



Future-Proof Your Business with Managed Cybersecurity Services

Leveraging Expertise for Enhanced Security

•Presented by: Ricardo Gravito

avit

part of  springboardnetwork

The network powering a sustainable secure digital future

Springboard **WORLDWIDE**



01

Actual Cyber Threat Landscape for Business

02

Challenges in Traditional Cybersecurity Approaches

03

Why Managed Cybersecurity Services

04

How Advanced Security Technologies Help

05

Integration and Support

06

Business Continuity and Resilience

07

Real-World Impact

08

Conclusion

01 - Actual Cyber Threat Landscape

Globally, the cybersecurity threat landscape continues to evolve rapidly and remains challenging, with more than half of organizations (54%) having experienced a cybersecurity incident in the past year, and three-quarters (73%) of all organizations believing they are likely to be disrupted by a cybersecurity incident in the next 12-24 months.

A key trend that this year's Index highlighted is that companies now see external actors as a bigger threat than internal ones. Among those surveyed, 62% highlighted that external actors are their biggest threat, while only 31% said the same for internal actors. This is a marked shift from 2023 when the two were seen as almost equal threats. One of the key drivers of this turnaround could be the fact that cybersecurity threats from external actors are becoming increasingly sophisticated.

While malware (76%) and phishing (54%) continue to remain the top types of attacks experienced, 37% of

Types of Attacks Experienced by Companies

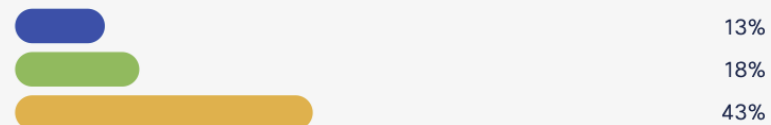


Actual Cyber Threat Landscape

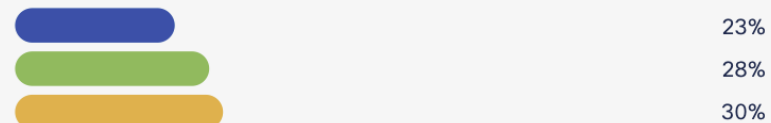
Number of Unfilled Cybersecurity-Related Positions

- Large companies (>1,000 employees)
- Mid-sized companies (250-999 employees)
- Small-sized companies (10-249 employees)

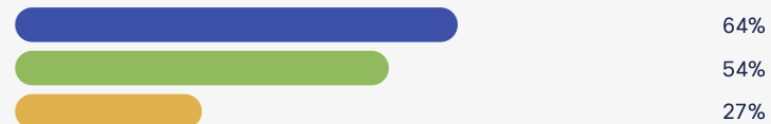
Between 1 - 5



Between 6 - 10



More than 10



Cybersecurity is also consuming an ever-growing share of overall IT budgets, with a majority (53%) of organizations surveyed devoting more than 10% of their total IT budget to cybersecurity — up from only 29% of organizations that allocated a similar amount in 2023. This highlights that executive leadership teams understand the critical nature of cybersecurity and its importance to their business growth.

However, progress is being stifled by a critical shortage of talent, which was highlighted as an issue for nearly nine out of 10 companies. Almost half (46%) of the companies said they had more than 10 unfilled cybersecurity roles on their teams at the time of our survey.

Actual Cyber Threat Landscape



Rise in sophisticated threats like ransomware, phishing, and APTs.



Increased attack surface due to remote work and cloud adoption.



Shortage of skilled cybersecurity professionals.

02 - Challenges in Traditional Cybersecurity Approaches



Fragmented security tools leading to complexity.



Delayed threat detection and response times.



High operational costs and resource constraints.

Challenges in Traditional Cybersecurity Approaches



Siloed Security Tools

Definition: Independent security tools that operate separately without coordination.

Characteristics:

Fragmented: Each tool handles specific security tasks independently.
Disjointed Response: Lack of unified threat intelligence and response strategies.
Resource Intensive: Requires more time and effort to manage multiple tools.

Challenges:

Gaps in Coverage: Inconsistent security practices across the organization.
Delayed Response: Slower detection and mitigation of threats.
Higher Costs: Increased operational costs due to managing multiple tools.

Integrated Solutions



Definition: Unified security platform that consolidates various security functions.

Characteristics:

Holistic: Provides a comprehensive view of the threat landscape.
Streamlined Operations: Centralized management simplifies security operations.
Efficient: Reduces complexity and enhances resource utilization.

Benefits:

Enhanced Detection: Better identification of sophisticated attacks.
Faster Response: Quicker detection and mitigation of threats.
Cost Effective: Lower long-term operational costs.

03 - Why Managed Cybersecurity Services



Outsourcing cybersecurity to specialized providers



Continuous monitoring, threat detection, and incident response



Access to advanced tools and expert personnel without in-house overhead

Why of Managed Cybersecurity Services



Managed security solutions

- Secure Endpoint
- Umbrella DNS/SIG
- Secure E-mail
- XDR
- SOC/SIEM
- Secure Firewall*
- Secure MFA*
- Incident Response



24/7 monitoring



Dedicated Security Teams



Monthly conference call
Advise on posture ,
Discuss events and Check
coverage.



Quarterly review on rule
base/exceptions & soft-
/firmware upgrades

Security Reference Architecture



TALOS

Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security
Operations



SOC services



eXtended Detection and Response (XDR)



Incident Response and Remediation Services



Cyber Resilience Assessment



Vulnerability Management & Scanning



Security Awareness Training



3rd Party Integrations

User/Device Security

ZERO TRUST WORKFORCE

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

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

Threat Protection | Secure Access Control | Managed Remote Access



Secure Access



ZTNA



RAaaS



DNS-layer
security



SSL
decryption



Secure web
gateway



Remote
browser
isolation



L7 firewall
+ IPS



Cloud access
security broker/
shadow IT



Data loss
prevention



Cloud malware
detection

SDWAN



Cisco
Meraki
SDWAN



SDWAN
by Viptela

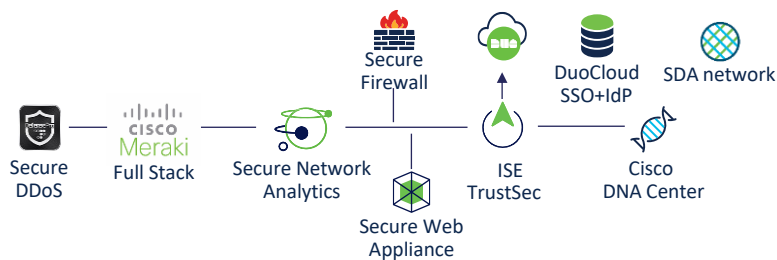


Secure
Firewall

On-Premises

ZERO TRUST WORKPLACE

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



SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security



Network
Edge



Cisco
Meraki
SDWAN



SDWAN
by Viptela



Secure
Firewall

IOT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT



Industrial
Router



Industrial
Firewall



Industrial
Switch/AP



Cyber
Vision



ISE
TrustSec

Application Security

ZERO TRUST WORKLOAD

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack



Cloud Native Security



ACI APIC



Secure
Workload



Secure Application
by AppDynamics

App Visibility | Detection | Response



Hybrid
Private



Public
Cloud



XDR Analytics



Secure
Firewall

The 3 Keypoints

Extended 24-7

Protection: Coverage across network, endpoints, cloud, and applications.

123

Cost Efficiency:

Predictable budgeting with reduced capital expenditure.

Scalability: Solutions that grow with your business needs.

04 –How Advanced Security Technologies help

Cisco Talos

One of the largest threat intelligence teams in the world

- Delivers real-time, actionable intelligence
- Feeds Cisco products with up-to-date threat data

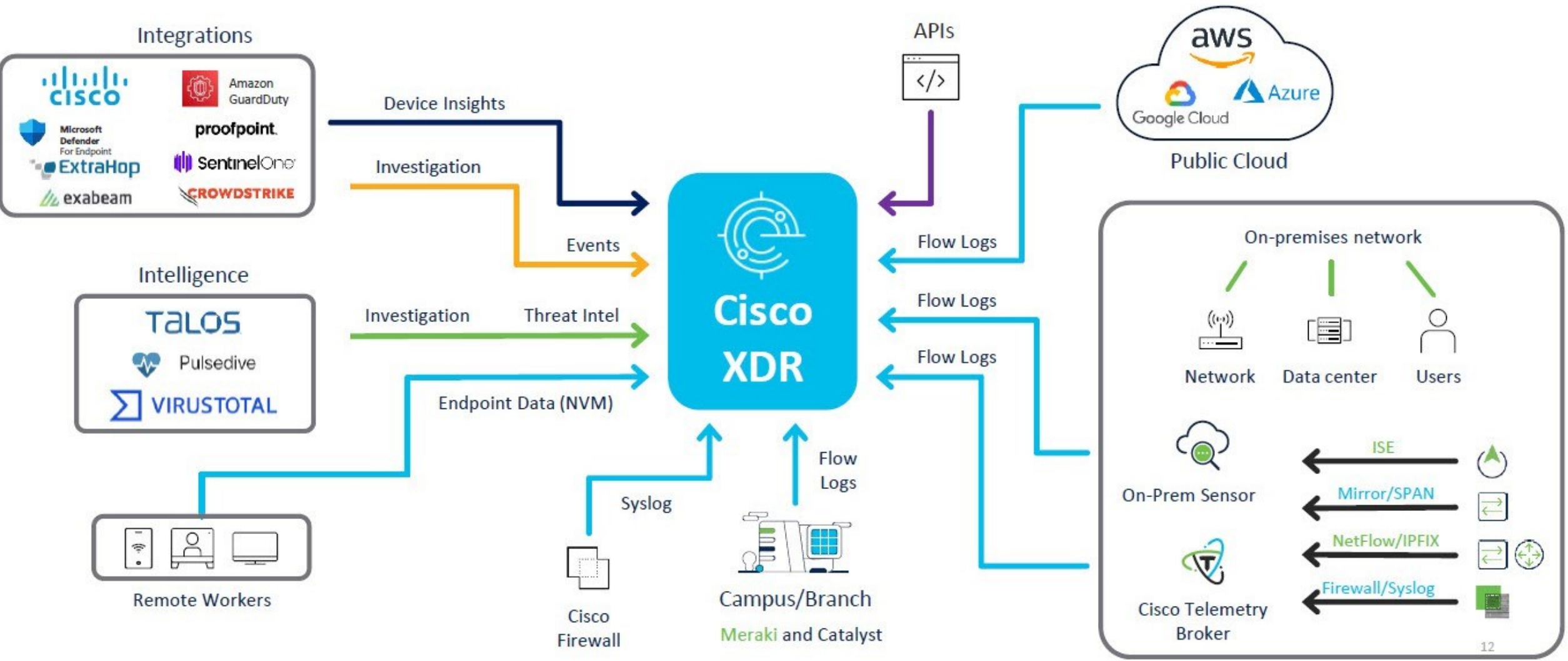
XDR

1. **Collect** – Ingests telemetry from endpoints, networks, email, and cloud.
2. **Correlate** – Uses analytics and intelligence to identify true threats.
3. **Respond** – Automates containment and remediation across all integrated tools.

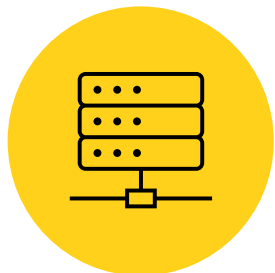
Umbrella

- DNS-layer security
- Blocks malicious domains and IPs before a connection is established
- Ideal for roaming users and remote offices

Cisco XDR Overview



05 - Seamless Integration and Support



Easy integration with existing IT infrastructure.

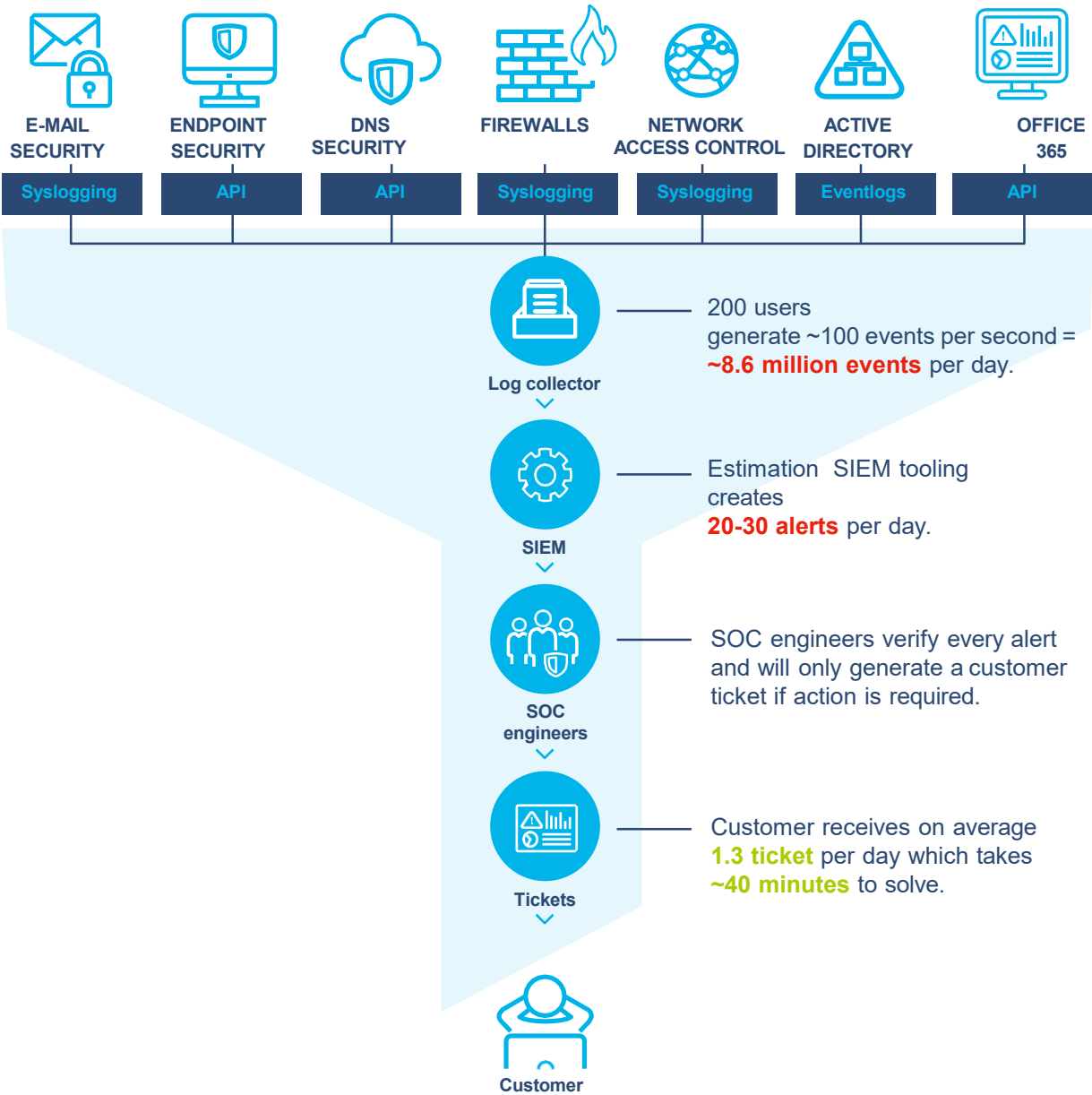


Dedicated support teams for ongoing assistance.



Regular updates and threat intelligence feeds.

Integration Managed Security Services



06 - Ensuring Business Continuity and Resilience



Rapid incident response minimizes downtime.

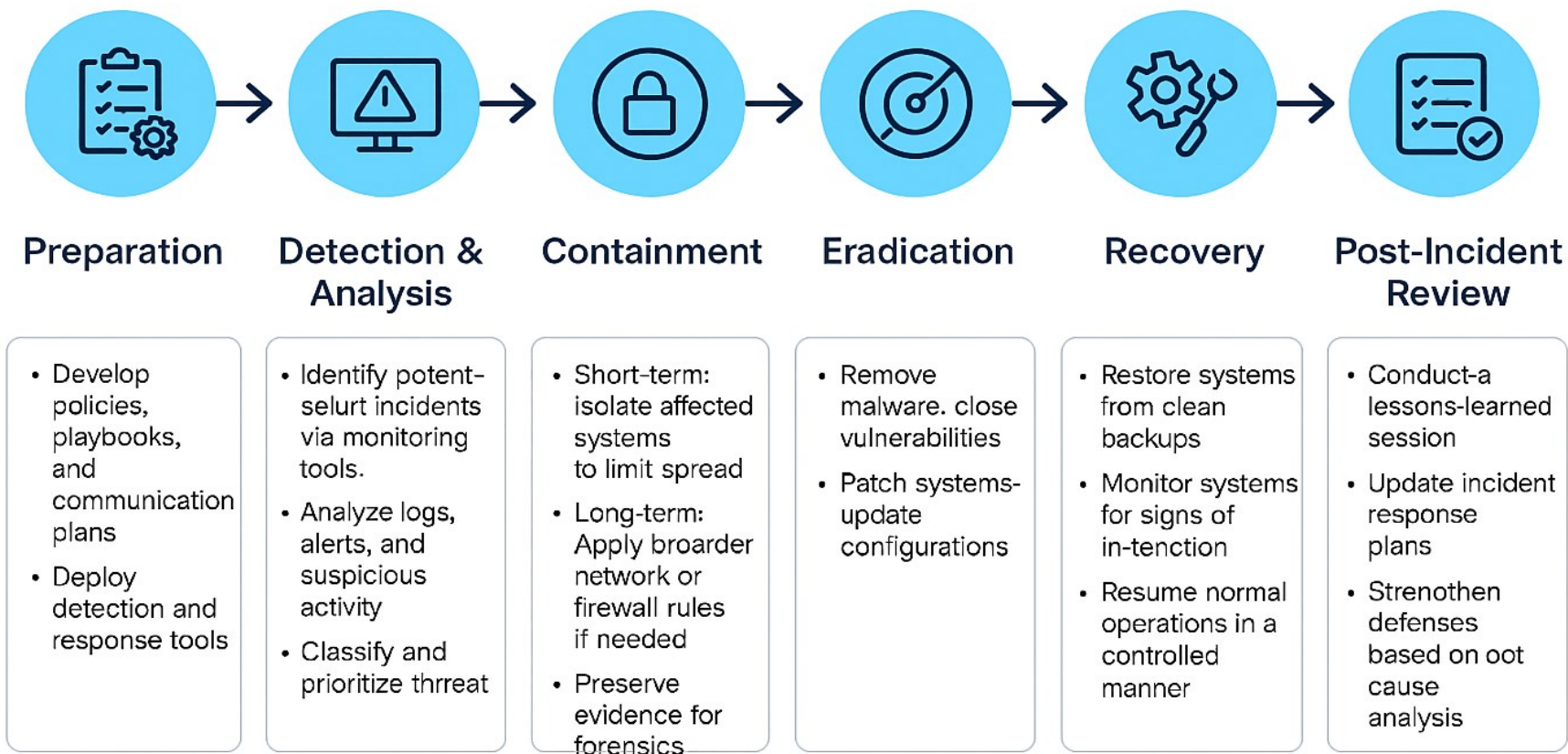


Business continuity planning and disaster recovery support.



Continuous improvement through regular assessments.

06 - Ensuring Business Continuity and Resilience



07 - Real-World Impact and ROI



showcasing reduced breach incidents.



Improved compliance with industry regulations.



Enhanced customer trust and brand reputation

07 - Real-World Impact



reduced breach incidents.



Improved compliance with industry regulations.



Enhanced customer trust and brand reputation

07 - Real-World Impact

TESTIMONIALS FROM SATISFIED CLIENTS

MANAGED SECURITY | CISCO



Cisco has been a reliable partner in protecting our infrastructure and ensuring continuous visibility across complex environments.”

NASA IT Security Manager



Cisco’s managed detection and response capabilities drastically improved our response time to threats, reducing incident handling from days to hours.”

Global Cybersecurity Director, Deloitte



With Cisco SecureX and Talos threat intelligence, we’ve seen a 60% reduction in security alert fatigue among our analysts.

KEY STATISTICS HILIGIPACT



97% of threats are automatically remediated before causing harm with Cisco SecureX and MDR services



60% reduction in dwell time (the time an attacker remains undetected)




85% faster mean time to detect (MTTD) with Cisco’s Threat Response tools



73% of clients report improved compliance posture after onboarding Cisco managed security services

Welcome to our network

avit

part of  springboardnetwork

