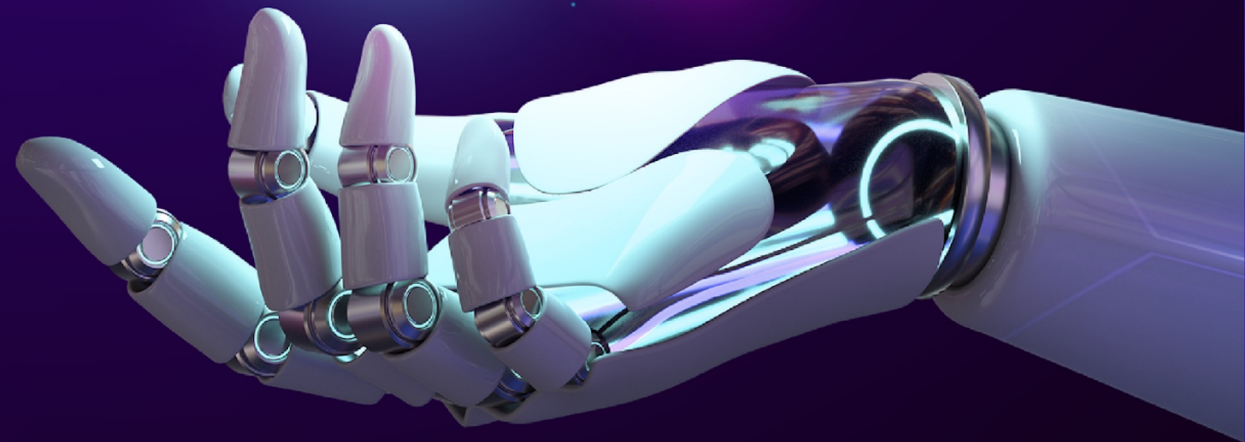


INFINITY GLOBAL SERVICES

Building Cyber
Resilience



ASSESS OPTIMIZE MASTER RESPOND



Agenda

- I. Threat landscape, challenges and opportunities
- II. About Infinity Global Services
- III. Big News
- IV. Our Pillars
- V. Infinity Global Services operations
- VI. Q&A

THE THREAT LANDSCAPE IS CONSTANTLY EVOLVING

+34%

Cyber-attacks

+59%

Ransomware attacks

27%

Of organizations experienced cloud security incident

Supply chain attacks

was responsible for 62% of Intrusion incidents



WE UNDERSTAND YOUR CHALLENGES & OPPORTUNITIES

We are moving quickly on **digital transformation**, moving to the cloud and migrating systems. Can you help us to make sure they are cyber secure?



What do we need to do to improve our existing security operations to match the current threat landscape?



Our remote workforce means **1,000s of new devices and endpoints** on our networks and systems, how do we track and manage them all?



How can we create a future of trust across the enterprise and with our customers?

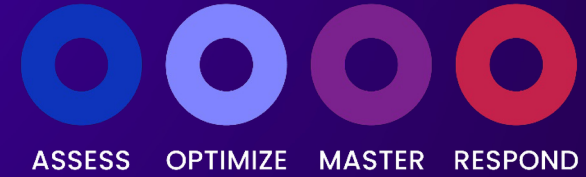


How do I manage the **complexity of compliance** with the evolving regulatory environment?



How do I prepare our organization for and defend against today's sophisticated cyberattacks?





Introducing:

Infinity Global Services (IGS)

Comprehensive, vendor agnostic cybersecurity services organization that offers Assessments, Consulting, Workforce Development, IR, MDR and Managed Services under one roof.

UNIFYING ALL CONSULTING AND MANAGED SERVICES ORGANIZATION UNDER ONE ROOF



Professional Services | Assessment | Training | MDR | Incident Response

Infinity Global Services (IGS)

Top Cyber Experts

+350

Security Consultants

+150

Security Researchers

Covering

Millions

of assets from Network,
Cloud & Endpoints

Leveraging

+150

Certified Trainers

2B

Security Decisions
Daily by **Threat Cloud AI**

100K

Customers

+100

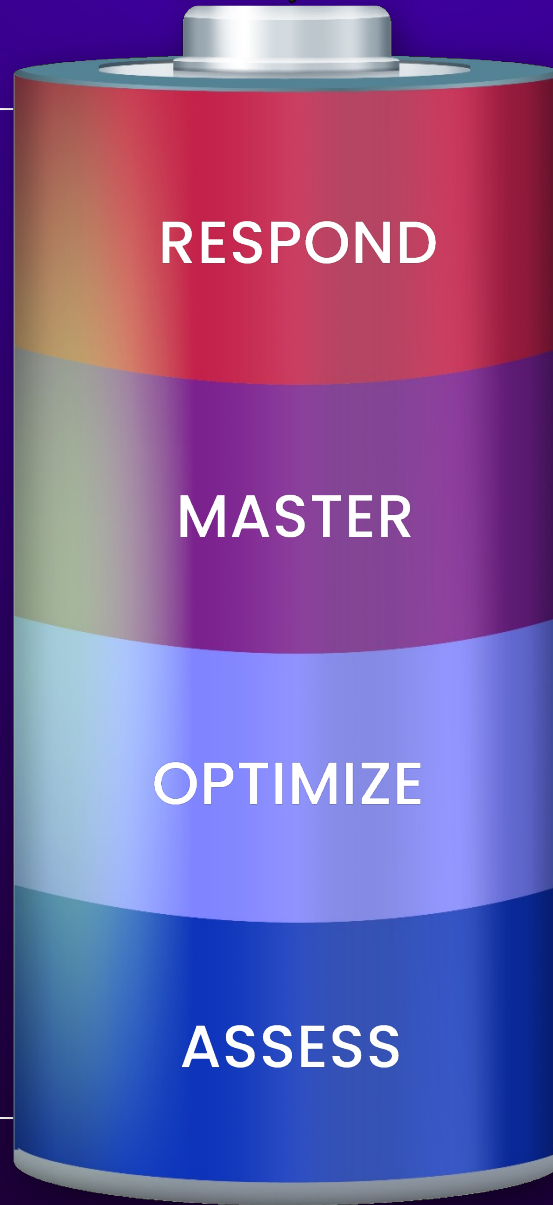
Locations

CYBER MATURITY JOURNEY

Supercharge Your Cyber Resilience



100%
⚡



+30 services

- MXDR
- MDR
- Incident Response
- Threat Hunting

- CISO Academy
- Certifications
- Skills Training
- Security Awareness
- Phishing Simulation

- Cloud Migration and Management
- SOC/NOC
- CISO as a Service
- Architecture & Design
- Cyber Research as a Service

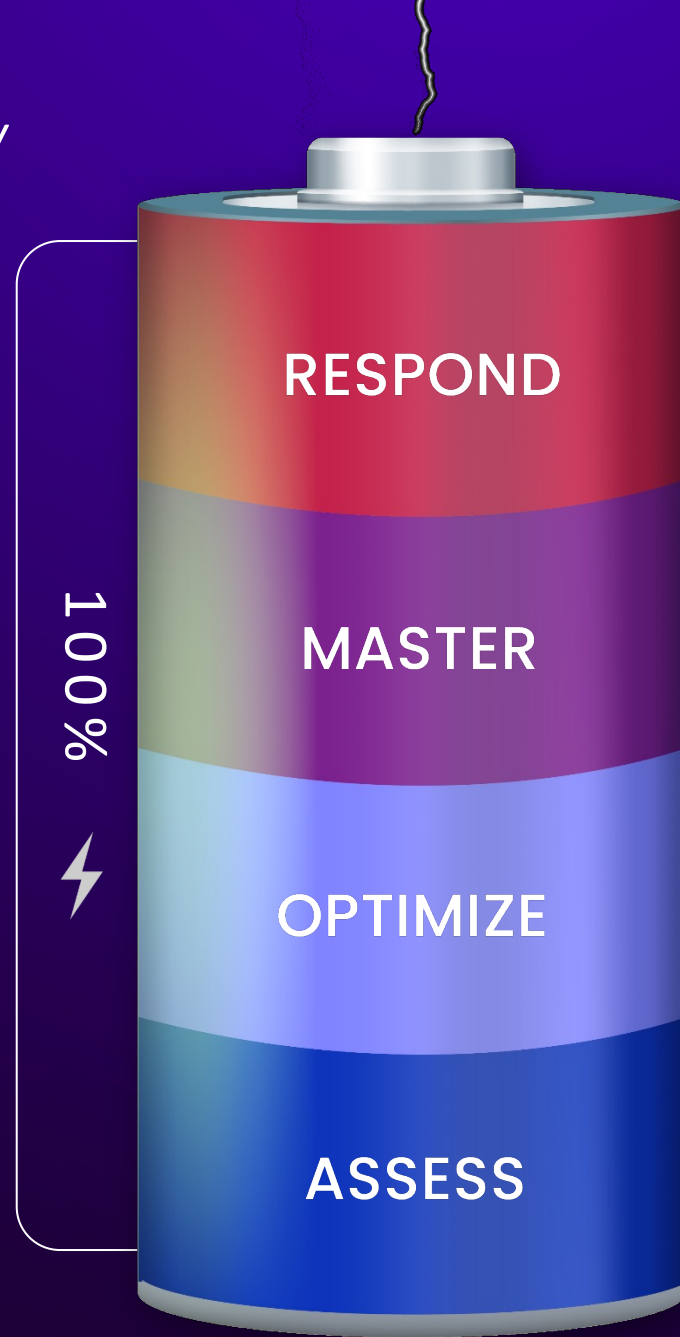
- Cyber Risk Assessment
- Threat Modeling
- Cloud Maturity
- Pen Testing

See the Services
Directory for a complete
list of our offering

We have big news for you
in today's presentation!

CYBER MATURITY JOURNEY

Supercharge Your Cyber Resilience



+30 services

NEW

MANAGED

Sample of managed services:

- SOC as a Service
- NOC as a Service
- Managed CSPM \ CNAPP
- Managed XDR and SIEM
- Cloud Migration and Management Services

See the Services
Directory for a complete
list of our offering

MANAGED

IGS Managed Services

NEW

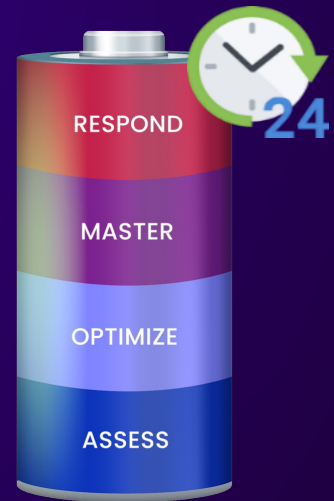
Service offering combining Proactive and Reactive Services

24/7 Global Team with Service Level Objectives

Check Point and 3rd Party Products and Services

Comprehensive Scope Coverage including

- Realtime monitoring
- Ongoing configurations and troubleshooting
- Continual policy tuning and Incident Management
- Advanced Check Point Product Support



IGS Managed Services

Examples of new expanded capabilities



SOC as a Service --->

NOC as a Service --->

Managed CSPM \ CNAPP --->

Managed XDR and SIEM --->

Cloud Migration and Management Services --->

Managed Firewalls – Quantum and 3rd Party

Managed Network and SDWAN

Check Point CloudGuard, Harmony and Microsoft Cloud

MDR / EDR Advanced – Harmony, Horizon and Microsoft Sentinel

Managed Microsoft 365 and lift-and-shift Migrations

ASSESS

CYBER RISK ASSESSMENT

Use Case: Helping leadership understand Cyber Security Risk

Assessment

- Documenting the attack surface
- Covering People, Processes and Technology
- Framework Driven NIST / NIS2 / CIS
- Full technology and process GAP analysis
- Threat Intelligence led Threat Modeling



$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

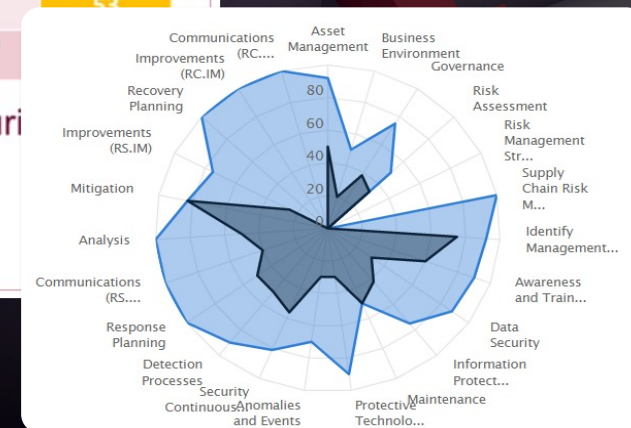
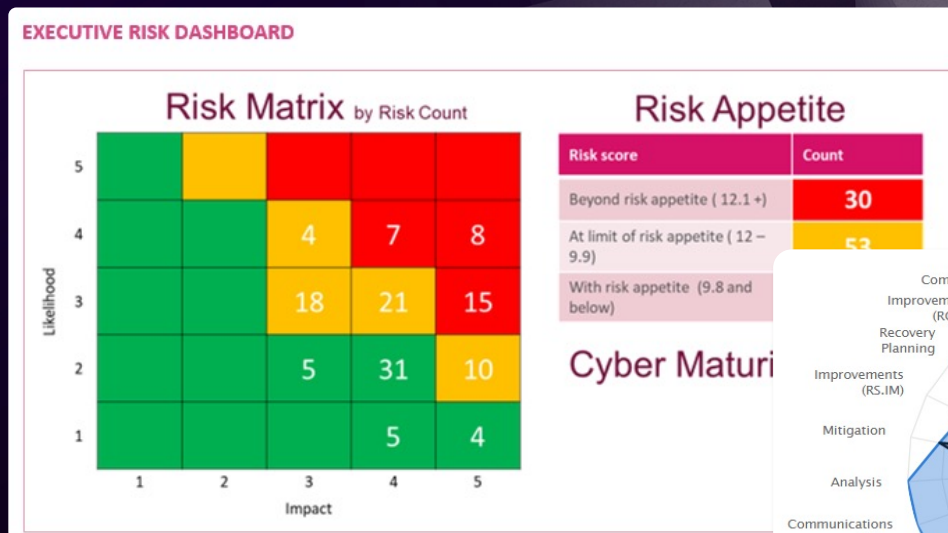
Short Description: CISO is required to have a practical and realistic view of their cyber risk

CYBER RISK ASSESSMENT

Use Case: Helping leadership understand Cyber Risk and take an action

Recommendations

- Detailed Report including Cyber Security Risk Register
- Vendor agnostic risk mitigation advise
- Remediation planning and roadmap



Outcome: CISO reports risk to the board and CIO and based on the gap analysis selects security technology to mitigate the risk

CLOUD SECURE TRANSFORMATION

Use Case: Cloud Security Analysis

Analysis

- Review cloud security and Risk posture
- Covering People, Processes and Technology
- Assess controls and environment
- DevSecOps and SDLC assessments
- Shared responsibility model analysis



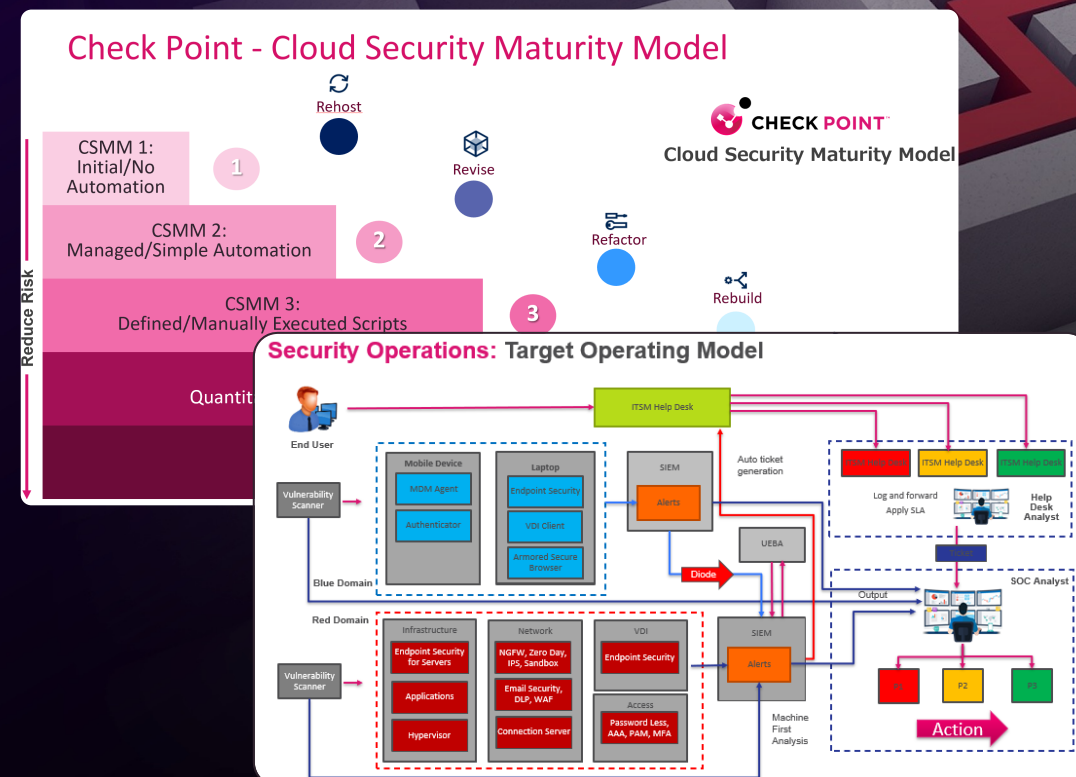
Short Description: Helping customers to understand their current security posture in the Cloud based on People , Process and Technologies in depth analysis

CLOUD SECURE TRANSFORMATION

Use Case: Cloud Security Analysis

Deliverables

- Cloud Security Maturity Modeling based on CSMM (CSA)
- Cloud Cyber Risk and Readiness Assessments
- POAM, SOP Development
- Target operating model development (TOM)
- Automation and code development



Short Description: Using Security Maturity Level, risks and relevant threats, to help customers navigate a move to the cloud while adopting new technology and operating model

OPTIMIZE

Global financial bank chooses Check Point Professional Services to assist with data center migration



Challenges

- Data center move presented a risk to global security operations
- Need to coordinate multiple global IT, business and security operations teams
- Dynamic security environment with constant policy changes

Approach

Leverage Check Point Professional Services' organization expertise and experience to mitigate data center migration risks.

- Build custom lab environment and document necessary migration steps
- Coordinate customer stakeholders around the globe
- Around the clock migration support

Global financial bank chooses Check Point Professional Services to assist with data center migration



Achieved Outcomes

- Smooth migration enabled by a global team of experts
- Minimal freeze window for changes allowed for a rapid return to normal security operations in support of business needs
- Mitigated risks thanks to custom lab environment and through documentations process

U.S. State government embarks on a digital transformation journey with Check Point Professional Services



Challenges

- Legacy security infrastructure unable to scale their future growth
- Desire to update team skill set, processes and procedures to build for the future without compromising immediate needs to support their constituents

Approach

Leverage Check Point Professional Services' resident engineer program

- Lead migration to new Check Point security architecture at data centers and remote locations
- Integrate resident engineer into IT security team as a mentor and guide
- Assist with defining a roadmap for the future

U.S. State government embarks on a digital transformation journey with Check Point Professional Services



Achieved Outcomes

- New security architecture is up and running with capabilities to support growing application needs of the state's constituents
- IT team has significantly grown in their knowledge of latest Check Point solutions
- Moving forward with implementing new architecture in the cloud

MASTER

CISO Academy

Enhancing Cybersecurity Leadership Skills through CISO Academy

Distinguish Yourself With Globally-Recognized Certifications
by Globally-Recognized Organizations



CISO'S SECRETS
PODCAST 

World's leading CISOs
share all their SECRETS
Tune in now!



SECURITY AWARENESS TRAINING

Mitigating Phishing Threats Through Security Awareness Training



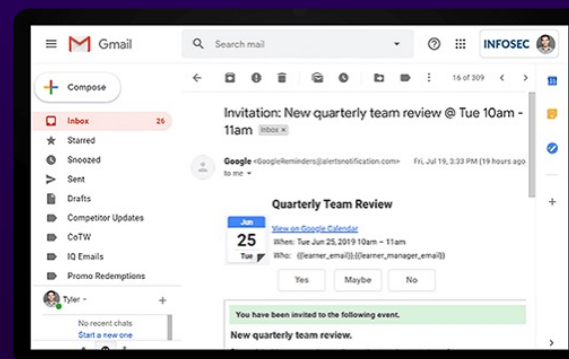
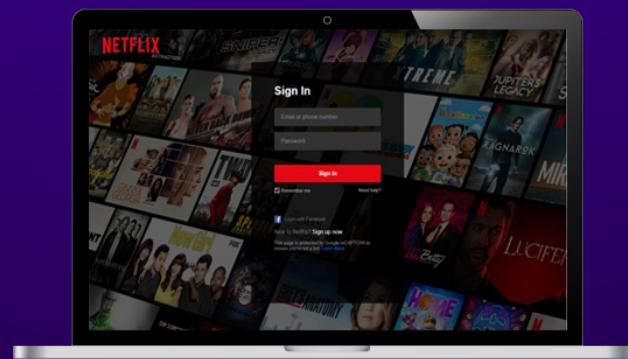
Security Awareness
LEARN MORE

Phishing Simulations
LEARN MORE

Program Automation
LEARN MORE

Reports & Assessments
LEARN MORE

Empower Your Workforce.
Secure Your Organization.



Supporting
30+
Languages

800
Training
Modules



RESPOND

MDR Identifying Active Threat Use Case

Use Case: Abnormal Login

- Detection: Multiple Email security product alerted and were aggregated into one MDR Case.
- Investigation: MDR SOC Analysts confirmed activity is abnormal.
- Escalation: Engage Check Point Incident Response Team.



MDR Identifying Active Threat Use Case

Use Case: Abnormal Login – The Details



MDR customer events can be aggregated into a single MDR case. This case contained alerts for:

- strange/Malicious Domain that mimics outlook.com
- first login from new device
- first login from new country
- first login from Privacy VPN

MDR SOC analysts worked quickly with the customer to confirm these alerts are true positives and proved a threat actor has compromised valid credentials.

To tell the whole story and create an event timeline, the customer leveraged some of their free reactive Incident Response hours.

IR Digital Forensics Use Case

Use Case: Data Breach - Same Case as MDR

- Detection: Abnormal login and compromised credentials discovered.
- Evidence Capture:
 - Logs from cloud applications
 - User mailboxes
 - Forensics images of workstations
- Analysis: Evidence reviewed to tell whole story, provide timeline, and identify data accessed by threat actor.
- Identify: Enumerate every file accessed/viewed by threat actor.
- Report & Recommendations: Full story of compromise, lateral movement, and data accessed. Security enhancement suggestions provided.



IR Digital Forensics Use Case

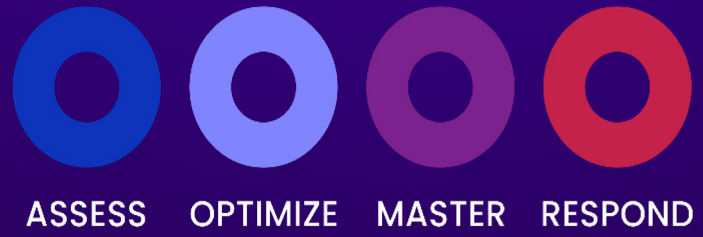
Use Case: Data Breach - Same Case as MDR



Leveraging the initial finding from our MDR SOC, the IR team jumped in to build the entire timeline and identify what data was accessed by the threat actor.

The most important deliverable to our customer was our IR report which includes:

- Timeline and description of Threat Actor activity from initial compromise to lateral movement
- Enumerates files accessed by Threat Actor
- Provides recommendations to prevent this attack chain wherever possible



AUGMENTING PARTNERS CAPABILITIES AROUND THE WORLD!



1. IGS augments its partners' capabilities, expanding their cybersecurity reach, benefiting both partners and customers.
2. The IGS partner program offers a spectrum of services, including security assessments, consulting, incident response (IR), and managed detection and response (MDR), enabling partners to provide comprehensive cybersecurity solutions.
3. Collaborating with IGS enhances customers' cybersecurity posture through access to a wide range of services, fostering trust in partner-provided solutions and proactive threat mitigation.

IGS PORTAL

Find the right **Security Services** for your organization.

Search any security service...

Search



ASSESS

Security evaluation and pentesting

- Risk Assessment
- Penetration Testing
- Maturity Assessment
- Readiness Assessment

[View more](#)

OPTIMIZE

Consulting and optimization

- Remote consultation days
- Advanced Technical Account
- Infinity Security Design
- Hybrid Cloud Security

[View more](#)

MASTER

Upskilling and training

- Training Courses
- Boot Camps
- HackingPoint
- Self-Paced Cyber Security Training

[View more](#)

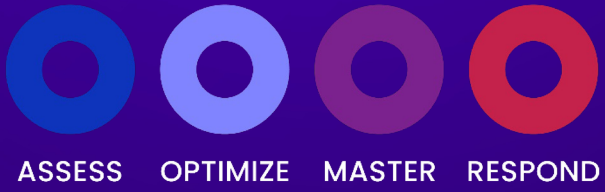
RESPOND

Incident response and NDR

- Incident Response
- Expert Malware Analysis
- Expert Threat Briefing
- Digital Forensics

[View more](#)

Discover the right security services for your organization.



THANK YOU FOR LISTENING

LEVEL UP YOUR SECURITY SERVICES

START NOW!

<https://IGS.CHECKPOINT.COM>

Connect an IGS services expert:

Services@checkpoint.com