication Material
Injection	Exploitation for Credential Access		
Manipulation		System Network Connections Discovery	Lateral Tool Transfer
Modification	Steal Web Session Cookie		Taint Shared Content
ontrol Mechanism	Unsecured Credentials	Permission Groups Discovery	Exploitation of Remote Services
Indicator Removal on Host	Credentials from Password Stores		
Modify Registry		File and Directory Discovery	Remote Service Session Hijacking
Trusted Developer Utilities Proxy Execution	Steal or Forge Kerberos Tickets		
		Peripheral Device Discovery	
Traffic Signaling	Forced Authentication		
Signed Script Proxy Execution	Steal Application Access Token	Network Share Discovery	
		Password Policy Discovery	
Rogue Domain Controller	Man-in-the-Middle	Browser Bookmark Discovery	
Indirect Command Execution		Virtualization/Sandbox Evasion	
BITS Jobs			

Example: What happened in SolarWinds

Security company FireEye release a blog saying a bad hacker or group called UNC2452 has hacked SolarWinds

IT Company SolarWinds says it may have been hit in a highly sophisticated attack

18,000 companies, government agencies, think tanks, universities and NGOs affected

https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

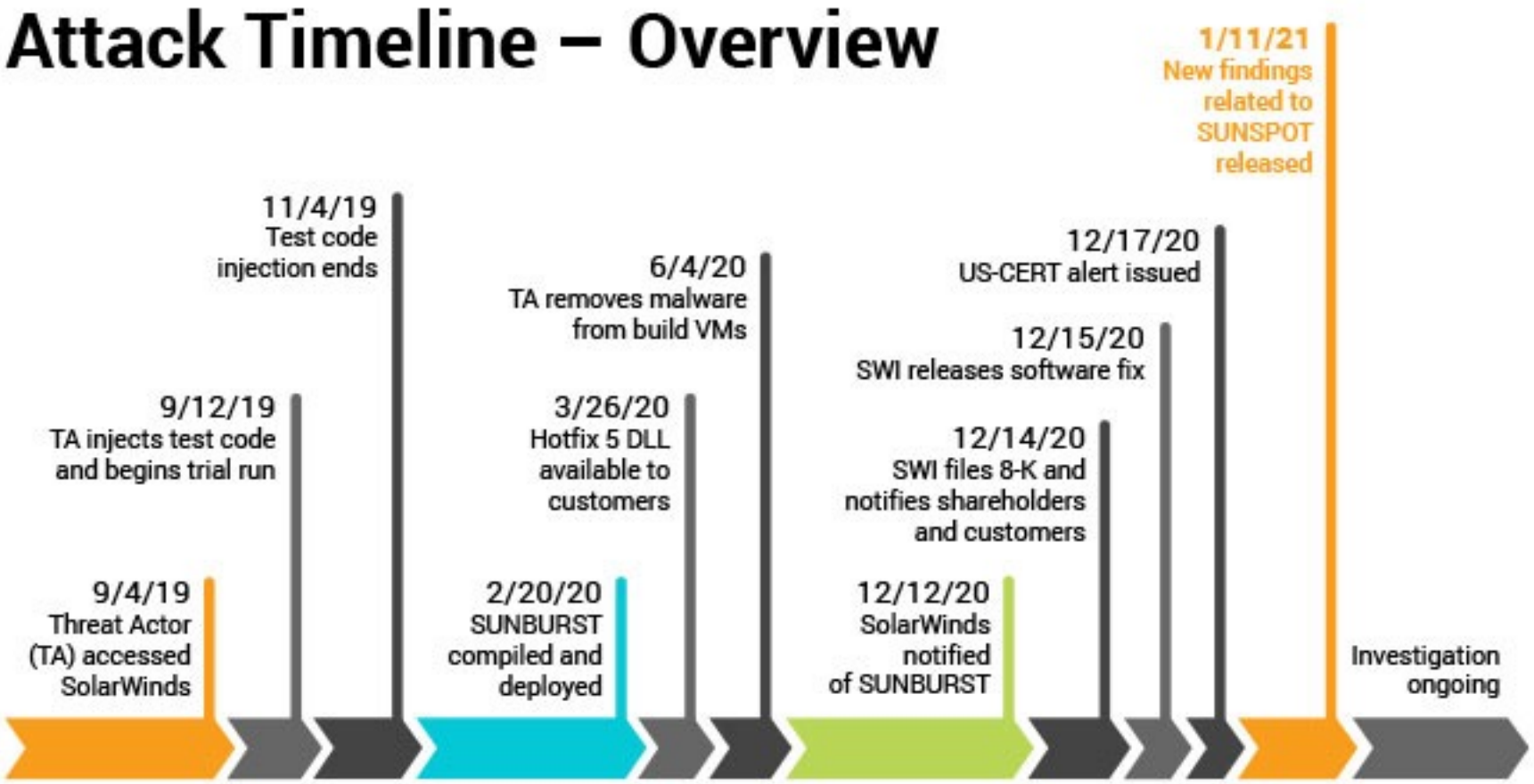
The Vector

- SolarWinds?
  - Software Company
    - Network Management Products
    - Orion is one of their popular products
  - Customers
    - Governments and major corporations
    - SolarWinds Orion was approved for use in many sensitive areas
    - Orion customers were careful and kept SolarWinds patched & updated

The Targets

- SUNBURST only activated if installed at one of a handful of places
  - 18,000 companies installed SUNBURST malware
  - 14 days later SUNBURST would peek out
  - SUNBURST would go live only if it was worth it
  - Everywhere else, SUNBURST went to sleep indefinitely

When



All events, dates, and times approximate and subject to change; pending completed investigation.

Actor’s Traits

- Very Sophisticated
  - Clean up trace evidence
  - Good security on their own servers
  - Good ability to hide their servers
  - Extensive efforts to hide their exploit

- Motivation Murky
  - Limited target selection among the 18,000
  - No financial interest
  - No Denial of Service
  - No data destruction or ransomware
  - No Personal Information Theft

Nobody likes compliance but it is important

- Company complies with regulations
- Legal requirements
- Internal policies and standards
- Helps companies pass external audits
- Identifies new compliance issues
- Conducts internal audits

Thanks!

marek@kumpost.net