



GUARDBYTE

Managed 24/7 SOC. Why it's a necessity

Lampros Katsonis
Solutions Director @ Guardbyte
l.katsonis@guardbyte.com.cy

WE NOW LIVE IN A DIGITAL ECONOMY

56% OF ALL INTERNET TRAFFIC IS
CRIMINAL IN NATURE.



GUARDBYTE

AN ERA WITH DATA BREACHES ON THE RISE

2005

157

data breaches

66.9 million

records exposed

2022

11,476

data breaches

1.66 billion

records exposed




GUARDBYTE

SecurityScorecard | All | Search companies, scorecards, portfolios and tags... | Contact support | Cyber911 | [Notification] | [User]

Dashboard | Scorecards | Portfolios | Core Tools | **Modules** | Professional Services

Viewing 144 IPs as: [Cards] [Table] | Download

Top countries



Cyprus	144
--------	-----

Top threat actors

APT37	125
DragonFly	31
APT1	30
APT32	30
EI-Machete	30
FIN8	30

Sort by: Minimum Rating

185.78.131.106 **144** | Last scan 27/11/2023, 04:39:52

Nicosia, Nicosia, Cyprus | 35.1856, 33.3...23
Primetel PLC | ASN: 8544

Threat actors (1)
APT37

Ransomware groups (1)
Quantum

Vulnerabilities (0)
No detected vulnerabilities


Malicious reputation (0)

Attributed to:
Infonet (57)
infonet.ee
Technology

Service information:
Ports (6)
162, 80, 67, 443, 68, 161

Products (1)
proxygen-bolt

Services (6)
dhcpc, https, snmptrap, http, snmp,



61% of small and medium businesses are now being hit by cyber attacks every year, and the average cost of a cyberattack has **increased to €2.2 million**, making it extremely difficult for businesses to recover.

How Do Data Breaches Occur?

A data breach occurs when a cybercriminal infiltrates a data source and extracts confidential information. This can be done by accessing a computer or network to steal local files or by bypassing network security remotely. The most common cyber attacks used in data breaches are outlined below.



RANSOMWARE



MALWARE



PHISHING



**DENIAL OF SERVICE
(DOS)**



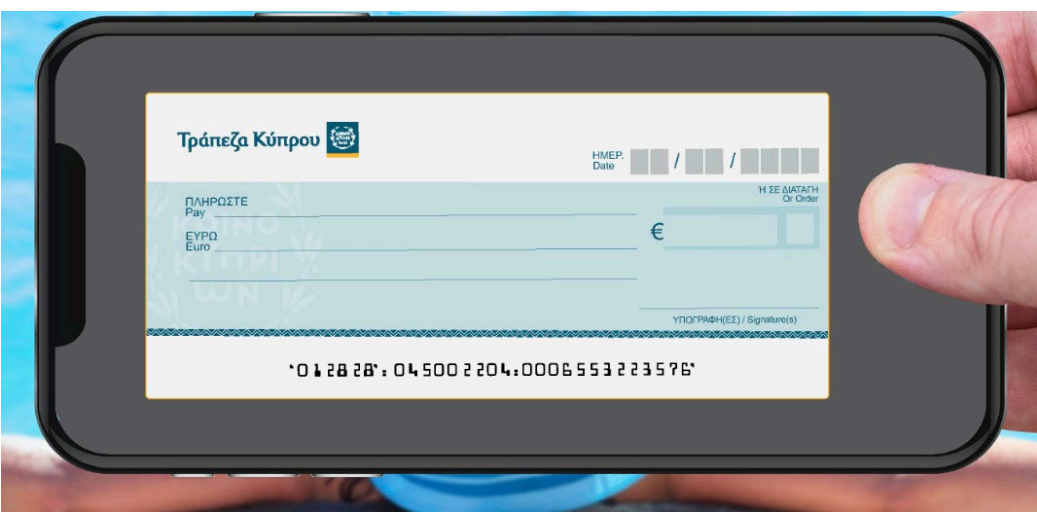
GUARDBYTE

Technology is evolving

7



www.guardbyte.com.cy




GUARDBYTE



www.guardbyte.com.cy



GUARDBYTE

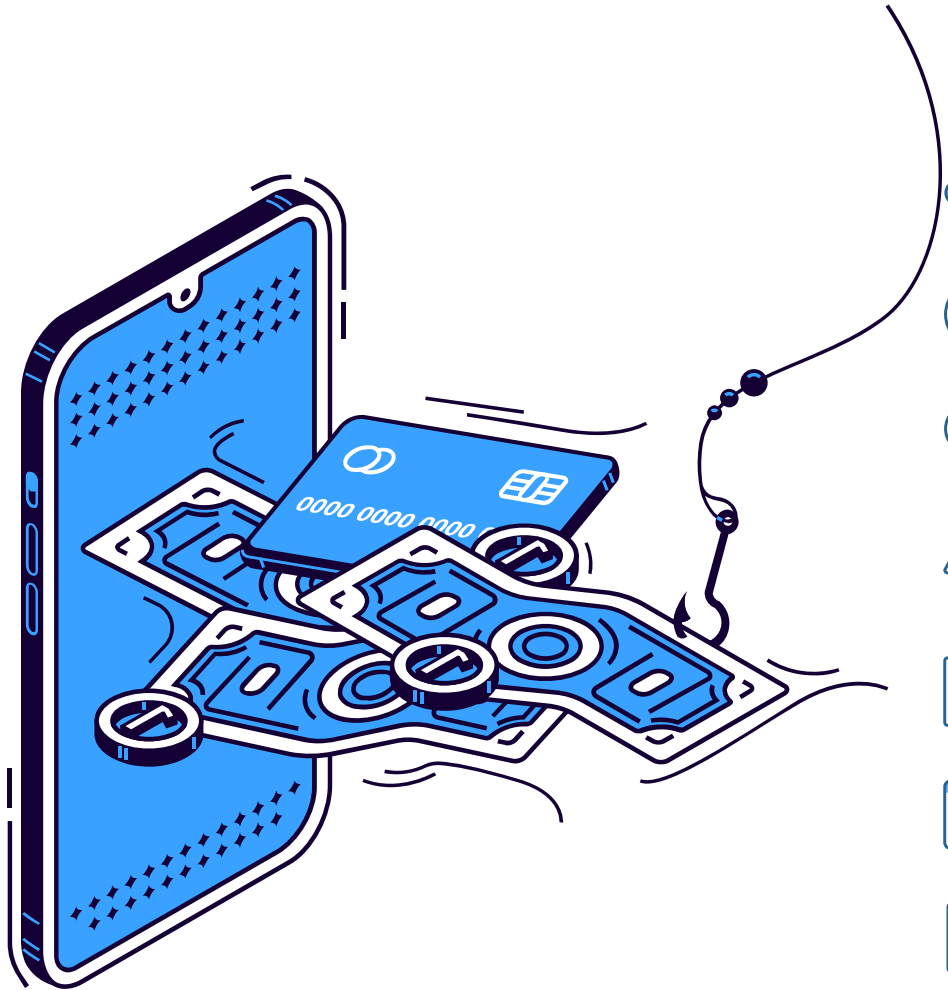
**Bad Guys are still able to hack
big corporations**



▼ Inbox	1163
APC	6954
Firewall	
[Redacted]	872
[Redacted]	685
Microsoft	
Panda	5235
Postmaster	827
Proxmox	442
Sophos	
[Redacted]	
[Redacted]	
Unify	9888
Veeam	14114
Drafts	[3]
Sent Items	
Deleted Items	221
Archive	
> Archives	
> Conversation History	
Junk Email	[10]
News Feed	
Outbox	
> Public Folders	
RSS Feeds	
[Redacted]	

Seems Familiar?

Yesterday's Security = Today's Cyber Threats



Expanding Attack Surface – Systems, Cloud, Remote Workforce



Lack of resources – time, technology, and budget



Talent shortage – skilled and experienced talent



Rapid increase, evolution and sophistication of cybercriminals



Regulatory standards and requirements growing and changing



Massive and overwhelming amount of data to monitor and analyze



Budget constraints – to cover the cost of necessary layers of security

Layered Security – Defense in Depth

Many Tools and Controls



Security Tools and controls



Endpoint devices



Firewalls, routers and switches



Antivirus or antimalware



Proxy Information



Identity and access management



Email: Microsoft 365



Web and DNS filtering



Dark web exposures



All These Security Measures = Massive Amount of Data


```
function(e, t, n) {
  var r, i = 0,
      o = e.length,
      a = M(e);
  if (a) {
    for (; o > i; i++)
      if (r = t.apply(e[i], n), r === !1) break
  } else
    for (i in e)
      if (r = t.apply(e[i], n), r === !1) break
  } else if (a) {
    for (; o > i; i++)
      if (r = t.call(e[i], i, e[i]), r === !1) break
  } else
    for (i in e)
      if (r = t.call(e[i], i, e[i]), r === !1) break;
  return e
}

function(e) {
  return null == e ? "" : b.call(e)
}

function(e) {
  return null == e ? "" : (e + "").replace(C, "")
}

function(e, t) {
  var n = t || [];
  return null != e && (M(Object(e)) ? x.merge(n, "string" == typeof e ? [e] :
    b.call(n, e))
```



What Is The Solution?

You need a Security Operations Center (SOC) on Your Side

A security operations center (SOC) is a centralized hub or command center that augments your overall IT & data security defense posture by harnessing the collective power of technology, processes, and people to aggregate, analyze, support, and manage the multiple security measures in place to protect your organization.



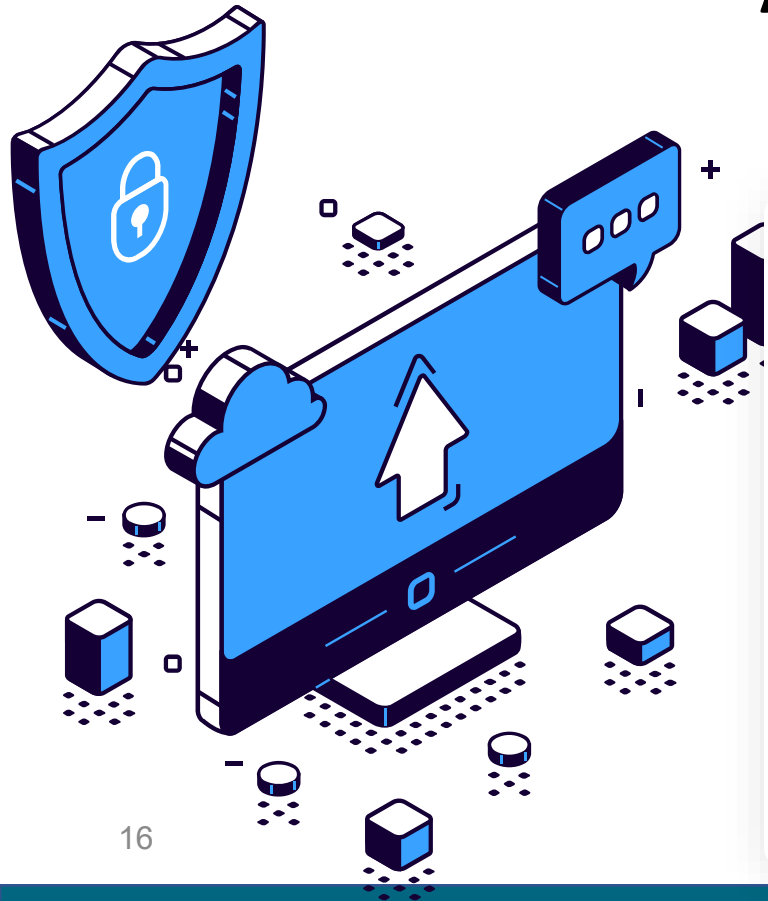
Did You Know?

- ✓ 40% of organizations still struggle with SOC staff shortages and finding qualified people to fill the cybersecurity skills gap.
- ✓ Small and midsize teams especially are concerned with downtime or business outage (50%) over threat hunting.
- ✓ A SOC will help empower organizations to detect, investigate and respond to cyberattacks an average of at least 51% faster or more.



24x7 Detection & Response

Across 3 Main Attack Pillars



1

Endpoints

- ✓ Windows, Linux & MAC OS
- ✓ Event logs, advanced breach detection/isolations & threat hunting

2

IT Network Infrastructure

- ✓ Edge Devices, Systems and Firewalls
- ✓ DNS, WHOIS, Threat reputation investigations and monitoring

3

Cloud Applications

- ✓ Microsoft 365 & AzureAD
- ✓ Event log analysis and monitoring of Active Directory access and activities
- ✓ Monitor & Identify Malicious logins or anomalous behaviors or changes

It's Time For A Proactive & Preventative Security Defense

What's In It For You?



Proactive & Preventative Security Management

- ✓ Improved Security Posture & Effectiveness of Security Tools/Strategies



24x7 x 365 SOC Cover/Support

- ✓ USA, UK, Germany, Cyprus



Overcome IT Skills & Resource Gaps

- ✓ Leverage Veteran IT & Cybersecurity Specialist and Analysts



Increased Threat Awareness & Risk Mitigation

- ✓ Real-time trending and expanded data analytics



Critical Documentation & Record keeping for:

- ✓ Event Log & Activity Tracking and
- ✓ Incident / Notification Records



CUSTOMIZABLE!

- ✓ Solutions Designed for the Unique Needs of YOUR Organization

People + Process + Technology = Comprehensive Security Defense



**Visit our Booth to find out
more**

THANK YOU

Lampros Katsonis

Solutions Director



l.katsonis@guardbyte.com.cy

T. [+357 22 150 771](tel:+35722150771) (CY)



www.guardbyte.com.cy