Security Operations and Incident Analysis

Network Security Workshop

What is a SOC?

- Security Operations Centre
- Centralized command center for network security event monitoring and incident response.
- responsible for detecting, analyzing, and reporting unauthorized or malicious network activity

- All SOCs require:
  - Effective tools
  - security analysts with comprehensive technical backgrounds
  - strong relationships with external organizations

SOC vs NOC

Security Operations Centre

- Focus on incidents and alerts that affect the security of information assets
- SOC analyst require security and reverse engineering skills

Network Operations Centre

- Monitor and maintain the network infrastructure
- Meet SLAs and manage incidents to reduce downtime
- Focus on availability and performance

SOC and NOC should complement each other

Types of SOC

Threat-centric SOCs

- proactively hunts for malicious threats on network; a simpler, scalable, threat-centric approach that addresses security across the entire attack continuum: before, during, and after an attack.

Compliance-based SOCs

- focused on comparing the compliance posture of network systems to reference configuration templates and standard system builds

Operational-based SOCs

internally focused organization that is tasked with monitoring the security posture of an organization's internal network

Roles in a SOC

Role	Description / Responsibility
SOC Manager	• Prioritize work • Organize resources with the goal of detecting, investigating, and mitigating incidents that could impact the business; • Determine day-to-day activities and base skills required by to perform the job successfully
Security Analyst	• Have foundation knowledge in basic networking, traffic capture, and device monitoring
Incident Response Handler	• Manage incident • Execute containment strategies and • Ensure the IR process is followed throughout
Forensics specialist	• Gather, retain, and analyze data for investigative purposes • Maintain the integrity of the data.
Malware reverse engineering specialist	• Analyze the malware behaviors in depth to determine the relevant tactics, techniques, and procedures, and the indicator of compromises. • May also write signatures to detect, hunt, and prevent the malware.

Security Analysts

Tier 1

- Continuously monitors the alert queue.
- Triages security alerts.
- Monitors the health of the security sensors and endpoints.

Tier 2

- Performs deep-dive incident analysis by correlating data from various sources.
- Determines if a critical system or data set has been impacted.

Tier 3

- Possesses in-depth technical knowledge on the network, endpoint, threat intelligence, forensics, malware reverse engineering, and the functioning of specific applications or underlying IT infrastructure
- Acts as an incident hunter, not waiting for escalated incidents.

SOC Playbook

- Security analytics is accomplished by collecting, correlating, and analyzing a wide range of event data
  - Because complexity is the enemy of reliability and maintainability. the playbook is an answer to this complexity.
- A SOC playbook is a collection of plays, which are effectively custom reports that are generated from a set of data sources
  - PLAYS - self-contained, fully documented, prescriptive procedures for finding and responding to undesired activity

SOC Playbook

- Example: COPS - Collaborative Open Playbook Standard
  - https://github.com/demisto/COPS

- Playbook Fields:
  - id: a unique id of the playbook, usually UUID
  - name: playbook name
  - description: the purpose of the playbook
  - tasks: an (ordered) list of playbook tasks

Read: Running SOC Playbooks as a Code

Incident Analysis

Kill Chain Model

- Follows the steps of the attacker to successfully compromise the target.
- Goal is to disrupt one link of the chain to stop the attack

Diamond Model

- Maps an adversary's tactics, techniques and procedures (TTP)
- Shows the core features of every malicious activity and their underlying relationships
- Goal is to understand the attacker's motivation and tools

Kill Chain Model

- 7 phases:
  - Reconnaissance
  - Weaponization
  - Delivery
  - Exploitation
  - Installation
  - Command-and-control
  - Actions on objectives

Source: PwC

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Kill Chain Model - Example

Reconnaissance | Weaponization | Delivery | Exploitation | Installation | Command and Control | Action on Objective

1 Attacker gathers information to help them create seemingly trustworthy places and messages to stage their malvertisements and phishing emails.

2 Attacker tries to fool users into opening emails or clicking on links.

3 Staging sites redirect from trustworthy-looking sites to sites that launch exploit kits and/or other malicious content.

4 When a user is at the compromised site, their system is scanned for vulnerabilities that are then exploited to take control of the user's system.

Kill Chain Model - Example

Reconnaissance | Weaponization | Delivery | Exploitation | Installation | Command and Control | Action on Objective

Once an exploit has taken control, the final dropped file/tool is installed that will infect and encrypt the victim's system—the ransomware payload. **5**

Once infected, the malware calls home to a CnC server, where it retrieves keys to perform the encryption or receive additional instructions **6**

Files on a hard disk, mapped network drives, and USB devices are encrypted and a notice or splash-screen pops up with instructions to pay the ransom to restore the original files **7**

Diamond Model

Adversary

- An adversary is the entity responsible for conducting an intrusion. An intrusion is considered any malicious activity.

Capability

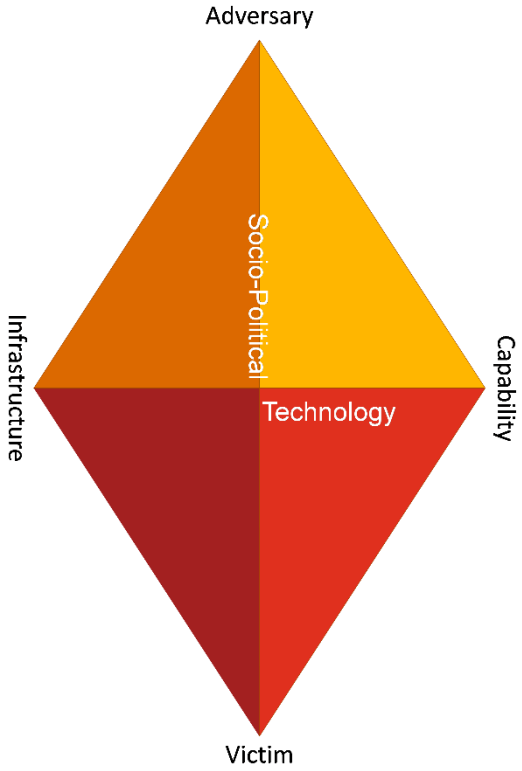
- A capability is a tool or technique that the adversary may use in an event

Victim

- The victim is the target of the adversary. As a SOC analyst, the victim is the customer.

Infrastructure

- Infrastructure is the physical or logical communications nodes that the adversary uses to establish and maintain command and control over their capabilities



Source: PwC

Read the whitepaper: https://www.threatintel.academy/diamond/

Security Data Collection

- Indicators of Compromise (IOC) data point that is extracted from security data and can be used as high fidelity predictor of system compromise.
- OpenIOC is an extensible XML schema to describe the technical characteristics that identify a known threat or methodology.

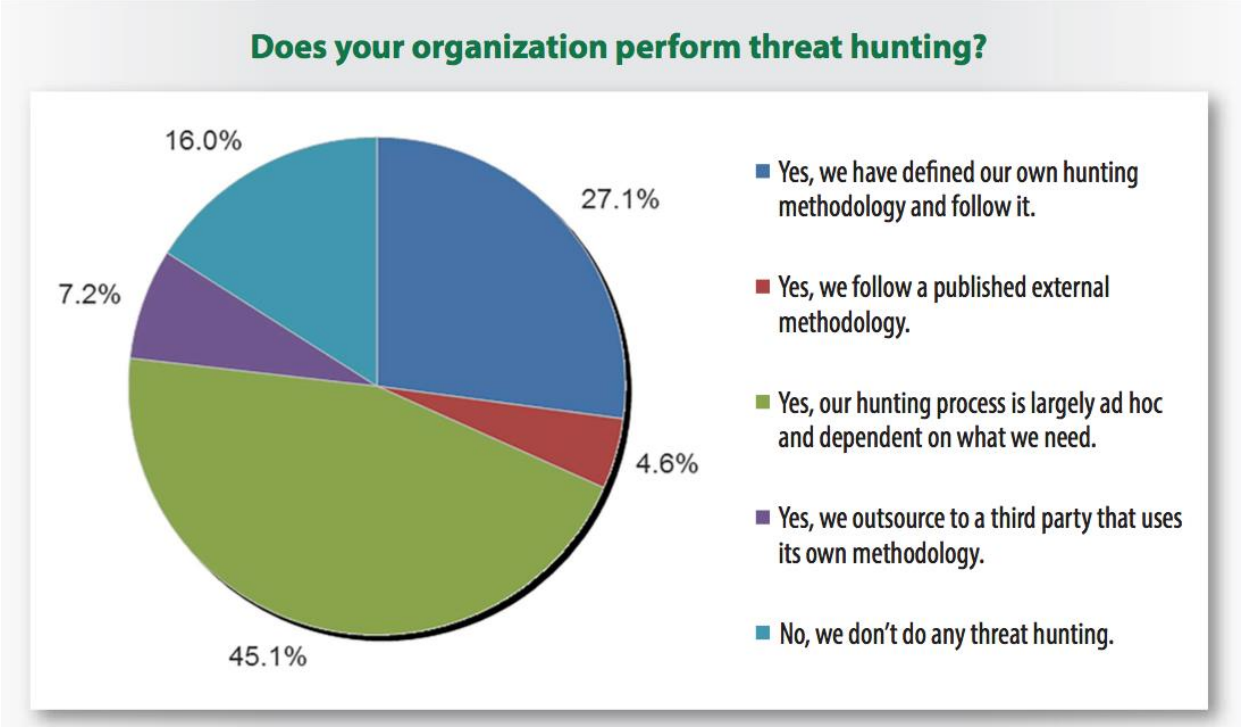
Hunting Cyber Threats

- a proactive approach to detect malicious activity that is not identified by traditional alerting mechanisms

threathunting.net

Hunting Cyber Threats

- Survey Results:
  - Most hunting organizations are reactive
  - Continuous hunting is not there yet



Source: The Who, What, Where, When, Why and How of Effective Threat Hunting

Hunting Maturity Model

HMM0
Initial

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

HMM1
Minimal

- Incorporates threat intelligence indicator searches
- Moderate or high level of routing data collection

HMM2
Procedural

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

HMM3
Innovative

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

HMM4
Leading

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

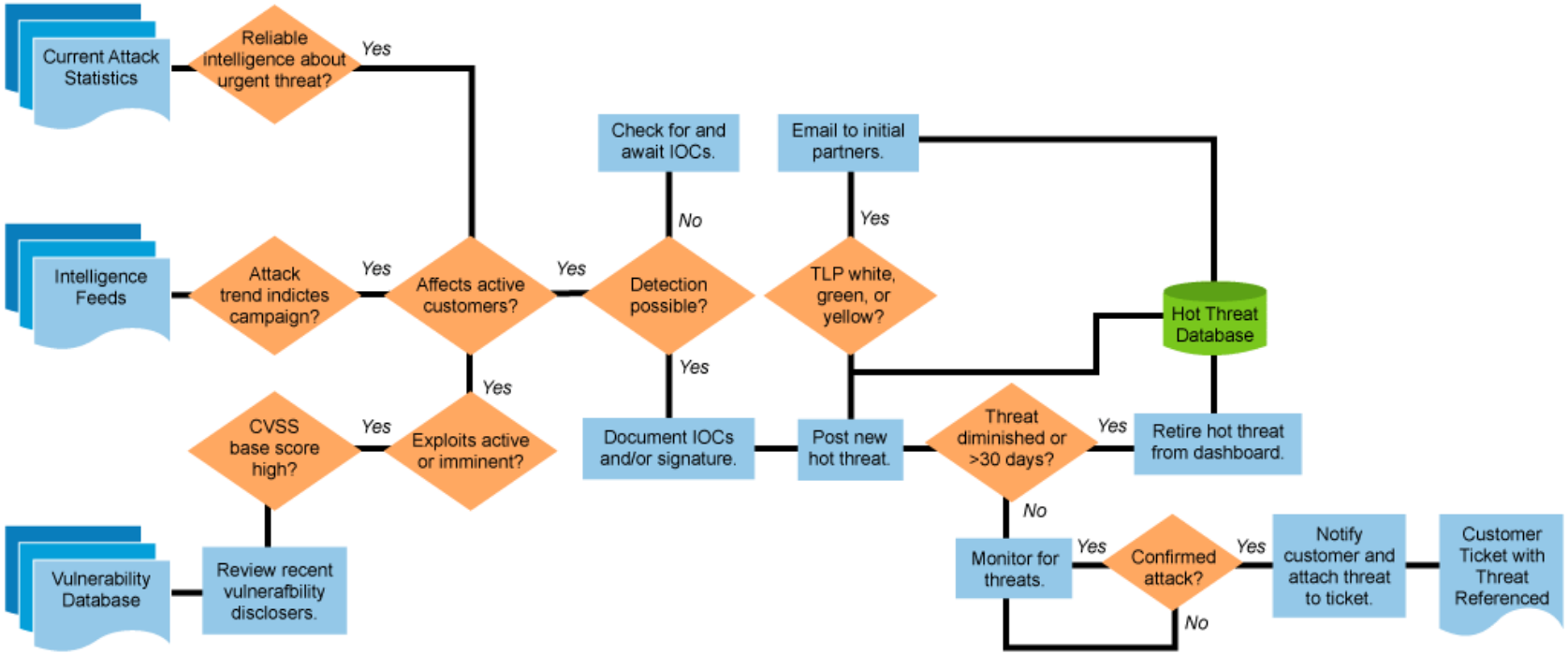
Source: A Simple Hunting Maturity Model

Hot Threat Dashboard

- A hot threat dashboard is a graphical depiction of currently monitored threats. It provides at-a-glance details about the top concerns for your network and resources.

Source: Implementing a Hot Threat Dashboard (Cisco)

Hot Threat Dashboard

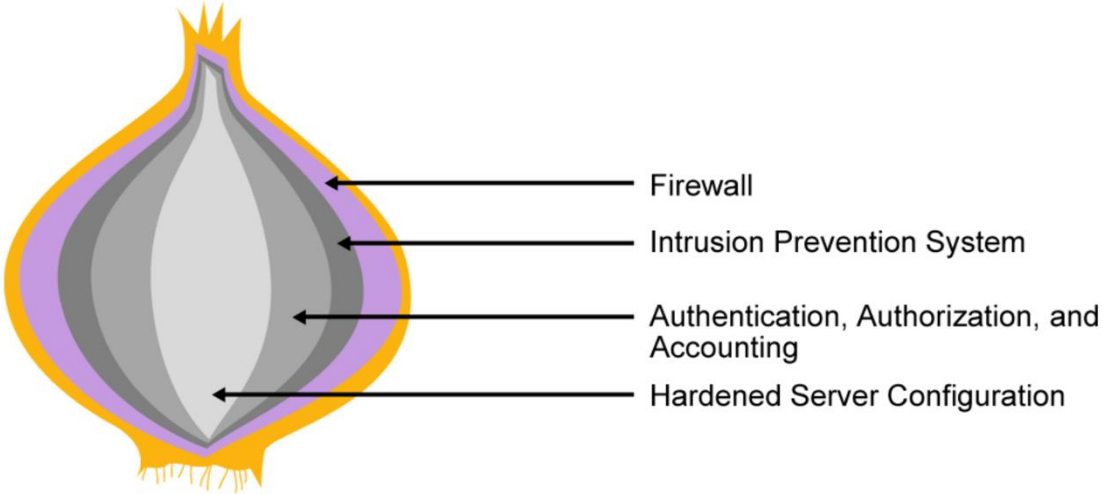


Source: Implementing a Hot Threat Dashboard (Cisco)

Network Security Technologies

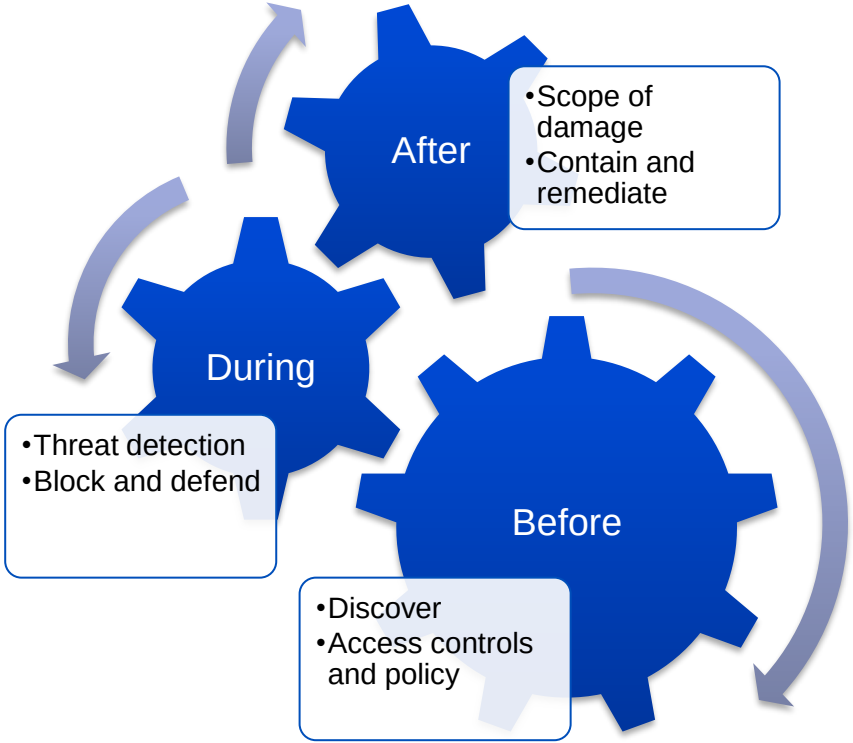
Defense-in-Depth Strategy

- A building block of other security design principles that applies a layer approach to security. It is aimed at providing redundancy controls at multiple levels to mitigate risk.



Network Security Technologies

- Defend across the attack continuum
  - A continuous model that is consistent with how companies secure, defend and audit their networks.
  - It is divided into 3 phases: before, during and after an attack.



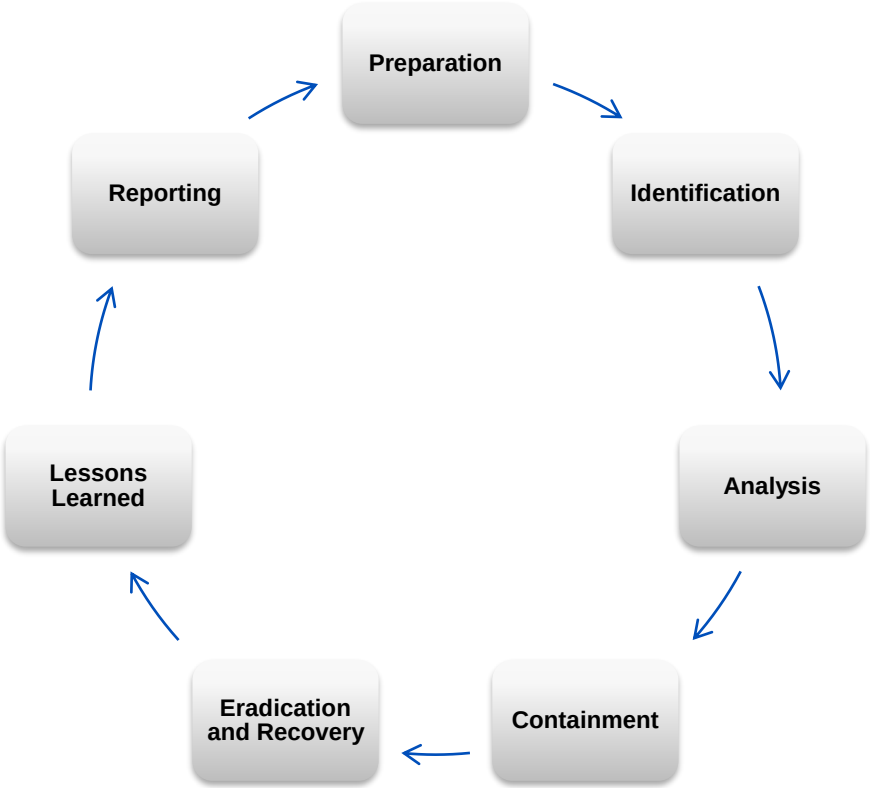
Source: Addressing the Full Attack Continuum (Cisco Whitepaper)

CSIRT

- Computer Security Incident Response Team

- Types:
  - PSIRT - software and hardware vendors
  - National CSIRT / CERT
    - Country-level CERT teams
  - MSSPs
    - Managed security services
  - Coordination Centres
    - Coordination between vendors, researchers, providers for vulnerability disclosure

Incident Response



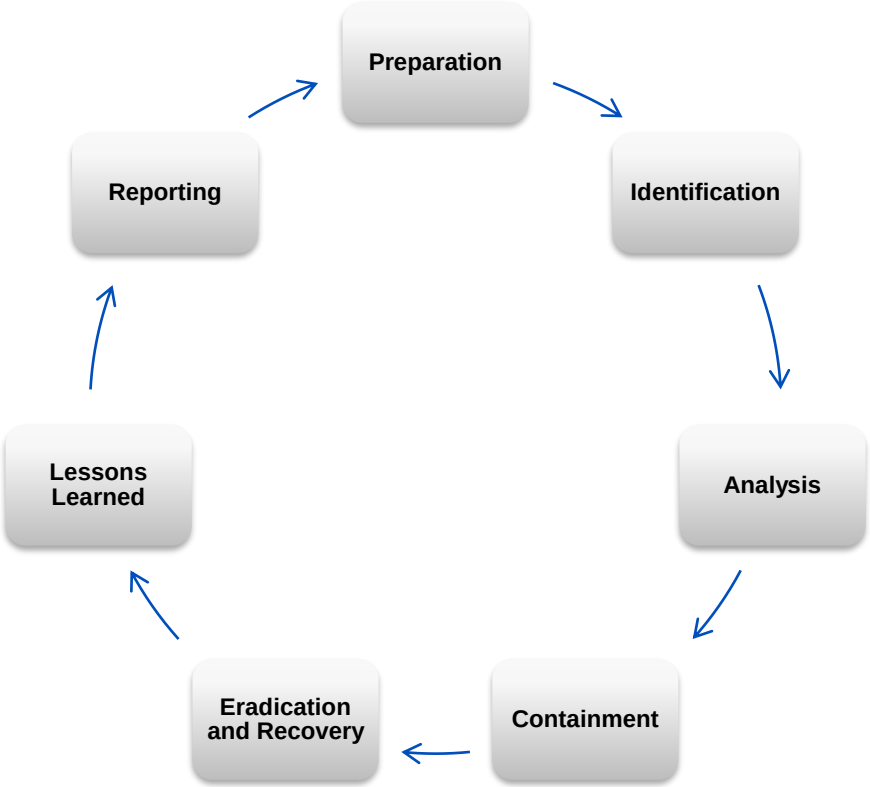
Preparation
Get the company and resources ready to handle security incident

Identification
When a true positive incident has been detected, the IR team is activated.

Analysis
The IR Team should work quickly to analyze and validate each incident, following a pre-defined process

Containment
Find scope of incident, network reachability, and how quickly containment is needed

Incident Response



Eradication and Recovery
Investigate to find origin of the incident and all traces of malicious code removed.

Lessons Learned
Analysis of how the incident happened and performs a Failure Mode and Effects Analysis (FMEA)

Reporting
Notify parties (internal and external) which occur at pre-defined intervals based on incident severity

CVSS 3.0

CVSS is a vendor agnostic, industry open standard that is designed to convey vulnerability severity and to help determine urgency and priority of response; does not calculate the chances of being attacked, but the chances of being compromised in the event of an attack and potential severity of damage.

https://www.first.org/cvss/calculator/3.0

GNU Bourne-Again Shell (Bash) 'Shellshock' Vulnerability (CVE-2014-6271)

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "Shellshock."

Metric	**Value**	**Comments**
Attack Vector	Network	Considering the worst case scenario: (web server attack vector).
Attack Complexity	Low	An attacker needs to only gain access to a listening service that uses the GNU Bash shell as an interpreter or interact with a GNU Bash shell directly.
Privileges Required	None	Some attack vectors do not require any privileges (e.g. CGI in web server).
Scope	Unchanged	No user interaction is required for an attacker to launch a successful attack.
Confidentiality Impact	High	The **vulnerable component** is the GNU Bash shell which is used as an interpreter for various services or can be accessed directly, therefore no change in scope occurs during the attack.
Integrity Impact	High	Allows an attacker to take complete control of the affected system.
Availability Impact	High	Allows an attacker to take complete control of the affected system.

https://www.first.org/cvss/examples

Case: WannaCry Ransomware

Microsoft | TechNet

United States (English) Sign in

Security TechCenter

Search TechNet with Bing

Home Security Updates Tools Learn Library Support

Security Advisories and Bulletins > Security Bulletins > 2017

MS17-013
MS17-012
MS17-011
MS17-010
MS17-009
MS17-008
MS17-007
MS17-006
MS17-005
MS17-004
MS17-003
MS17-002
MS17-001

Microsoft Security Bulletin MS17-010 – Critical

Print
Share

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

Version: 1.0

Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the **Affected Software and Vulnerability Severity Ratings** section.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

For more information about the vulnerabilities, see the **Vulnerability Information** section.

For more information about this update, see Microsoft Knowledge Base Article 4013389.

On this page

IN THIS ARTICLE

MS17-013
MS17-012
MS17-011
MS17-010
MS17-009
MS17-008
MS17-007
MS17-006
MS17-005
MS17-004
MS17-003
MS17-002
MS17-001

Vulnerability Information

Print
Share

Multiple Windows SMB Remote Code Execution Vulnerabilities

Remote code execution vulnerabilities exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerabilities could gain the ability to execute code on the target server.

To exploit the vulnerability, in most situations, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server.

The security update addresses the vulnerabilities by correcting how SMBv1 handles these specially crafted requests.

The following table contains links to the standard entry for each vulnerability in the Common Vulnerabilities and Exposures list:

Vulnerability title	CVE number	Publicly disclosed	Exploited
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0143	No	No
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0144	No	No
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0145	No	No
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0146	No	No
Windows SMB Remote Code Execution Vulnerability	CVE-2017-0148	No	No

Mitigating Factors

Microsoft has not identified any mitigating factors for these vulnerabilities.

Workarounds

The following workarounds may be helpful in your situation:

- **Disable SMBv1**
  For customers running Windows Vista and later

  See Microsoft Knowledge Base Article 2696547.

IN THIS ARTICLE

Search CVE List | Download CVE | Update an ID | Request a CVE ID | Data Feed

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Follow CVE

Full-Screen View

CVE-2017-0143

SMBv1 server in Microsoft Windows

What is the CVSS score?

CVE-ID

CVE-2017-0143 Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143
- BID:96703
- URL:http://www.securityfocus.com/bid/96703

Date Entry Created

20160909 Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20160909)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE list, which standardizes names for security problems.

SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

https://cve.mitre.org

NIST National Vulnerability Database

CVE-2017-0143 Detail

Modified

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

Source: MITRE **Last Modified:** 03/16/2017 + View Analysis Description

Quick Info

CVE Dictionary Entry: CVE-2017-0143
Original release date: 03/16/2017
Last revised: 03/17/2017
Source: US-CERT/NIST

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 8.1 High
Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H (legend)
Impact Score: 5.9
Exploitability Score: 2.2

CVSS Version 3 Metrics:

Attack Vector (AV): Network
Attack Complexity (AC): High
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS Severity (version 2.0):

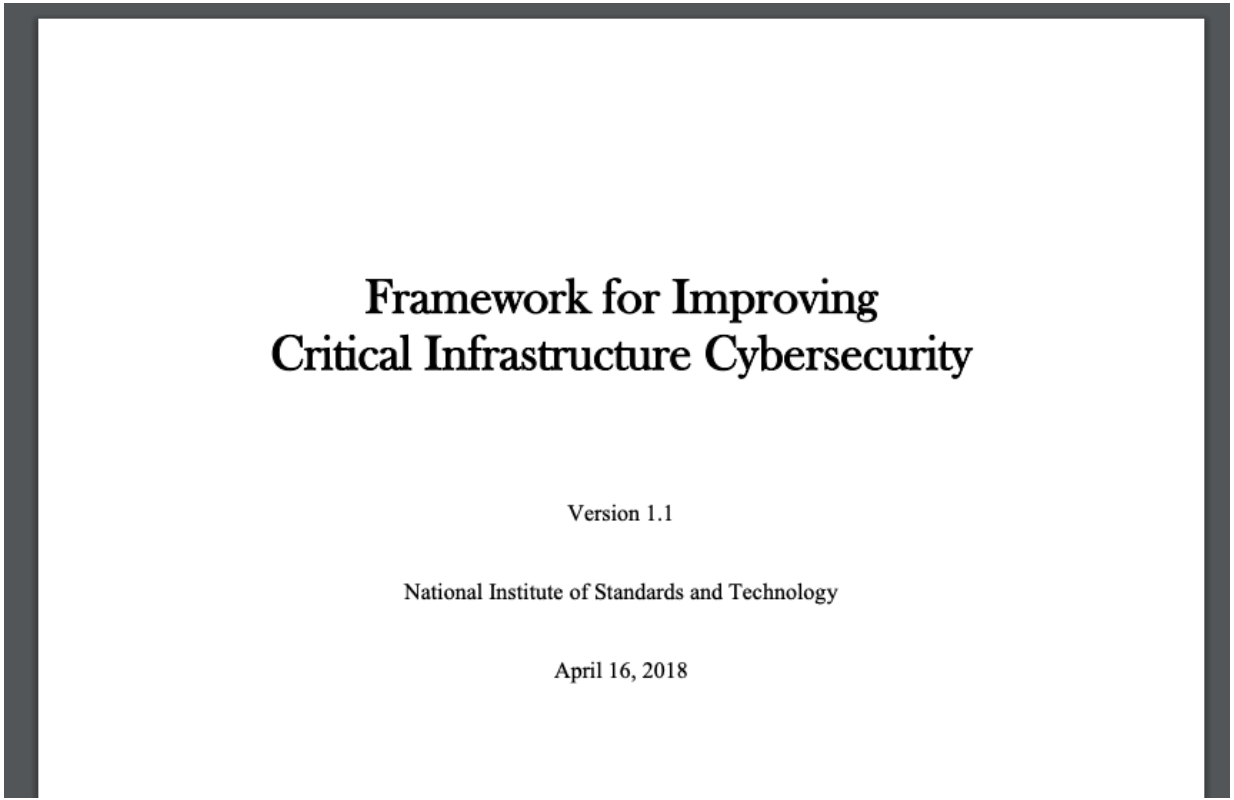
CVSS v2 Base Score: 9.3 HIGH
Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

https://nvd.nist.gov/vuln/detail/CVE-2017-0143

Cybersecurity Framework



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

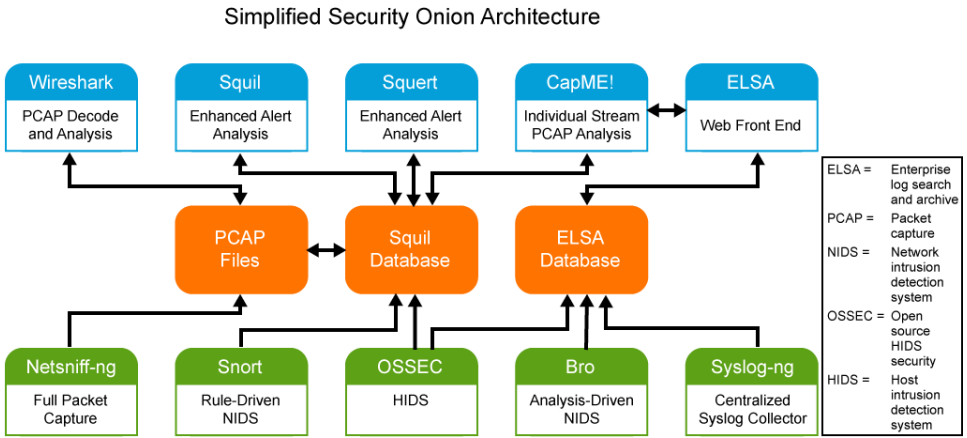
https://www.nist.gov/cyberframework

Bug Bounty

- “Crowdsourced security”
- Develops can receive recognition and compensation for reporting bugs, exploits and vulnerabilities

Source: Bugcrowd

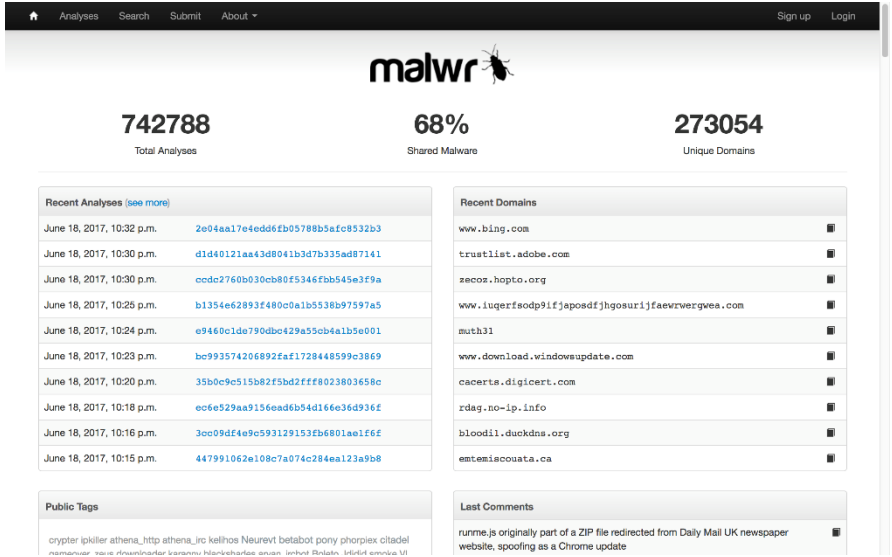
Security Tools



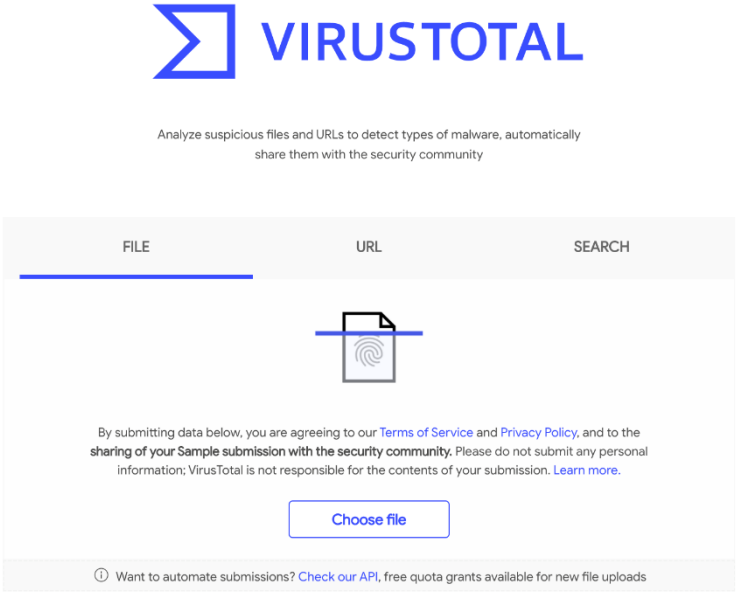
Network Security Monitoring (NSM)

Source: Security Onion

Security Tools



Cuckoo Sandbox

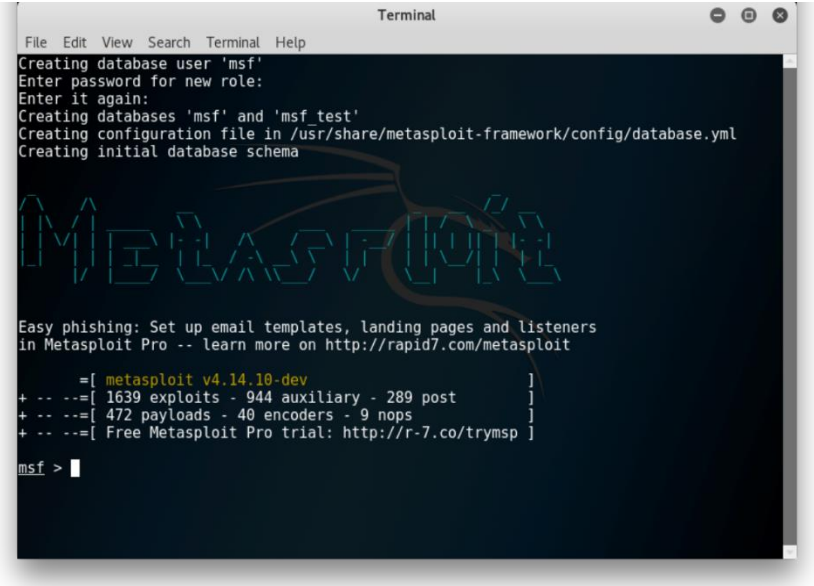


virustotal.com

Malware analysis

Security Tools

- Metasploit



Penetration Testing Tools

OpenSOC Project

- a collaborative open source development project dedicated to providing an extensible and scalable advanced security analytics tool
- Big Data security analytics framework designed to consume and monitor network traffic and machine exhaust data of a data center. OpenSOC is extensible and is designed to work at a massive scale.

http://opensoc.github.io/

Questions

Thank You!

END OF SESSION