Gateway Digital

G'SECURE LABS
INFORMATION & CYBER SECURITY CONSULTING SERVICES

CYBER SECURITY IN 2021

CHALLENGES & TRANSFORMATION

www.gsecurelabs.com

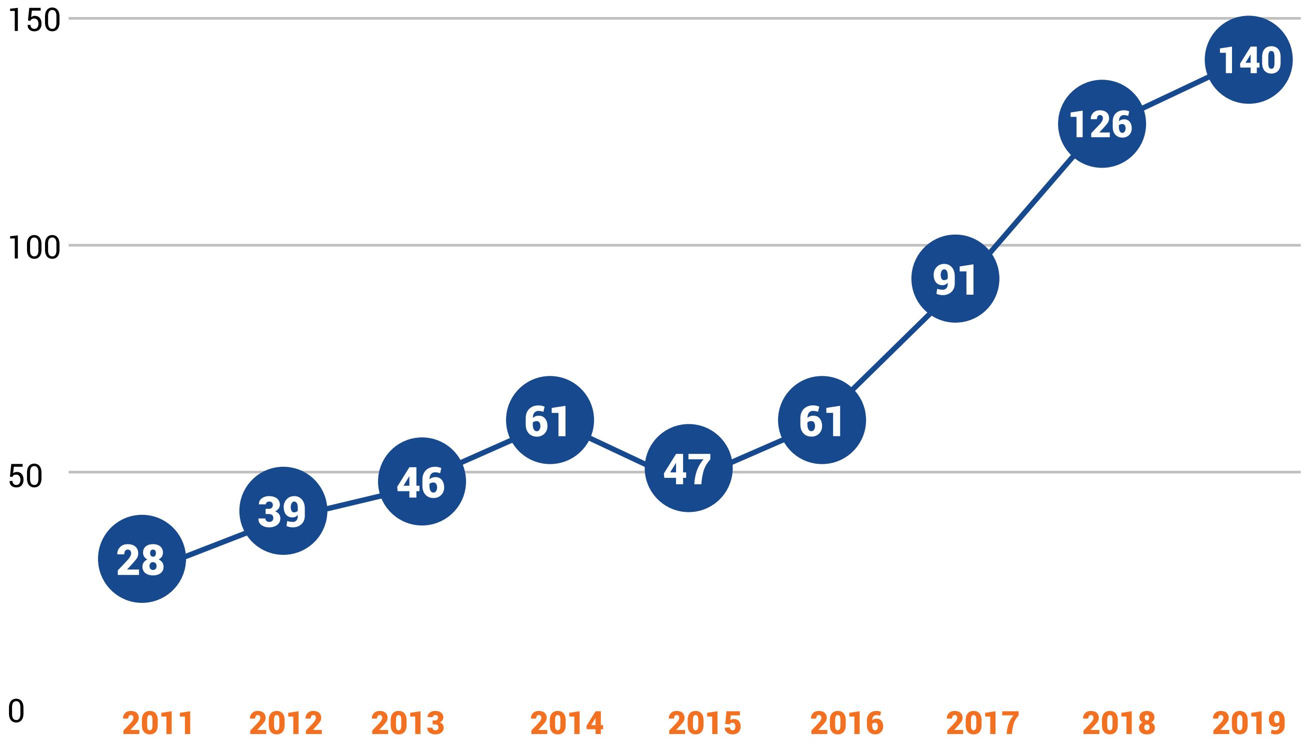
Introduction

Gateway Digital's Cybersecurity Service arm **G'SECURE LABS** delivers SaaS-based Managed Detection & Response Services. Our unique approach of augmenting the security practices using AI & ML-based engines transforms the security service outcomes in terms of accuracy of detection, speed of response, and time to recover.

Our state-of-the-art cybersecurity operation centres are equipped with intelligent technologies and an elite panel of cybersecurity experts to safeguard your digital ecosystem.

We have designed a proactive stack of assessment and testing services to reduce the attack surfaces and ensure that your digital assets are robust to handle any cyber-attacks.

NUMBER OF CYBER BREACHES: 2011 - 2019



Cybersecurity Trends in Past Decade

Cybersecurity breaches have grown exponentially in the past decade is expected to continue on its growth rate. In the past decade, cybersecurity practices have evolved based on varying trends of attack methods, malware sophistication levels and motives of attackers. Here are some trends observed in the cyber-attacks.

As per leading cybersecurity research organizations:

» There were 144.91 million new malware samples in 2019 (AV-Test), and we're already at 113.10 million new samples in 2020. (as of midway through November 2020)

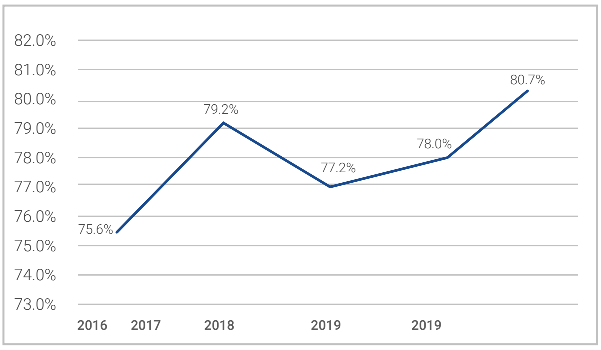
» In 2019, 93.6% of malware observed was polymorphic, meaning it has the ability to constantly change its code to evade detection. (2020 Webroot Threat Report)

» Almost 50% of business PCs and 53% of consumer PCs that got infected once were re-infected within the same year. (2020 Webroot Threat Report)

Additionally, it shows that there are no exceptions in terms of targets for attacks, and almost every organization irrespective of its size or industry has experienced some other kind of cyber breach.

» Malicious hackers are now attacking computers and networks at a rate of one attack every 39 seconds. (University of Maryland)

» 81% of surveyed organizations were affected by a successful cyberattack. (CyberEdge Group 2020 Cyberthreat Defense Report)



The above chart indicates the percentage of companies targeted by at least one cyber-attacks in a year.

What has been most challenging?

The most vulnerable asset in the current security scenario is DATA. It is a common fact the data in motion is more vulnerable than data at rest, But the emerging challenge of RANSOMWARE attacks have compelled security specialists to think otherwise. The incidents related to ransomware attacks have grown manifolds in a couple of years and are expected to grow more.

Interestingly the Nordic region has come across a new racket call ransomware-as-a-service which helps the hackers to create targeted ransomware attacks. The given facts suggest the gravity of the problem.

» US ransomware attacks cost an estimated $7.5 billion in 2019. (Emsisoft)

» Almost 200 million ransomware attacks occurred in the first nine months of 2020, representing a large increase over the previous year. (SonicWall)

» A ransomware attack in early 2020 on the New Orleans city government cost the city upwards of $7 million. (SC Magazine)

» In February 2020, a ransomware attack cost Denmark-based company ISS upwards of $50 million. (GlobeNewswire)

» Since 2016, a total of 172 ransomware attacks have cost US healthcare organizations $172 million. (Comparitech)

» One out of five Americans has dealt with a ransomware attack. (The Harris Poll)

» Ransomware is involved in 27 percent of malware security incidents, up from 24% in 2019. (Verizon 2020 Data Breach Investigations Report)

» Ransomware payments continued their steep incline in Q3 2020. The average sits at $233,817, which is up 31% over the previous quarter and a whopping 468% over Q3 2019. (Coveware's Q3 2020 Ransomware Marketplace report)

The average downtime due to a ransomware attack was 19 days in Q3 of 2020 compared to 12.1 days in Q3 2019. (Coveware's Q3 2020 Ransomware Marketplace report)

The ransomware not only has caused business loss due to downtime but also have severely damaged the financial standing and brand reputation of the organizations. The facts and figures which confirm this are -

» Ransomware attacks can be extremely costly. For example, an attack involving the NotPetya ransomware cost shipping firm Maersk more than $200 million.

» In 2019-2020, the average global cost to remediate a ransomware attack was $761,106. (Sophos The State of Ransomware 2020)

» Organizations in India, Brazil, Turkey, Belgium, Sweden, and the US are most likely to be hit by ransomware attacks. In India, the prevalence is especially high, with 82% of organizations dealing with ransomware. Brazil has the next highest rate at 65%. (Sophos The State of Ransomware 2020)

» The number of mobile ransomware Trojans decreased over the course of 2019 and the first half of 2020. Kaspersky saw 23,294 in Q2 2019 and just 3,805 in Q2 2020. (Kaspersky Labs)

» **The percentage of victimized organizations that paid associated ransoms rose considerably this year, from 45% to 57.5%"** mentions Imperva in their 2020 Cyberthreat Defense Report.

What else is Alarming?

It would not be wise to consider that the hackers' toolbox only contains ransomware, some research studies and statistics indicate that tricks used by hackers have become more sophisticated and challenge the traditional methods of cybersecurity.

Some of the popular tricks used by black hat guys are cryptojacking and social engineering. The processing power required for cryptocurrency has motivated cybercriminals to develop simpler programs which can infect user machines and then harness the power for crypto mining.

"The percentage of victimized organizations that paid associated ransoms rose considerably this year, from 45% to 57.5%" mentions Imperva in their 2020 Cyberthreat Defense Report.

Apart from Cryptojacking, the most popular and emerging attack vector is social engineering as it is a known fact that the weakest link in most of the cases of cyber breaches is the end-users.

Cybercriminals use all the methods to target uninformed and unwatchful users which cause major problems for CISOs, CIOs and other security teams. It has been evident in the past that the negligence of an internal user can bust even a robust security framework.

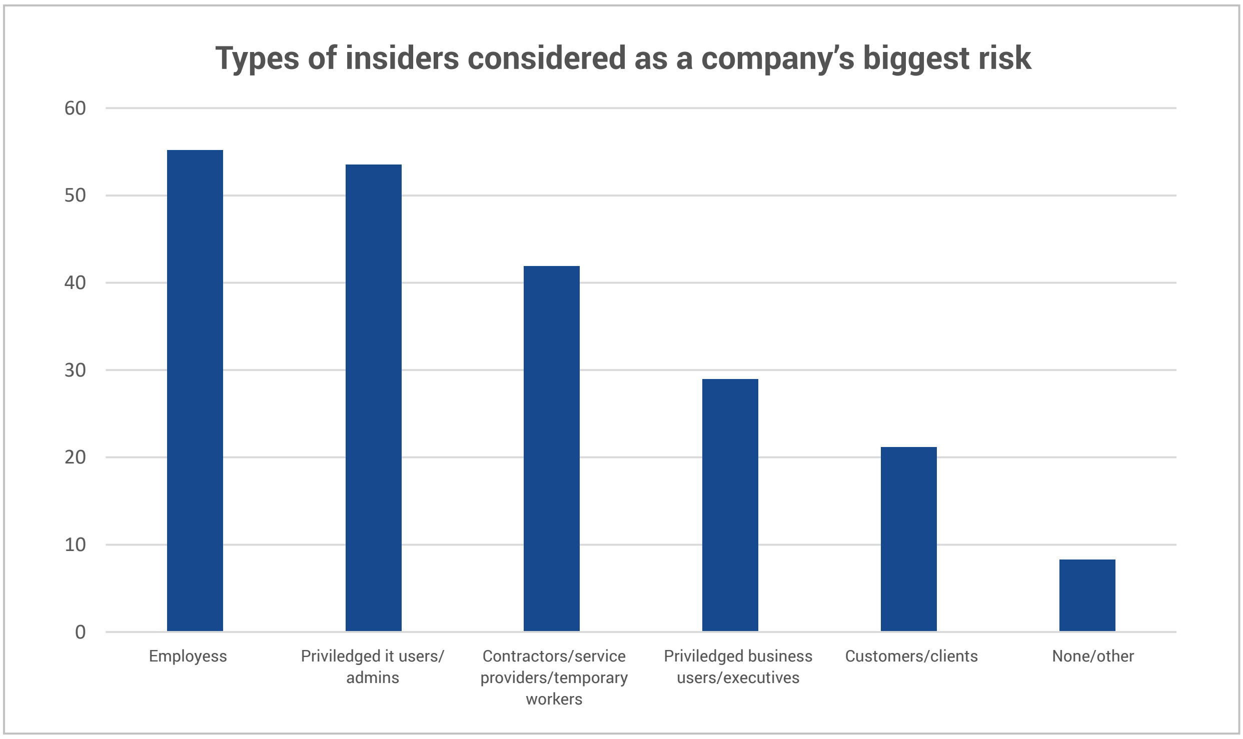


Figure 22: Types of insider threats and their risk level[324]

Phishing attacks are have reached to their highest level in last 2-3 years.

- In Q3 of 2019, APWG observed more than 260,000 phishing attacks. (APWG's Phishing Activity Trends Report for Q3 2019)

- **Almost 74% of phishing attacks involve credential phishing.** (Cofense's Phishing Threat and Malware Review 2019)

- The most frequent targeted attack vector is spear phishing. (Symanetc's Internet Security Threat Report 2019)

SPEAR PHISHING

65%

of groups used spear phishing as the prmary infection vector

INTELLIGENCE GATHERING

96%

of groups' primary motivation contirues to be intelligence gathering

Symantec's Internet Security Threat Report 2019

- **Scammers and attacks send out 6.4 billion fake emails every day.** (EY – Global Information Security Survey 2018-2019)

- **Small organizations receive malicious emails at a higher rate.** (Symantec's Internet Security Threat Report 2019)

- **Mining companies are most likely to receive malicious emails.** (Symantec's Internet Security Threat Report 2019)

» **Webmail and SaaS users are the biggest targets of phishing attacks.** (APWG's Phishing Activity Trends Report for Q3 2019) The most targeted industry segments are:

» Phishing is the number one type of threat action involved in data breaches. (Verizon's 2020 Data Breach Investigation Report)

» Verizon reports that **30 percent of phishing emails in the U.S. are opened,** with 12 percent of those targeted by these emails clicking on infected links or attachments. (Verizon)

» Microsoft reported **a huge increase of 250% in phishing emails between January and December 2018,** analyzing more than 470 billion email messages every month for this particular threat and for malware. (Microsoft Security Intelligence Report Volume 24)

» The volumes are enormous even for specific attacks: a single campaign during Q1 2018 sent out **550 million phishing emails** over that 3-month period. (EY – Global Information Security Survey. 2018-2019)

» The business world is also aware of this gigantic issue: **22% of surveyed decision-makers see phishing as the biggest threat.** (EY – Global Information Security Survey 2018-2019)

» **30% of phishing sites used HTTPS in 2017** compared to just 5% during 2016, trend experts believe will continue to grow. (ENISA Threat Landscape Report 2018)

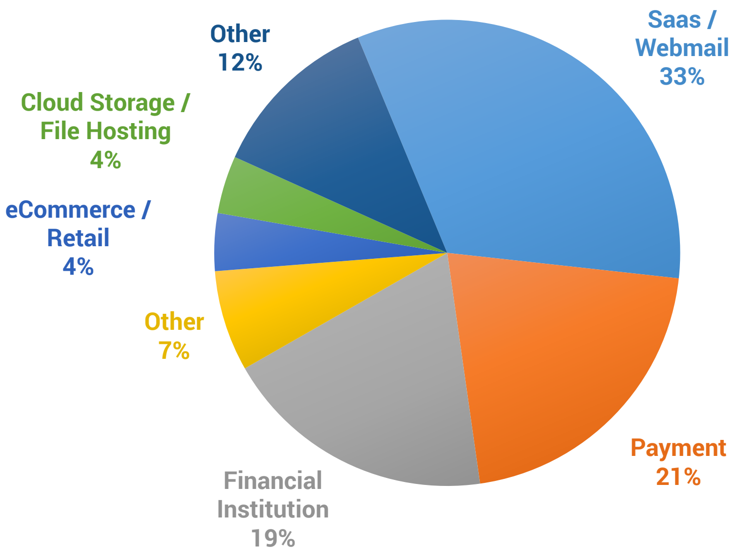
» In 2017, phishing campaigns were short-lived: **phishing websites typically stayed online for 4-8 hours.** (ENISA Threat Landscape Report 2018)

» What's more, in 2017, **phishers used 28% more malicious attachments compared to malicious URLs** in the phishing emails they sent. (ENISA Threat Landscape Report 2018)

» **41% of phishing domains include a single character swap, 32% have an additional character, and 13% have added or removed leading or final domain's characters** to confuse and deceive their victims. (ENISA Threat Landscape Report 2018)

The most targeted industry segments are:

MOST- TARGETED INDUSTRY SECTORS, 3Q2019



APWG's Phishing Activity Trends Report for Q3 2019

Do only large companies get affected?

This myth has been there for quite some time that companies with large scale operations and fat revenue books are the target of cybercriminals. The fact we need to learn is that the cybercrime business has also flourished and extended its reach to the mass market.

It is no longer only nation or state-sponsored attacks, but you can find a bunch of cybercriminals in small cities. Hence, it is no longer valid to think that only big guys need to worry, the victims of cybercrime range from individuals to small shops to multi-national companies.

> *While attacks on household names make headlines, Symantec's telemetry shows that it is often* ***small and medium sized retailers,*** *selling goods ranging from clothing to gardening equipment to medical supplies, that have had* ***formjacking code*** *injected onto their websites. This is a global problem with the potential to affect any business that accepts payments from customers online.*
>
> - 2019 Internet Security Threat Report by Symantec

As we have discussed the current scenario of cybersecurity challenges, we should also discuss what is that 'extra' which is required to overcome these challenges

The history of cybersecurity practices has seen an evolution from manual operations to products to artificial intelligence. Since the sophistication and volume of cyber-attacks have grown exponentially, it can be said neither the products nor the services can alone solve this problem. Let's understand some of the key pointers which will show us the path forward.

Holistic View

The key hindrance in fighting with the current cybersecurity threats will be fractured security stack. It will be of key importance that the isolated security modules are connected and can be watched through a single pane of glass view.

Combination of Man and Machine

To stand against emerging cyber challenges, every organization would require a fine blend of an elite team of experts and intelligent tools. Since its difficult of everyone to achieve this, third-party vendors providing 24x7 SOC services can be of help.

Seamless Monitoring

Since the attack methodologies are sophisticated than they ever were, a 24x7 monitoring, detection and response are inevitable in the current scenario. As this would require a different setup, the companies can choose to take help of professional SOC service providers.

Lots of Automation

The way cyber-attacks are increasing the current approach of manual intervention has to move to as much automation as possible. The need of automation is related to the fact that we have reached the phase when real-time detection and response needs to be realized, and also the limited team of cybersecurity experts should be utilized to solve critical and high-risk problems and response to low risk and redundant breaches.

Zero Trust Zone

The concept of least privilege is elementary in cybersecurity practice but is often not implemented carefully. In this scenario, an organization has to be ready to adopt Identity & Access Management concepts and move towards role-based privileges and access.

Insider Threat Protection

As we have seen from facts and figures that the insider and social engineering attacks are the most prominent attack tactics in coming time. This has been a consistent challenge for cybersecurity teams as the way digitation has grown in the last few years; cyber hygiene practices have not been followed carefully.

This has resulted in ever-rising numbers of social engineering attacks like phishing, online frauds and accidental data loss. In coming time organization have to adopt best cyber hygiene policies and provide training to staff for best practice.

Advance tools and Technologies

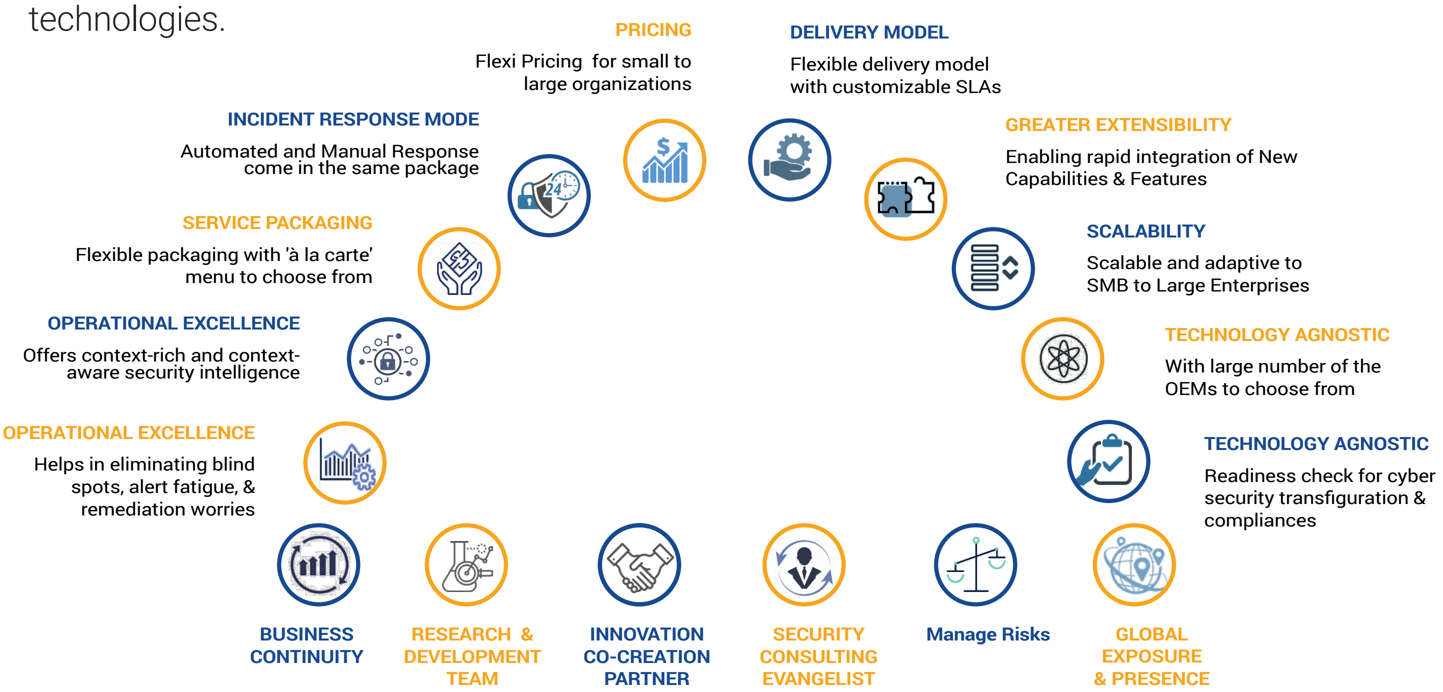
The way cyber challenges have aggravated; the organizations have to change the approach while choosing cybersecurity products. The current situation demands the products to be intelligent and should have learning capabilities. The products should not only act as per configuration but should also be able to transform dynamically in the case arises. For example, the endpoint security products should have strong user baselining function should be able to alert end-user that why the specific action should not be taken.

Proactive Security Services

The exponential increase in digitation related project has transformed the IT operations of the organization and the global pandemic situation as added to it. This has increased the overall attack surface and created many new threat vectors which the cybersecurity experts have to deal with.

How Can Gateway Digital Help?

Gateway Digital through its cybersecurity arm G'Secure Labs, has been engaged in helping organizations to defend against current cyber security challenges. Our state of art 24x7 SOC centres is equipped with a fine blend of an elite team of the cyber security team and intelligent technologies.



PRICING
Flexi Pricing for small to large organizations

DELIVERY MODEL
Flexible delivery model with customizable SLAs

INCIDENT RESPONSE MODE
Automated and Manual Response come in the same package

GREATER EXTENSIBILITY
Enabling rapid integration of New Capabilities & Features

SERVICE PACKAGING
Flexible packaging with 'à la carte' menu to choose from

SCALABILITY
Scalable and adaptive to SMB to Large Enterprises

OPERATIONAL EXCELLENCE
Offers context-rich and context-aware security intelligence

TECHNOLOGY AGNOSTIC
With large number of the OEMs to choose from

OPERATIONAL EXCELLENCE
Helps in eliminating blind spots, alert fatigue, & remediation worries

TECHNOLOGY AGNOSTIC
Readiness check for cyber security transfiguration & compliances

BUSINESS CONTINUITY

RESEARCH & DEVELOPMENT TEAM

INNOVATION CO-CREATION PARTNER

SECURITY CONSULTING EVANGELIST

Manage Risks

GLOBAL EXPOSURE & PRESENCE

1. 24x7x365 SOC Operations for Seamless Security :

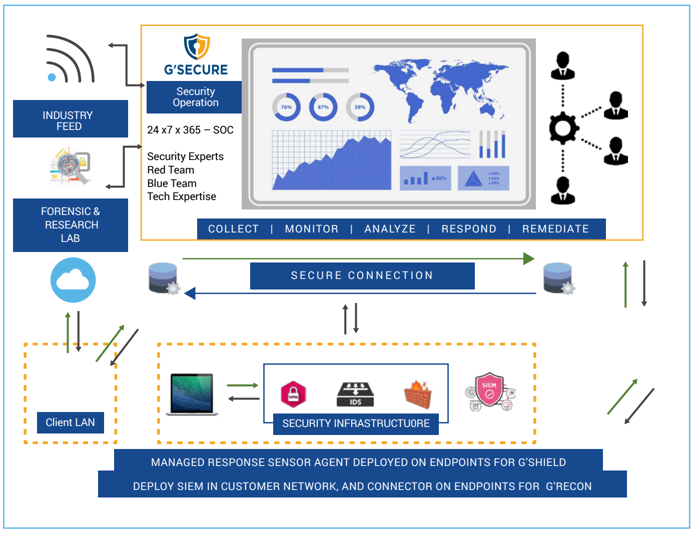
Our 24x7x365 operations are designed to cover security assessment, incident response, and remediation, our SOC centre leverages AI & ML-based technologies and industry-specific security experts to provide bespoke security services. Our security approach is built on consolidating the fractured security stacks and automating the response actions to achieve accuracy, real-time response and faster recovery.

CYBER SECURITY OPERATIONS

- CSOC in Europe and India
- NIST, GDPR Compliant
- Team of Cybersecurity Specialists

MANAGED SERVICES OPERATIONS

- Remote management and monitoring
- Secure connection to your network
- Advance Forensics
- Red & Blue Team Services
- All data is local to you
- Data only for select escalations sent to our CSOC
- Process: Collect, Monitor, Analyze, Respond, Remediate



INDUSTRY FEED
FORENSIC & RESEARCH LAB
G'SECURE
Security Operation
24 x7 x 365 – SOC
Security Experts
Red Team
Blue Team
Tech Expertise
COLLECT | MONITOR | ANALYZE | RESPOND | REMEDIATE
SECURE CONNECTION
Client LAN
IDS
SIEM
SECURITY INFRASTRUCTU0RE
MANAGED RESPONSE SENSOR AGENT DEPLOYED ON ENDPOINTS FOR G'SHIELD
DEPLOY SIEM IN CUSTOMER NETWORK, AND CONNECTOR ON ENDPOINTS FOR G'RECON

2. Managed Detection and Response (MDR):

Our MDR Practice is designed by weaving a robust fabric of best in class cybersecurity solutions and an expert workforce to provide blanket protection from new-age threats and cybersecurity risks. With 2x7x365 monitoring, detection and response, we safeguard your entire digital space. We underline our managed security services through SOC as Service, SIEM as a Service and consultative services.

Our MDR Services Include:

- **Monitoring, Detection & Response on a 24 x 7** basis backed up by SLA's for critical network assets & applications.
- **Security incident management and response** by team of experience and qualified teammembers.
- **Threat Hunting & Response** Orchestration
- **Blue Team Services.**
- **Integration** with best suited **SIEM technology.**
- **Bi-weekly reports** with threat **logs pattern, response history and UEBA**

- Consultative Remediation
- Periodic Penetration and Application Security Testing Services.
- Security Posture Assessment
- Detailed Forensics and Reporting
- Threat modelling & Security maturity model consultation
- Red Team Services
- IAM Security Services

3. Vulnerability Assessment & Penetration Testing:

We take one step ahead and make sure that your digital assets and applications are robust and can stand against wave of cyber intrusions. Our vulnerability assessment and testing service defines, identifies, classifies, prioritizes vulnerabilities and test them in controlled environments. This improves your proactive defense against technological vulnerabilities that can lead to intrusions, fraud and service interruptions.

Our Proactive Defense Suite includes:

Infrastructure Assessment & Testing:

- **Active & Passive Reconnaissance –** Gaining information on the organization
- **Vulnerability Assessment –** Automated and Manual assessment of infrastructure
- **Black Box and White Box Testing –** Testing through disclosed & undisclosed information.
- **Application Security Testing –** testing application in dynamic and static modes.
- **Security Posture Assessment & Cyber Security Defense Maturity Evaluation –** Actualization for better preparation
- **Offensive Security Services –** Blue Team & Red Team services through offensive security experts and ethical hackers.

På Gateway Digital vill vi stå i teknikens och möjligheternas framkant. Vara det självklara valet på er digitala resa och tillsammans med både hjärta och hjärna stå för nytänkande och handlingskraft. Där vi vägleder och skapar lösningar som ger konkreta resultat. Våra konsulter gör skillnad för en bättre, digital och samtidigt en mer hållbar värld.

Vill du vara med på vår resa att digitalisera Sverige och världen? Välkommen till Gateway!

Gateway Digital®

G'SECURE LABS
INFORMATION & CYBER SECURITY CONSULTING SERVICES

For Information and a Free Security Posture Assessment Service Connect with us:

✉ hello@gatewaydigital.se

thegatewaydigital.com/se/
gsecurelabs.com