UNDER DEFENSE

SECURITY OPERATIONS CENTER

Keep your client's data safe and business going & growing with SOC continuous protection

- Business Need of Security Operations Center
- SOC Benefits
- NOC vs SOC
- UnderDefense Incident Response

Version 2 二版 www.version-2.com

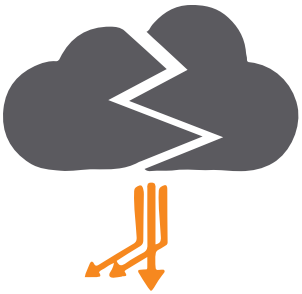
Business necessity of Security Operations Center

Every single organization, that is connected to the network has been or is in risk to be hacked or compromised.

What can it mean for your business?

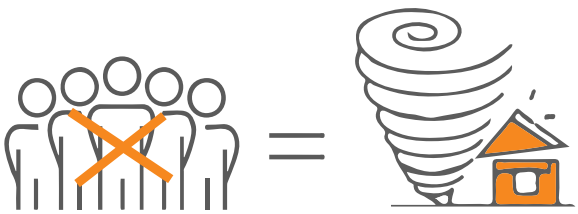
money & reputation
loss

data
loss



resources
damage

- Stop of business operation, which will cause money, resources & clients loss.
- Business can be stolen or might be at risk to be stolen in the near future already.

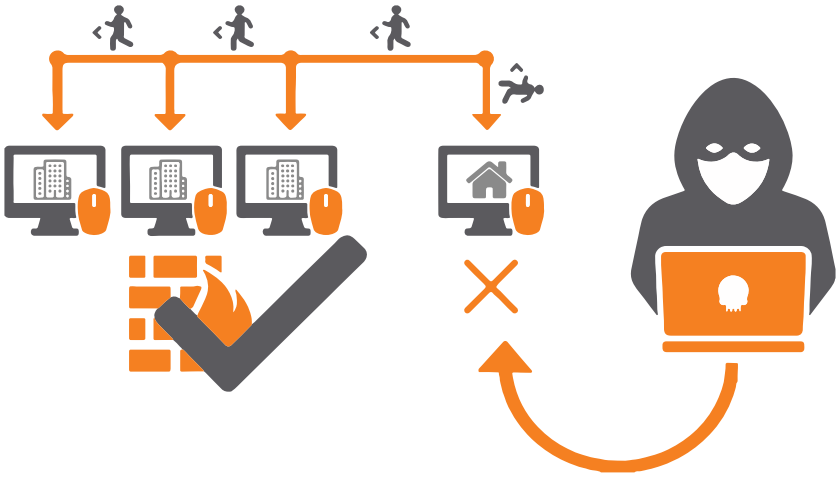


Non existence of Skilled Experienced Cyber Security team who could monitor the business and insights around-the-clock to prevent the catastrophe may lead to business disaster.

9h From 8am to 5pm you are protected

16h But who protects you from 5pm to 8am?

You have to be aware of your risks of disaster and it is not just 8 to 5 Monday through Friday work shifts. Hackers have different schedules and nowadays cybercrime and espionage operate like any other business - when other 16 hours your business is resting - that's where the cyber-intruders come in - and they don't knock on the door.



✓ even if 100 - served
✗ but 3 - not

YOU CAN BE HACKED!

To be overall secure and be able to protect all the assets from being compromised you have to make sure your security plan accounts for the entirety of your organization's critical infrastructure. A plan that doesn't include threat intelligence updates leaves your organization vulnerable to emerging threats.

SOC Benefits

We provide three most important assets for your business and your clients:

UnderDefense SOC is a 24x7x365 Cyber Security Defense through managing security of all your network devices, servers and Cloud Infrastructure. Our professional cyber security experts assist organizations with anomaly and intrusion detection, providing deep analysis and alerting of suspicious events, identifying gaps in existing security controls, and highlighting advanced persistent threat (APT) behavior.

Together we define the main goals you eager to achieve as soon as possible and the scope for our delivery of Managed Security Service/Security Operation Center.

1

People (experts)

2

Process
(drive complince)

3

Tools (managing security of infrastructure, SIEM)

UnderDefense quickly identifies security breaches, resulting in faster response and remediation times.

ability to prevent business disaster & chaos

UnderDefense provides with loyal, predictable, ongoing fixed cost.

lets you set the appropriate budget with no further changes.

UnderDefense specializes in Splunk, provide consulting, remote management, address complex security monitoring, compliance and reporting requirements.

rare and high quality expertise at your service on demand.

Affordable services and lower costs let small and medium businesses own UnderDefense Virtual SOC, stay safe, secure 24/7.

save money & afford your business run stable, confident and secure.

Full access to security expertise which is difficult to find and hire.

we cover a full spectrum of your organization's security services needs.

UnderDefense provides services to companies of different sizes and industries.

our services is the right fit for your business

UnderDefense SOC is ready to use.

0 money spendings on in house implementations.

You pay as you go.

full control of where your business money goes

Huge ROI and quick, tangible and visible result.

your PoD is Security Operations Center that will bring more clients, money and references.

Unique and high quality expertise in both offence and defence sides.

we are experts in hacking so that we can catch the hacker in your system and defend it.

Modern business has to be agile, to detect and respond incidents faster. SOC is the right instrument to resolve this problem - to have full visibility, control, notification and response to latest cyber threats.

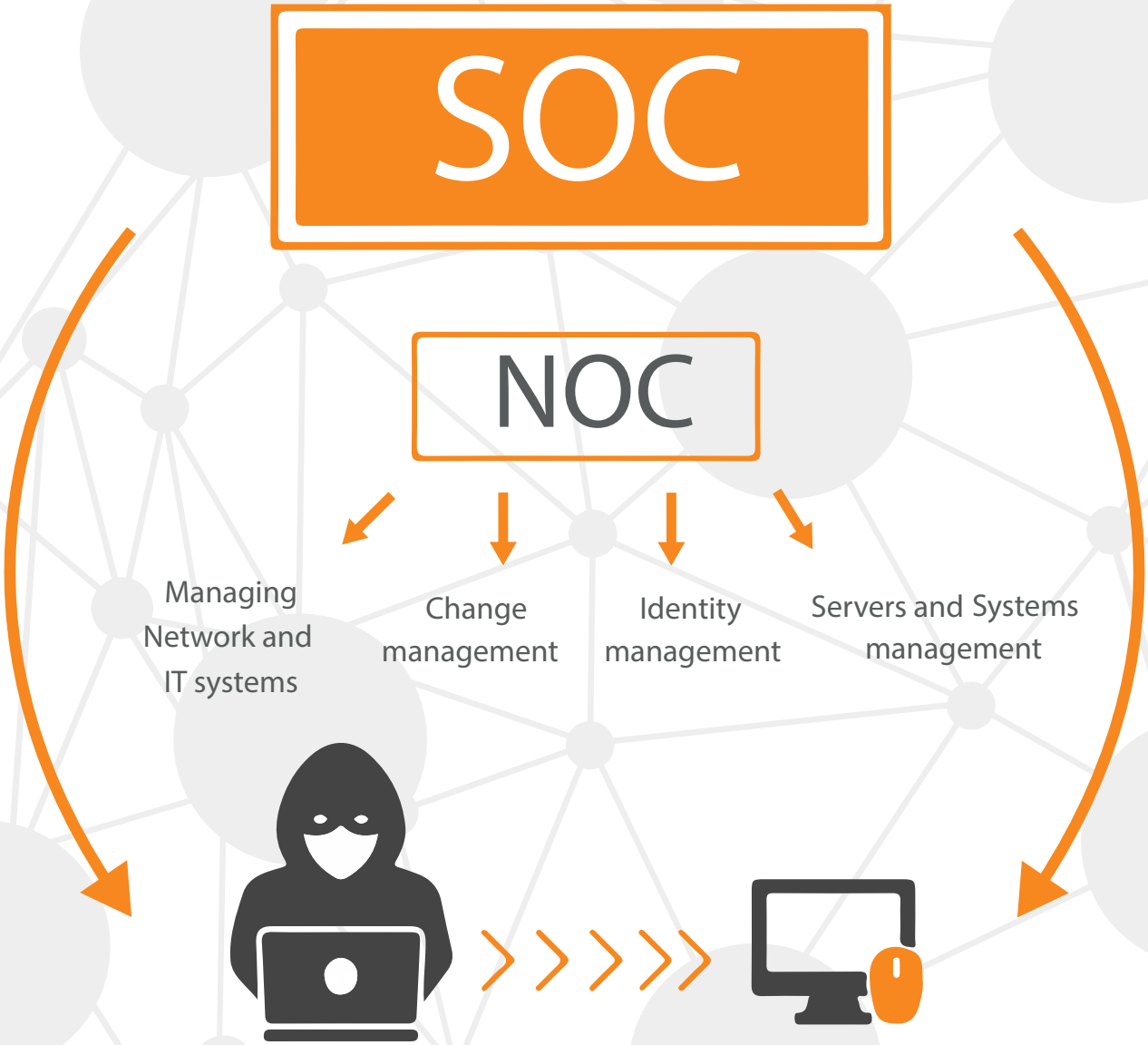
visibility

control

notification

response

With UnderDefense SOC there is always a team of certified professional cyber security experts who 24 hours a day 7 days a week and 52 weeks a year monitors your system and responds to the attacks that are here to ruin your business.



UnderDefense SOC team provides the 360-degree security visibility that you need for full situational awareness across your cloud, hybrid cloud, and on-premises environments. Our approach combines the essential capabilities your organization needs into a single solution, including asset discovery, vulnerability scanning, intrusion detection, behavioral monitoring, SIEM, log management, and threat intelligence.

NOC is helpless without SOC when it comes to Security

Security Operations Center is a higher level of business security, development and growth.

Network Operations Center and Security Operations Center don't compete - these two centers supplement each other.
Network Operations Center or Internal IT is a basic service existing inside your business while Security Operations Center is an upper layer, a higher level of business security, development and growth.

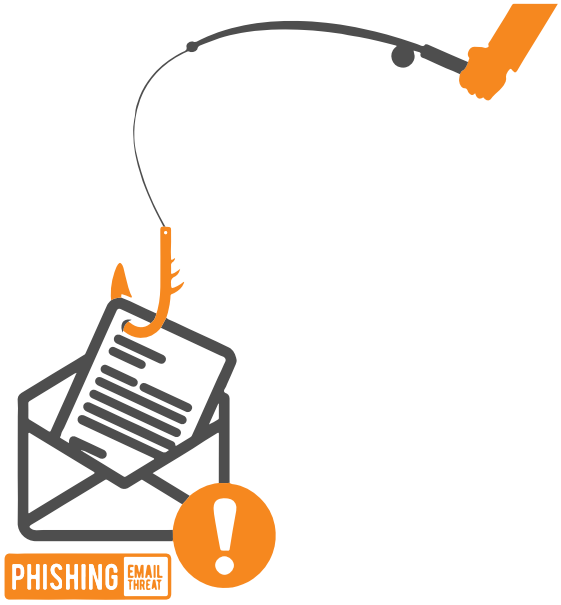
SOC helps your business grow successfully

Having NOC at your organization indeed has its benefits but to be fully secure and safe NOC is not enough to protect your business. NOC staff won't be aware of any type of malware, ransomware or just random hacker who compromises your network, clients database using the holes in your system to steal the important data.
Security Operations Center team is a perfect fit to implement your system and make these two centers cooperate and help your business grow and successfully perform providing your customers with the most high quality services.

Your customers will feel secure, happy and special

You choose to make your clients feel safe even in times of massive hacker attacks. We make sure you stay uncompromised and are ready to deliver service around the clock and make you customers feel secure, happy and special.

Email and SMS phishing, Mobile malware Ransomware, Insider threats, Internet of Things attacks - typically you should consider those types of threats and take constant care of them, they are most usual and only cyber security staff can take care of those types of intrusions, moreover - they happen mostly at the time any organization's staff in off work. These kinds of attacks might increase in frequency, they're difficult to defend and defeat, easy to misuse, might come out from disgruntled employees, misplaced or stolen employees devices.



SOC
(upper layer)

- 24x7 Incident detection and response
- Malware Analysis
- Network Behavior anomaly detection
- Intrusion and Breach Detection
- Log Management (SIEM)
- Insider threat and Data Leakage monitoring
- Vulnerability Detection & Awareness
- Incident Response
- Network Forensics

NOC
or Internal IT
(basic layer)

- Managing Network and IT systems
- Change management
- Firewall, IDS/IPS, Active Directory management
- Identity management
- Servers and Systems management
- Backup and Restore
- Antivirus management
- Patch management
- VPN access
- VoIP
- Applications

UnderDefense Incident Response

Incident Response Toolkit within UnderDefense SOC consists of 4 key do's:

PREPARE

Invite team members
Fine-tune response policies and procedures
Run simulations (firedrills / table tops)

ASSESS

Engage appropriate team members
Evaluate precursors and indicators
Track incidents, maintain logbook
Automatically prioritize activities based on criticality
Log evidence
Generate assessment summaries

REPORT

Generate reports for management, auditors
Document results
Conduct post-mortem
Update policies and procedures
Track evidence
Evaluate historical performance

MANAGE

Generate real-time IR plan
Coordinate team response
Choose appropriate containment strategy
Isolate and remediate cause
Instruct evidence gathering and handling

Your clients data leakage is something you can't allow to happen - and that's where we come in. Situations like this need immediate actions and UnderDefense Incident Response Plan within our SOC is responsible for the prevention of such threats and anomalies. Such actions can't be performed automatically by some sort of device but they have to be led by a human to fully understand the cause, analyze and identify gaps and close them to prevent it in the future.

We are not Competitors

but a Supplement to your existing team

UnderDefense Security Extension
Our SOC is designed to serve your organization as a remote extension of your security staff.

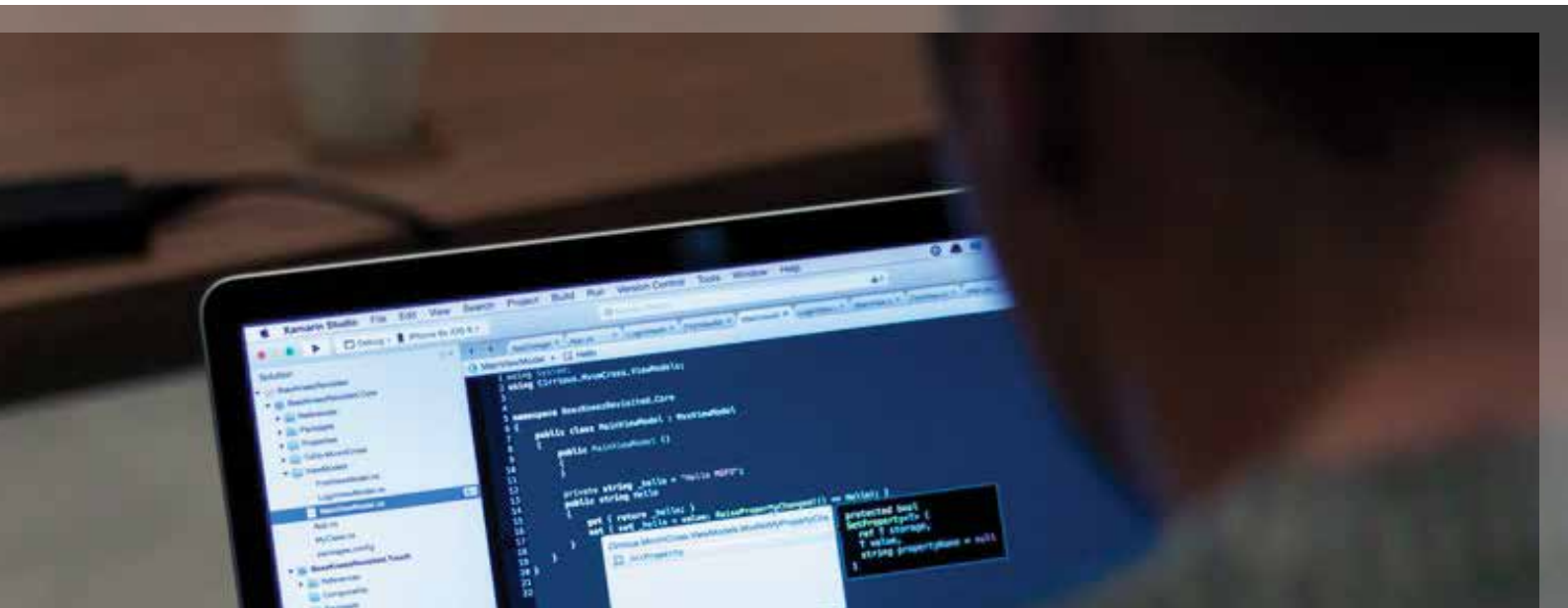
UnderDefense SOC team will allow your Security and IT do more interesting and important stuff like trainings, education, Forensics, Certifications, Red Teaming, Completing Compliance.
Our SOC team serves as a force multiplier for your existing staff, allowing you to focus on core business needs.

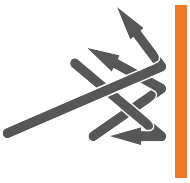
For operations across the world, UnderDefense systems, solutions and people are engaged in delivering security monitoring, Endpoint Security, email encryption and secure mobile platform, keeping the business, brand and reputation safe & sound.

Our clients are delighted to have an ability to rely on us and our vast experience to deliver flawless, innovative IT services.

We are not here to replace someone's staff or already existing teams but to supplement you with the much needed services to make your business more successful and to help it grow faster but fully secured.

Motivated hackers don't compromise your network with the same old threat - they always come up with new things to break the system down - because that is their constant fun game they play and make money by stealing them from you. Because your time - is money, to be exact - their money. While you're wasting time on looking for the right solution when the attacker has already been inside - they're getting richer every minute. Smart businesses don't look for the solution to prevent the catastrophe by fact - they have done it in the past and now are safe developing the business, reaching heights and sleep with the peace in mind while our Security Operations Center experts monitor the network and solve every littlebig thing that occurs along the way.





UNDER DEFENSE

CyberSecurity Solutions

Protecting your business

We at UnderDefense are dedicated to supporting organizations around the world in planning, building, managing, and running successful security operations programs, meeting and maintaining compliancy regulations and exceeding organizations abilities to run their businesses securely and confidently.

Our team of talented and professional cyber security experts partner with enterprise-class organizations to provide a full package of Cyber Security services and solutions including Security Assessments, Compliance Solutions, Product Advisory Services, Threat and Vulnerability management, Incident Response management, Network and Security architecture and implementation, and much more.

We don't just do; we think, innovate, and create new security capabilities to combat tomorrow's threats today.

Version 2 | 版一

www.version-2.com

Hong Kong | Taiwan | Singapore | Macau | Mainland China

Hong Kong & Macau
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

Taiwan
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

Singapore, Malaysia & SEA
Tel : (65) 6296 4268
Email : sales@version-2.com.sg