ALGOSYSTEMS
THE PATH FORWARD

Algosystems Solutions & Services

Cyber Security in focus


There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco
Algosystems Managed Services
ALGOSYSTEMS
THE PATH FORWARD

Threat Landscape 2025 – Actors & Sectors

Global

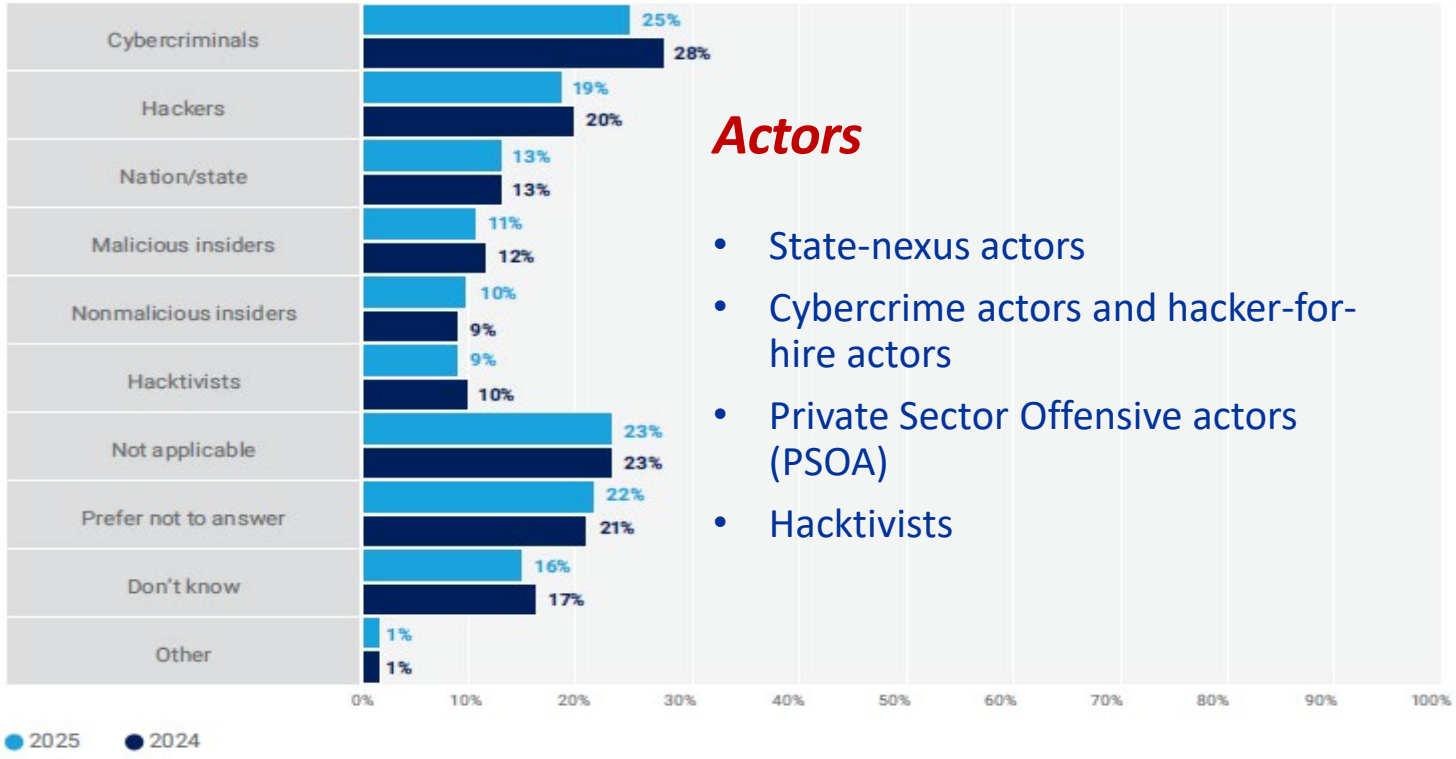
Ransomware will cost its victims around

- $265 billion USD annually by 2031
- up from $42 billion in 2024
- $20 billion in 2021

Global

A new attack (on consumers and organizations) occurrs every two seconds as ransomware perpetrators progressively refine their malware payloads and related extortion activities.

Cybersecurity Ventures - Cybercrime Magazine



Actors

- State-nexus actors
- Cybercrime actors and hacker-for-hire actors
- Private Sector Offensive actors (PSOA)
- Hacktivists

Sectors

- Public administration (38.2%)
- Unknown (28.5%)
- Transport (7.5%)
- Digital Infrastructure & Services (4.8%)
- Finance (4.5%)
- Manufacturing (2.9%)
- Media & Entertainment (2.3%)
- Business Services (2.2%)
- Energy (1.7%)
- Education (1.7%)
- Health (1.2%)

ISACA - STATE OF CYBERSECURITY 2025 - Global

Ελλάδα - Threat Landscape

200% αυξήθηκαν μέσα σε δύο χρόνια οι κυβερνοεπιθέσεις στην Ελλάδα

Πάνω από 15,2 εκατομμύρια ψηφιακές απειλές εντοπίστηκαν μόνο το 2024.

Φουρλής

«Δυστυχώς είχαμε υποτιμήσει τον κίνδυνο!».

Τα λόγια του προέδρου του ομίλου Fourlis Βασίλη Φουρλή στον απόηχο μιας από τις μεγαλύτερες κυβερνοεπιθέσεις που συντελέστηκαν εις βάρος ελληνικής επιχείρησης, κοστίζοντας κάπου 20 εκατ. Ευρώ κατά δήλωσή της.

Πρώτο Θέμα 4/5/2025

Our Solutions

- Networking
- Collaboration
- Cybersecurity
- Cloud Transformation
- Systems & Data Center
- Mobility & Digital Transformation
- Systems & Application Availability

Network

- *Software Defined Networking (SDN / SDWAN)*
- *Switches*
- *Access Points*
- *Routers*
- *Network Observability*

Cloud

- *M365*
- *Azure Infrastructure*
- *M365 Security*
- *Intune*

Systems

- *Servers*
- *Virtualization*
- *Backup Software*
- *Data Center Creation*
- *Data Center Migration*

Professional Services

Algosystems Cyber Security Solutions

Services

- SOC - Security Operation Services
- Incident Response & Forensics
- SecOps Managed Services
- Firewall Security Audit Services
- Vulnerability Assessment Services
- Web Application Protection Services
- GRC Services
- Assurance Services

Products

- Perimeter & Network Security
- Endpoint Security
- DNS Security
- Mail Security
- CASB/Cloud Security
- Application Security
- Data Security
- Mobile Device Management
- Privileged Access Management
- SD WAN
- Network Detection & Response
- SASE
- Zero Trust
- Secure File Sharing

Algosystems
Managed Services

- Security Operations Center
- Incident Response/Forensics
- SecOps – MDR, NDR, FWs, DNS Security
- Network Operations Center
- Firewall Security Audit as a Service
- Managed Network Traffic Control & Analysis
- Disaster Recovery as a Service
- Web Application Firewall as a Service
- Managed DDoS
- Vulnerability Assessment as a Service
- Vulnerability Remediation
- Patch Management as a Service
- Breach & Attack Simulation as a Service
- Phishing Campaigns as a Service

Managed SecOps Services – Why?

- Workforce shortage
- Skills shortage
- 24/7 operation
- Failure to notice alerts at an early stage
- Miscommunication inside the organization
- Overwhelmed by large number of alerts/systems

As a Service
Right mix of people & time

Decrease MTTR

Cooperation with other teams

Continuous Improvement

Managed SecOps Services

- *Monitor alerts*
- *Investigate incidents*
- *Ongoing support*

Phases

- *Assessment and Initial Configuration*
- *Continuous Monitoring and Analysis*
- *Incident Response*
- *Continuous Improvement*

Managed SecOps Services

Incident Response

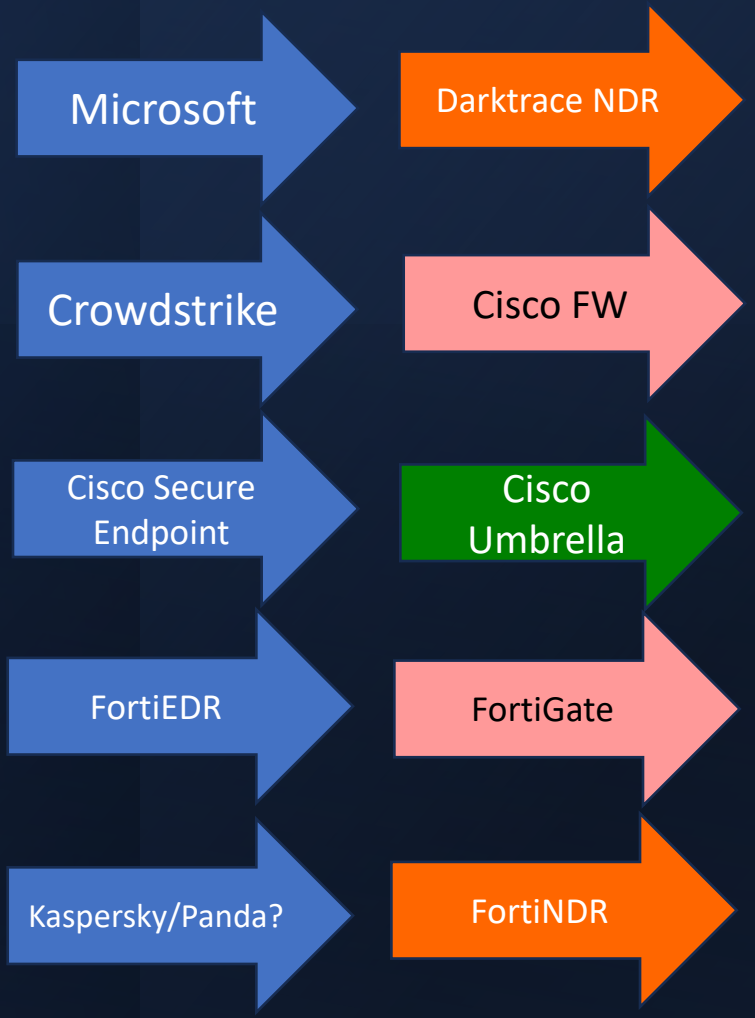
Threat Hunting

How

- *Human Expertise*
- *Advanced Security Technology*
- *Schedule-Operations*
- *Incident Handling*

What

- *Monitor Networks*
- *Analyze Security Incidents*
- *Respond to Threats*



Managed EDR

Service Initiation

Onboarding

- *Grant access to management console*
- *Retrieve & document current configuration*

Assessment & Initial Configuration

- *Configuration Assessment*
- *Propose Changes on Policies based on gaps*
- *Installation on new endpoints/agents*

Service Run

Continuous Monitoring & Analysis

- *Monitor endpoints for suspicious activity*
- *Analyze EDR logs & alerts for potential threats*
- *Report to Customer Team*

Incident Response– only on EDR

- *Investigate & Remediate EDR incidents*
- *Contain & Eradicate Threats*
- *Post incident analysis & recommendations*

Continuous Improvement

- *Review & Update EDR Policies & Procedures*
- *Analyze EDR data to identify areas of improvement*
- *Configuration improvements to enhance EDR Effectiveness*

Managed FWs

Service Initiation

Onboarding

- *Grant access to management console*
- *Retrieve & document current configuration*

Assessment & Initial Configuration

- *Thorough security assessment of FW rules & policies*
- *Identification and addressing of any vulnerabilities ensuring optimal security posture*
- *Configuration of firewalls to align with industry best practices and regulatory compliance requirements*

Service Run

Continuous Monitoring & Analysis

- *Continuously monitor FWs for suspicious activity*
- *Analyze Firewall logs and alerts for potential threats*
- *Leverage advanced threat intelligence to detect suspicious activity and potential breaches*
- *Provide monthly based reports on FW findings*

Incident Response – only on FWs

- *Investigate and remediate FW incidents*
- *Contain & eradicate threats also with other teams*
- *Provide post-incident analysis and recommendations*

Continuous Improvement

- *Review & Update FW Policies & Procedures*
- *Analyze FW data to identify areas of improvement*
- *Implement continuous improvement initiatives to enhance FWs' effectiveness*

Managed DNS Security

Service Initiation

Onboarding

- *Grant access to management console*
- *Retrieve & document current configuration*

Assessment & Initial Configuration

- *Configuration Assessment*
- *Propose Changes on Policies based on gaps*
- *Configure policies and settings based on industry best practices*
- *Installation of new agents*

Service Run

Continuous Monitoring & Analysis

- *Monitor DNS traffic for malicious activity including malware, phishing and ransomware attacks*
- *Analyze DNS logs & alerts for potential threats & anomalies*
- *Respond to DNS security alerts in a timely manner to mitigate risks*
- *Report to Customer Team*

Incident Response – on DNS Security Console

- *Investigate & Remediate DNS security incidents promptly*
- *Contain & Eradicate Threats also with other teams needed*
- *Post incident analysis & recommendations*

Continuous Improvement

- *Review & Update DNS Security Policies & Procedures*
- *Configuration improvements to enhance DNS Security effectiveness*

Managed NDR

Service Initiation

Onboarding

- *Grant access to management console*
- *Retrieve & document current configuration*

Assessment & Initial Configuration

- *Configuration Assessment*
- *Configuration of the statistical analysis models for False Positives elimination*
- *Duplicate Packets minimization*
- *New systems identification & categorization*

Service Run

Continuous Monitoring & Analysis

- *Continuously monitor network for suspicious activity*
- *Security Events analysis*
- *Threat Hunting*
- *Provide monthly based reports on NDR findings*

Incident Response – only on NDR

- *Investigate and remediate NDR incidents*
- *Statistical analysis of Security Events with logs from other security systems*
- *Security Events' report & IoCs logging*
- *Provide post-incident analysis and recommendations*

Continuous Improvement

- *Review & Update NDR Policies & Procedures*
- *Analyze NDR data to identify areas of improvement*
- *Implement continuous improvement initiatives to enhance NDR effectiveness*

ALGOSYSTEMS

Τομέας Πληροφορικής & Επικοινωνιών

ICT Division

Thank You

Algosystems S.A., Λ. Συγγρού 206, 176 72, Αθήνα 206 Sygrou Avenue, 176 72, Athens

Τηλ. /Tel. (+30) 210 9548000 E-mail welcome@algosystems.gr www.algosystems.gr