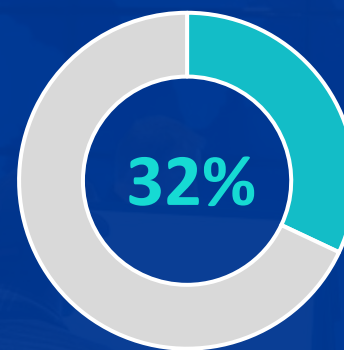


SOPHOS

Risk Management, focusing on what matters

Ben Verschaeren
July 2024

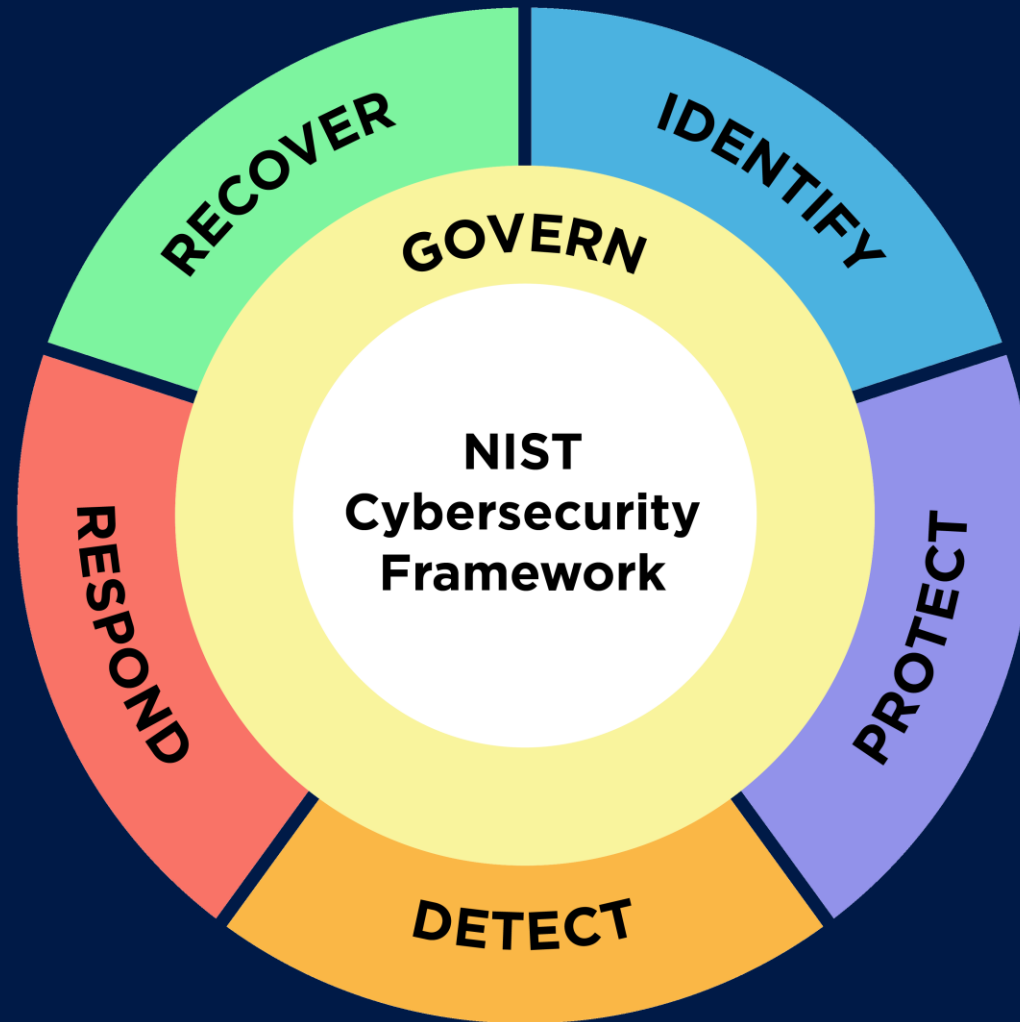
A **third** of ransomware attacks start with an exploited unpatched vulnerability



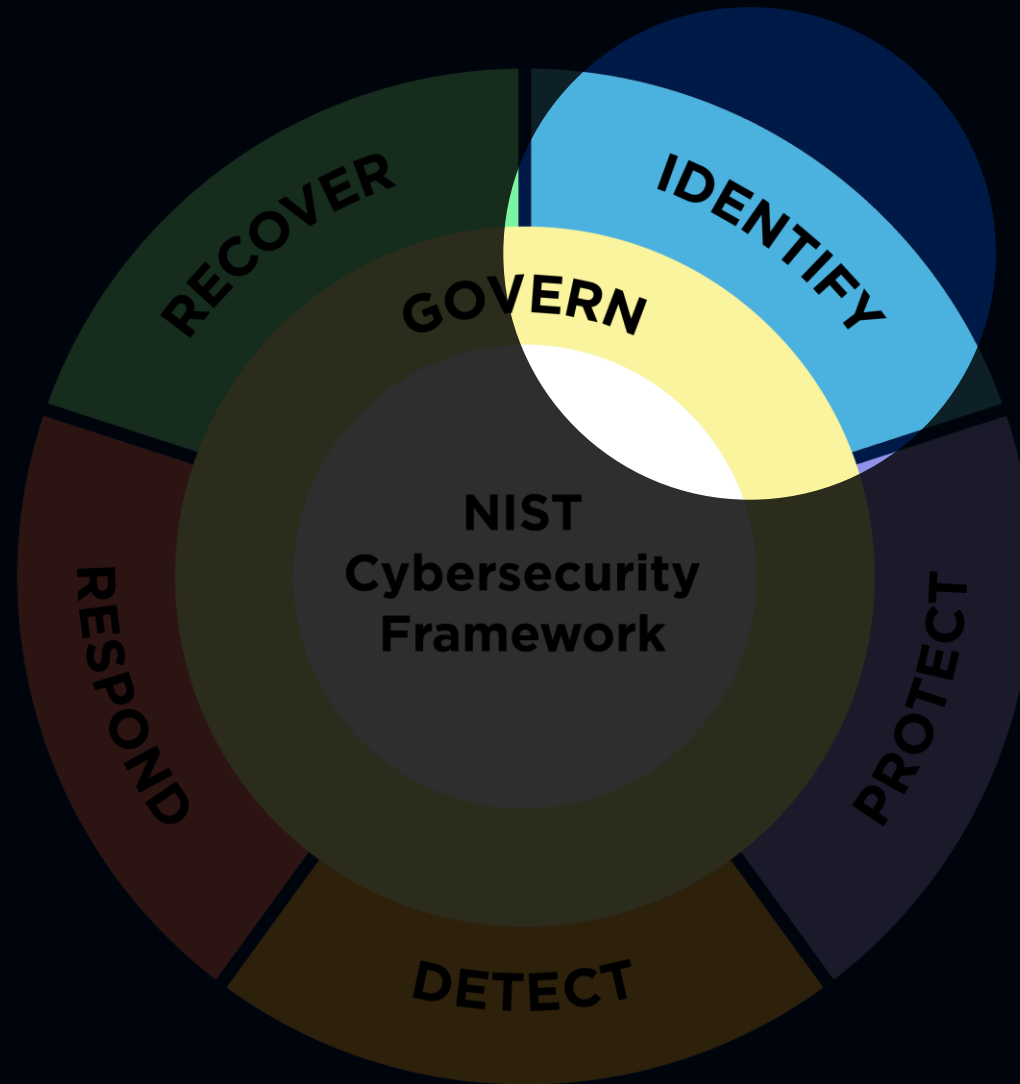
What is the Attack Surface?

- The attack surface encompasses all the points of entry through which an attacker can try to infiltrate a system or exfiltrate data.
- Components:
 - Networks: Internet-facing networks, cloud services, and internal networks.
 - Hardware: Servers, routers, firewalls, IoT devices.
 - Software: Applications, operating systems, APIs.
 - Human Factors: Social engineering, phishing attacks.

The Visibility Disconnect



The Visibility Disconnect



1.0.0

Menu

Australia

Internet Exposure Dashboard

Module 11

Ports Open

8,189,160

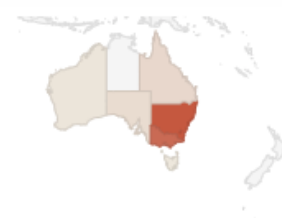
Module 15

Industrial Control Systems

1,647

Module 18

Map of ICS



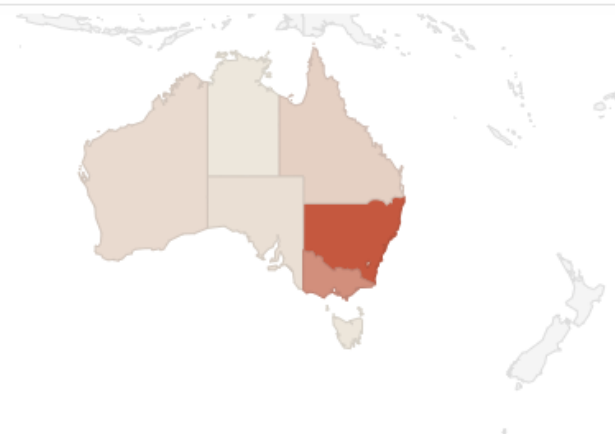
Module 15

Cisco IOS XE WebUI

2,225

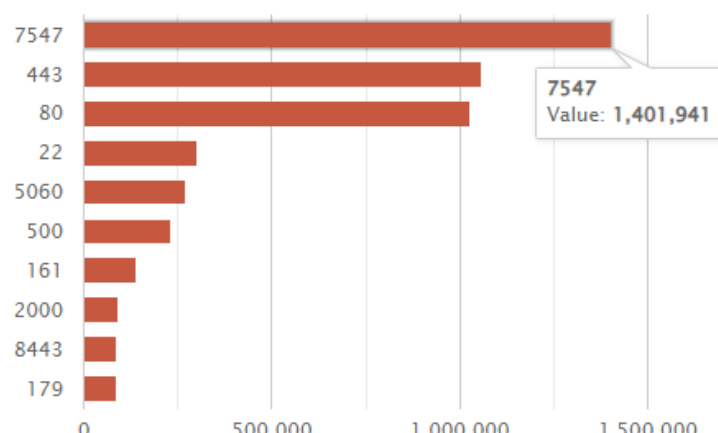
Module 13

Map of All Services



Module 12

Port Usage



Port	Usage
7547	1,401,941
443	~1,100,000
80	~1,050,000
22	~250,000
5060	~200,000
500	~150,000
161	~100,000
2000	~50,000
8443	~50,000
179	~50,000

Module 114

Top Vulnerability

CVE-2022-32548

Module 15

BlueKeep Unpatched

261

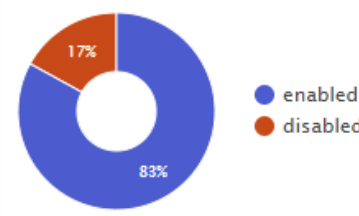
Module 19

Compromised Databases

543

Module 111

SMB Authentication



83% enabled
17% disabled

Module 110

Ivanti Pulse Secure

1,312

1.0.0

Menu

Australia

Internet Exposure Dashboard

Module 11

Ports Open

8,189,160


Module 15

Industrial Control Systems

1,647

Module 18

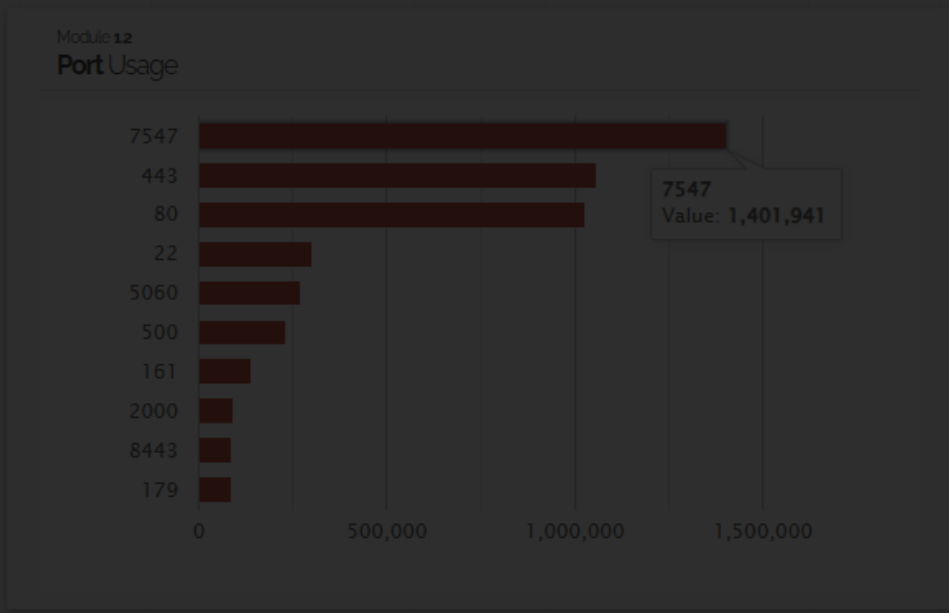
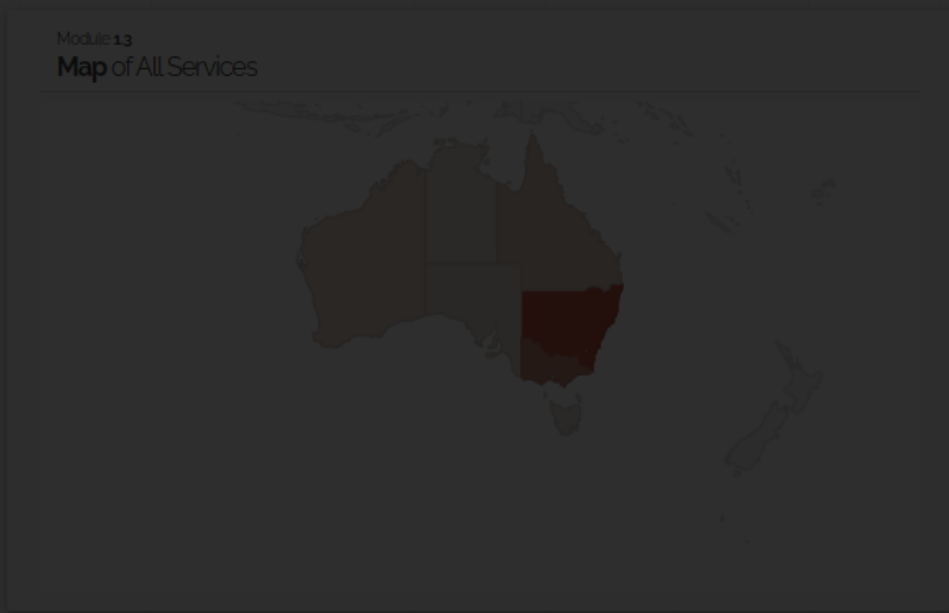
Map of ICS



Module 15

Cisco IOS XE WebUI

2,225



Module 114

Top Vulnerability

CVE-2022-32548

Module 15

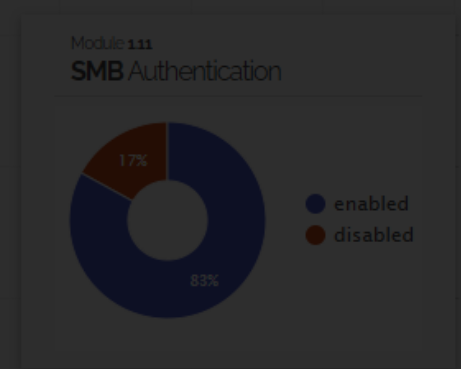
BlueKeep Unpatched

261

Module 19

Compromised Databases

543



Module 110

Ivanti Pulse Secure

1,312

APJ - ANZ

Vulnerabilities

- cve-2022-32548: 11813
- cve-2015-0204: 3036
- cve-2015-4000: 2371
- cve-2020-0796: 1505
- cve-2015-1635: 514
- ms15-034: 514
- cve-2024-23897: 429
- cve-2019-0708: 285
- cve-2014-0160: 292
- cve-2021-31206: 251
- ms17-010: 6

Ports

- 7547: 1434549
- 443: 1129366
- 80: 1100442
- 22: 303452
- 5060: 254244
- 500: 229834
- 161: 150430
- 179: 101727
- 2000: 82159
- 8443: 88408
- 8081: 393688
- 8089: 10763

Focusing on External Attack Surface Management (EASM) and the importance of patching vulnerabilities that are actively exploited.

Key Components of EASM

- Continuous Discovery
 - Automated tools to continuously discover and inventory all external-facing assets
- Risk Assessment
 - Evaluating the security posture of these assets to identify vulnerabilities
- Mitigation
 - Applying security measures to reduce identified risks, such as firewalls, DDoS protection, and secure configurations
- Monitoring
 - Ongoing surveillance to detect new vulnerabilities and threats in real-time

Lets play a game...

- Would you rather have hands for feet or feet for hands?
- Would you rather patch informational alerts or invest time in patching what matters?

Vulnerabilities 9

Filter Search Vulnerabilities 9 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
INFO	HTTP (Multiple Issues)	Web Servers	3		
INFO	HTTP (Multiple Issues)	CGI abuses	2		
INFO			CGI Generic Tests Load Estim...	CGI abuses	1		
INFO			External URLs	Web Servers	1		
INFO			Nessus Scan Information	Settings	1		
INFO			Nessus SYN scanner	Port scanners	1		
INFO			Web Application Sitemap	Web Servers	1		
INFO			Web mirroring	Web Servers	1		
INFO			Web Server Crafted Request ...	Web Servers	1		

Host Details

IP:
DNS:

OS: CISCO PIX 7.0
Start: July 7 at 8:55 PM
End: July 7 at 9:14 PM
Elapsed: 19 minutes
KB: [Download](#)

Vulnerabilities

Critical

High

Medium

Low

Info

Understanding Actively Exploited Vulnerabilities

- Vulnerabilities that are currently being exploited by attackers in the wild.
- Examples: Zero-day vulnerabilities, known CVEs (Common Vulnerabilities and Exposures) with active exploit code available.
- Criticality: These vulnerabilities pose immediate risk and require urgent attention to prevent breaches.

Tenable have got this right:

Vulnerability Priority Rating (VPR)

- Takes into consideration the CVE
- Uses continuous threat intelligence to change and reprioritise threats
- Calculates risk score based on the risk that is being posed.

CYBERSECURITY ADVISORY

#StopRansomware: CL0P Ransomware Exploits CVE-2023-34362 MOVEit Vuln

Release Date: June 07, 2023

Alert Code: AA23-158A

RELATED TOPICS: [MALWARE](#), [PHISHING](#), [AND RANSOMWARE](#), [CYBER THREATS AND ADVISORIES](#)



ACTIONS TO TAKE TODAY TO MITIGATE CYBER THREATS FROM CL0P RANSOMWARE

1. Take an inventory of assets and data, identifying authorized and unauthorized devices and software.
2. Grant admin privileges and access only when necessary, establishing a software allow list that only executes legitimate applications.
3. Monitor network ports, protocols, and services, activating security configurations on network infrastructure devices such as firewalls and routers
4. Regularly patch and update software and applications to their latest versions, and conduct regular vulnerability assessments.

Updated June 16, 2023

This CSA is being re-released to remove old Fortra GoAnywhere Campaign IP addresses and to add new addresses. See the update below.

End of Update

MOVEit zero-day exploit used by data breach gangs: The how, the why, and what to do...

Little Bobby Tables is back!

Written by Paul Ducklin

JUNE 05, 2023

NAKED SECURITY

CVE-2023-34362

MOVEIT

PROGRESS

Last week, Progress Software Corporation, which sells software and services for user interface development, devops, file management and more, alerted customers of its *MOVEit Transfer* and related *MOVEit Cloud* products about a [critical vulnerability](#) dubbed **CVE-2023-34362**.

As the name suggests, MOVEit Transfer is a system that makes it easy to store and share files throughout a team, a department, a company, or even a supply chain.

In its [own words](#), “MOVEit provides secure collaboration and automated file transfers of sensitive data and advanced workflow automation capabilities without the need for scripting.”

Unfortunately, MOVEit’s web-based front end, which makes it easy to share and manage files using just a web browser (a process generally considered less prone to misdirected or “lost” files than sharing them via email), turned out to have a SQL injection vulnerability.



Sophos MDR

24/7 threat hunting, detection, and response delivered by an expert team as a fully-managed service.

[Learn More](#)

DIY



SHODAN



MISP
Threat Sharing



Nessus
vulnerability scanner

MITRE

Sophos Managed Risk

1 | ATTACK SURFACE VISIBILITY

Mitigate risk by knowing what you own

2 | CONTINUOUS RISK MONITORING

Extend your team with vulnerability experts

3 | PRIORITIZE VULNERABILITIES

Know what to patch and why

4 | IDENTIFY NEW RISKS FAST

Get alerted to new critical vulnerabilities

The image displays two overlapping screenshots of the Sophos Managed Risk and External Attack Surface Management (EASM) web interfaces. The top screenshot shows the 'Managed Risk' dashboard, which includes a header with navigation links (SOPHOS, Dashboards, My Products, XDR, Alerts, Reports, People, Devices) and a main content area with a 'Managed Risk' section. The bottom screenshot shows the 'External Attack Surface Management' configuration page, which includes a header with the same navigation links and a main content area with sections for 'External Attack Surface Management' and 'Managed Domains and IP Addresses'. The 'Managed Domains and IP Addresses' section contains input fields for 'Top Level Domains' (with examples 'domainexampleone.com' and 'seconddomainexample.com') and 'IP ranges' (with example '100.0.0.0/32'). The 'Schedule Scan and Reports' section includes a 'Weekly scan start day' dropdown (set to 'Sun') and a 'Weekly scan start time' dropdown (set to '4:00 AM').

Managed Risk

description. Cupcake ipsum dolor. Sit amet marshmallow topping cheesecake muffin. Halvah croissant candy canes bonbon candy. Apple pie jelly beans topping carrot cake danish tart cake cheesecake. Muffin danish chocolate soufflé pastry icing bonbon oat cake. Powder cake jujubes oat cake. Lemon drops tootsie roll marshmallow halvah carrot cake.

External Attack Surface Management

External Attack Surface description. Cupcake ipsum dolor. Sit amet marshmallow topping cheesecake muffin. Halvah croissant candy canes bonbon candy. Apple pie jelly beans topping carrot cake danish tart cake cheesecake. Muffin danish chocolate soufflé pastry icing bonbon oat cake. Powder cake jujubes oat cake. Lemon drops tootsie roll marshmallow halvah carrot cake.

This page allows for External Attack Surface Management configuration.

External Attack Surface Management

description. Cupcake ipsum dolor. Sit amet marshmallow topping cheesecake muffin. Halvah croissant candy canes bonbon candy. Apple pie jelly beans topping carrot cake danish tart cake cheesecake. Muffin danish chocolate soufflé pastry icing bonbon oat cake. Powder cake jujubes oat cake. Lemon drops tootsie roll marshmallow halvah carrot cake.

Managed Domains and IP Addresses

Top Level Domains

domainexampleone.com × seconddomainexample.com ×

Enter up to five TLDs.

IP ranges

100.0.0.0/32 ×

CIDR notation allowed.

Schedule Scan and Reports

Reports will be sent to MDR contacts and available in the MDR Notification center.

Weekly scan start day

Sun Mon Tue Wed Thu Fri Sat

Weekly scan start time

4:00 AM Los Angeles, California (GMT -7:00)

In Summary

- Know your attack surface
- Continually monitor your attack surface
- Have your teams focus on what matters – which is what is actively being exploited

