UnderDefense

39
Security engineers

28
Publications

19
Certified experts

4
Products launched for our clients

Certifications

Ph.D. in Security

UNDER DEFENSE

Recognitions, Awards & Partnerships

Technologies

We work with tools you already have and turn them into security powerguns:

If you are still in a looking-for-the-best SIEM mode, we can advise/provide a customized solution. Our analysts provide specific recommendations based on data from your environment and past trends.

splunk> partner+

UnderDefense is Splunk partner and our team is holding the following Splunk certifications:

- Splunk Certified Consultant I
- Splunk Administrator
- Splunk Power User
- Splunk Sales engineer 1
- Splunk User
- Splunk Sales Rep 1
- Splunk Sales Rep 2
- Splunk Sales IT & App
- Splunk UBA User

UnderDefense is also a developer of Splunk apps and plugins like:

- App for Eset Remote Administrator | Splunkbase
- TA for Eset Remote Administrator | Splunkbase

TAERA APPERA

UNDER DEFENSE

Security Monitoring packages

Our Security Monitoring is customized for the needs of each company. There are three basic models of cooperation:

Build SOC for you

When you decided to build a SOC with your local team, and need support to select, plan, implement and configure SIEM/IR tools for your team and setup appropriate process. We consult you on most optimized solutions needed for your specific case, maintain your SIEM, building new correlation for your deployment

Co-managed SIEM/MDR

When you already have or plan to buy a SIEM but you want to get answers and ROI from your investment but you can't hire security team or security team don't want to work during night shift, so you need to extend your security team with UD engineers to configure, maintain and monitor

Remote SOC team

When you have own CIRT team in-house and require our analysts for monitoring and notifications only. In this case, we can work in your own environment or use our AWS cloud deploy Splunk to monitor incidents and notify CSIRT team. You will receive reports of findings and be on constant communication with the security team

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Service components

Basic Fully managed service include: AWS deployed and manages Splunk, 8x5 Security monitoring team Tier 1-3 with 20 minutes SLA for critical alerts with notification, reporting and IR guidance.

Following componenets included:

Incident Management and reporting

- Security logs monitoring methodology
- Real-time incident handling
- Trend analysis

Development and adaptation

- Changes to log sources and formats
- Changes in search criteria
- Create reports and dashboards
- Create and change alarm structures

Operations

- NOC/SOC-delivery
- Service monitoring
- SLA
- SIEM management

Compliance reporting

- Compliances reports
- Deviation reports

UNDER DEFENSE

Benefits of Co-Managed SIEM

Move Beyond Alerts to Improve Risk Awareness

- Co-Managed SIEM provides you with risk awareness beyond alerts; you will quickly receive incident investigation and risk validation.

Accelerate Analysis, Containment and Response

- Reduce the amount of time it takes to respond to known and unknown threat activity by leveraging. We prioritized threat response engine.

Expand Your Team and Lower Costs

- Reduce the need to build your own team of SIEM engineers and threat analysts by leveraging. We are your virtual team 24x7x365.

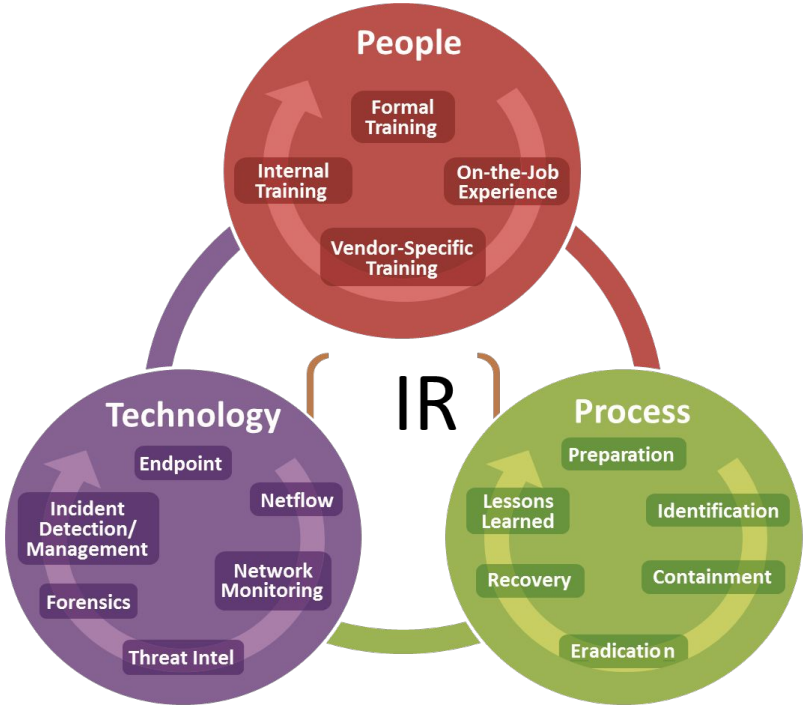
Shift to Intelligence Driven Operation

- Your current cyber security strategy is enhanced by our Global Threat Intelligence Center tools and resources.

UNDER DEFENSE

Accelerated Response with co-managed SIEM

- Move Beyond Alerts to Improve Risk Awareness
- Effectively managing and monitoring your SIEM technology requires an intricate balance of **people, processes** and **technology**. This challenging task is made even more difficult with an increasing volume of threats across an expanding attack surface, evolving compliance demands, talent shortages and tight budgets.
- We provide you with access to SIEM experts **24x7x365** to increase your ability to find and respond to threats in your environment.



UNDER DEFENSE

SOC for SMB / Enterprise

- Avoid capital expenses – it's ready to use. Cloud based Amazon AWS Co-Managed Splunk Enterprise Security SIEM infrastructure
- Predictable, ongoing fixed cost
- Very scalable & flexible, you pay as you go
- Huge ROI and quick, tangible and visible results
- Access to security expertise which is difficult to find and hire
- Expertise in SecOps and SIEM tools
- 8X5, 12,5 OR 24x7 security monitoring, incident detection and response
- Service Level Agreement (SLA)
- You define the SCOPE for MSS/SOC
- You own everything, if you decide to terminate a contract – everything continues to operate

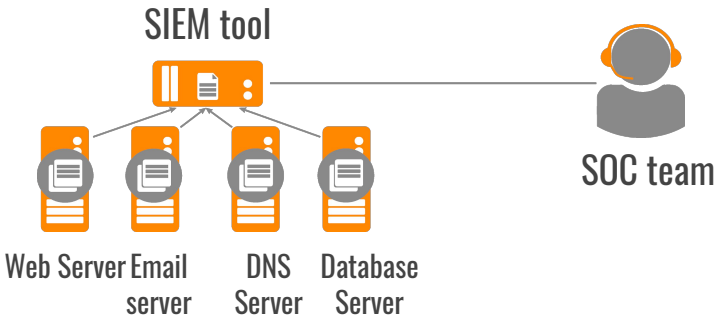
UNDER DEFENSE


SECURITY MONITORING

Processes: how it works

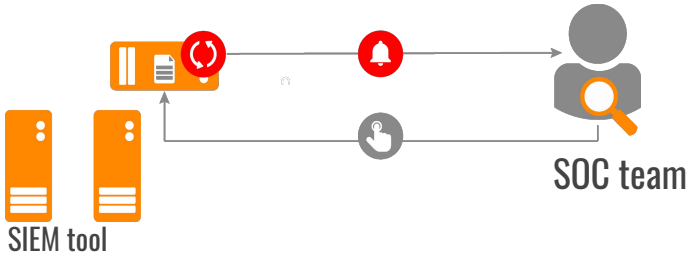
Stage 1 - Configuration phase

The SIEM is installed and logs are collected from log sources



Stage 2 - Monitoring phase

They are analysed using SIEM alert system due to their urgency

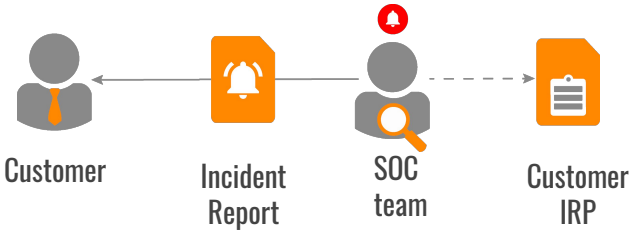


We take care of:

- Deployment and Data analytics
- Correlation rules updates
- SIEM Configuration and maintenance
- Orchestration infrastructure

Stage 3 - Incident Response

Security Analysts negotiate with customer IR plan and provide the Incident Reporting

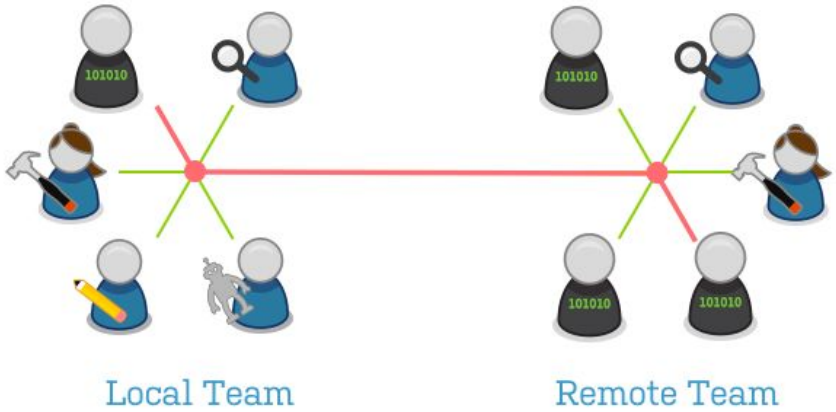


UNDER DEFENSE

SOC for existing IT Security Team

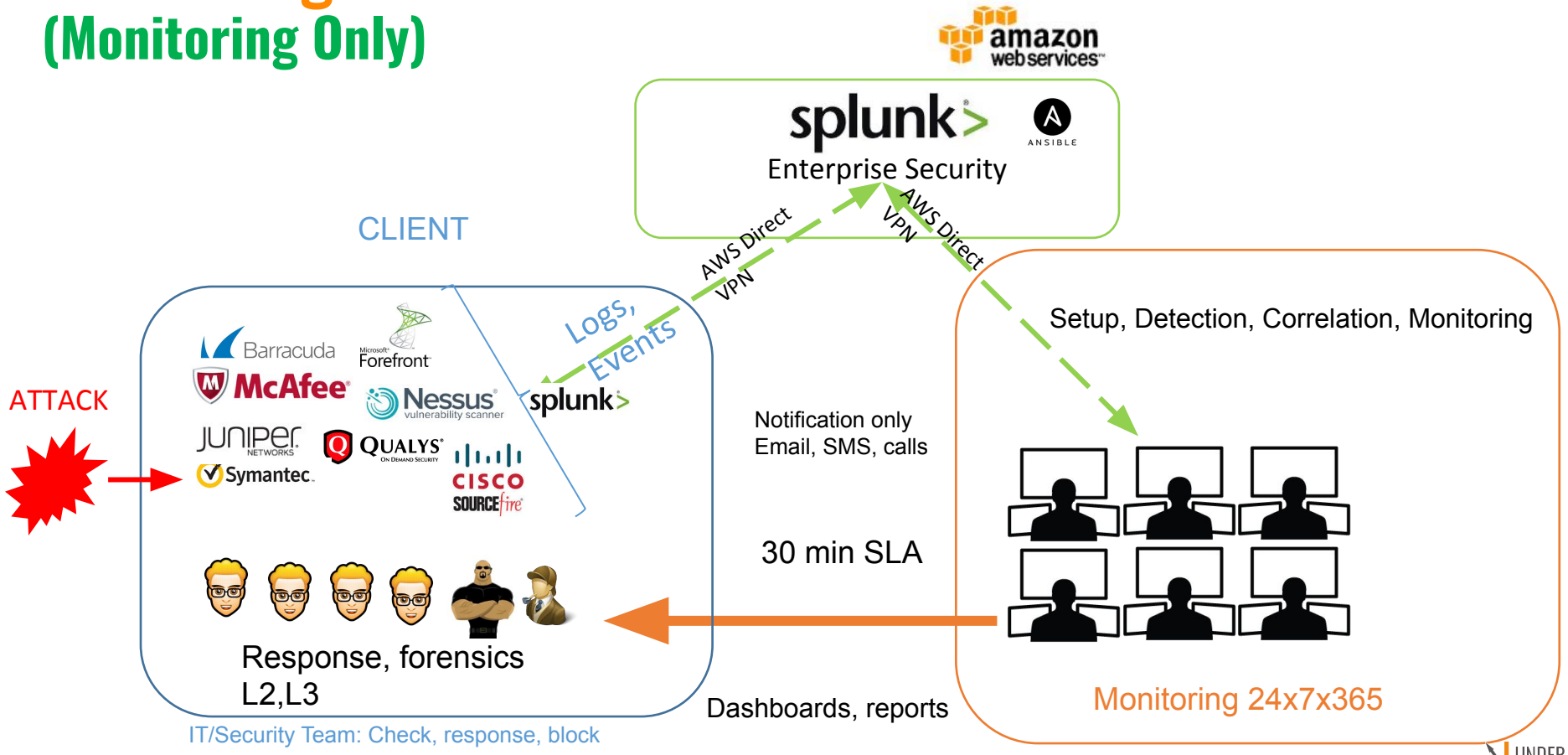
- Our Managed Security Services & SOC are designed to serve as a remote extension of your security staff
- Our cost and location model are optimized to reduce costs, increase efficiency, provide 24x7x365 coverage from multiple locations

- Our team serves supplements your staff allowing you to focus on core business needs. Allow your Security and IT to do more value added services like:
  - Red Teaming / Offensive Security
  - Education
  - Trainings
  - Certifications
  - Forensics
  - Completing compliance

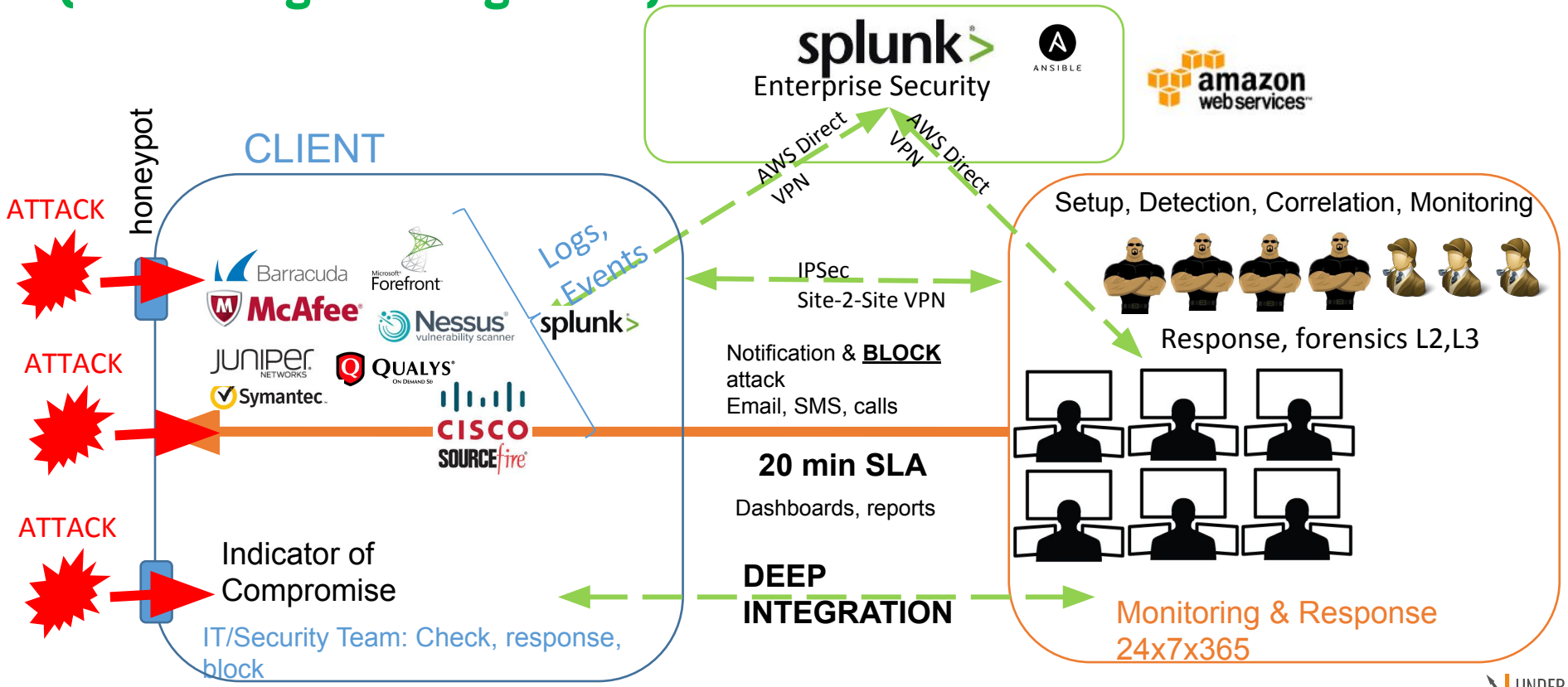


UNDER DEFENSE

Co-Managed SOC for SMB
(Monitoring Only)



Co-Managed SOC for SMB
(Monitoring & Management)



UNDER DEFENSE

PREPARE

Improve Organizational Readiness

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

REPORT

Document Results & Improve Performance

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

ASSESS

Identify and Evaluate Incidents

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

MANAGE

Contain, Eradicate, and Recover

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

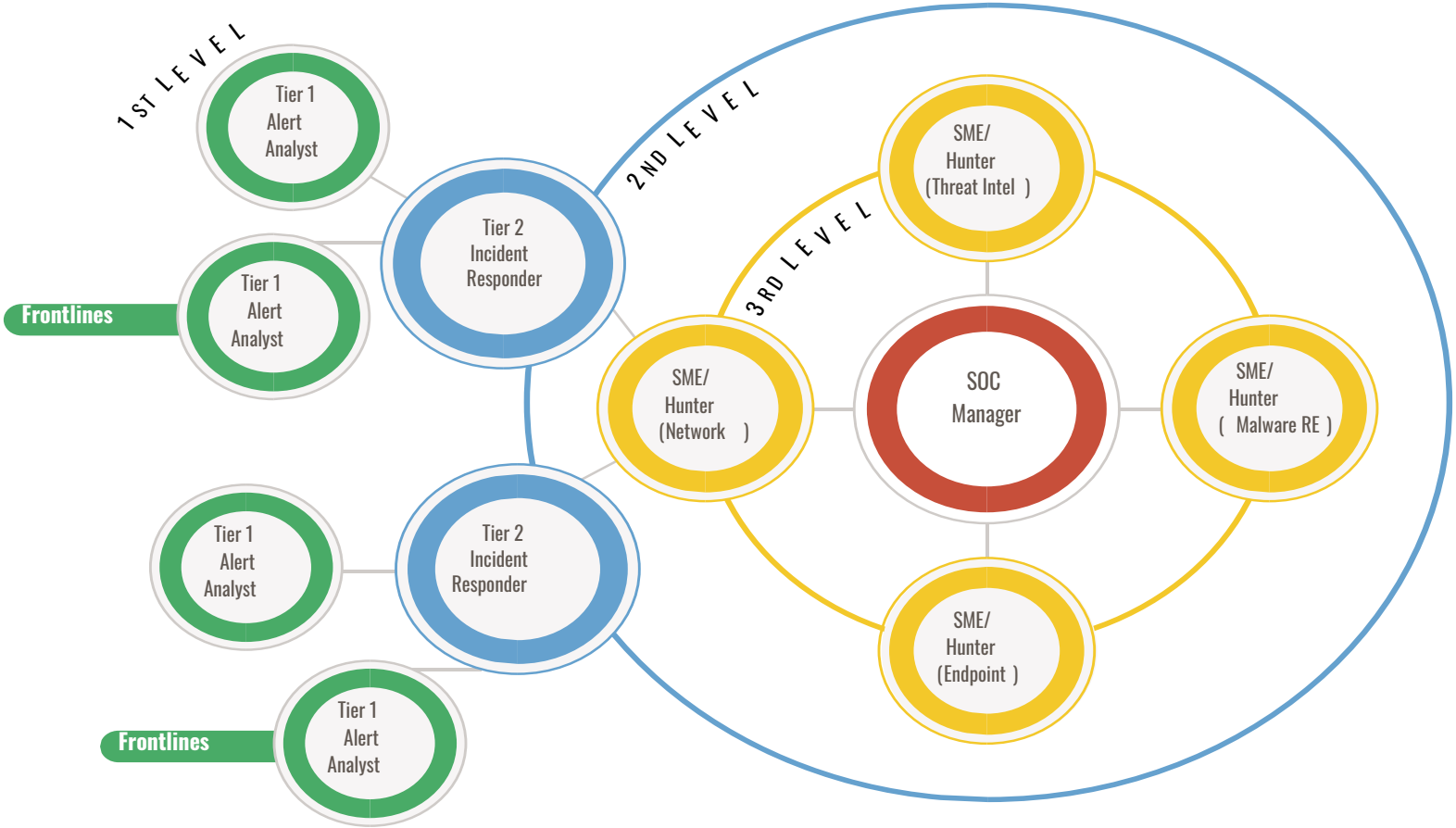
UNDER DEFENSE

Case study

UNDER DEFENSE

Building and running Splunk based SOC for client with 2TB logs per day

UnderDefense SOC organization



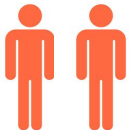
UNDER DEFENSE

Hybrid Team Model to cover additional 8x5 or 12x5 or fully 24x7 monitoring

SOC Director

- Track performance and Value
- Ultimately responsible for constituency mission
- Focused on full scope of cybersecurity
- Review weekly teams results & compliance reports
- Cyber news: Collection & Analysis
- Team coordination

UnderDefense



Tier 1: Monitoring

- Analysis of Alerts
- Call Center
- Real Time monitoring & triage
- Detect anomalies
- 20 min SLA before transferring to Tier 2
- Close False Positive

Tier 2: Detection & Threat hunting

- Incident Analysis
- Connect the dots of disparate activity
- Correlation Searches and Alerts Improvement

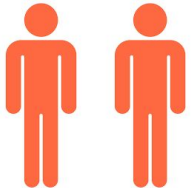
Tier 3: Remote Forensics

- Forensic
- Insider threat case support

Splunk Admin Lead

- SOC Infrastructure
- Job Inspection
- Scripting & Automation
- Tool engineering & connection to SIEM
- Agent tuning & maintenance
- Cluster monitoring & maintenance

Escalate



Client CSIRT
Tier 3: Incident Responder

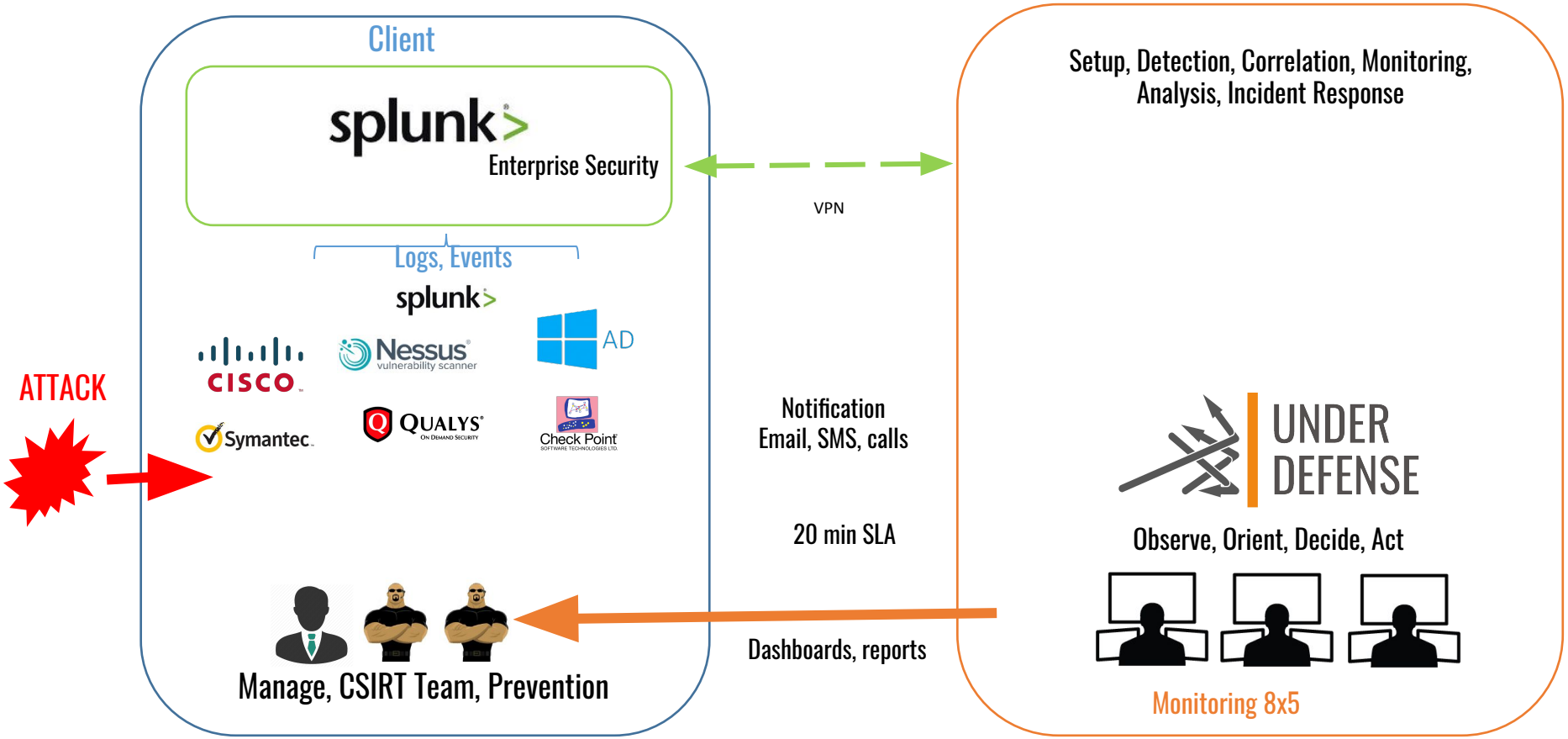
- Incident Coordination & Response
- Remote/ Local forensic analysis
- Forensic artifacts handling & analysis
- Emergency alerts & warnings
- Cyber Situational Awareness
- Prevention

RED TEAM TESTING

- Vulnerability scanning & Assessment
- Product Security Assessment
- Security Consulting
- Social Engineering

UNDER DEFENSE

Co-Managed SOC (hybrid) with on-prem SIEM on client side



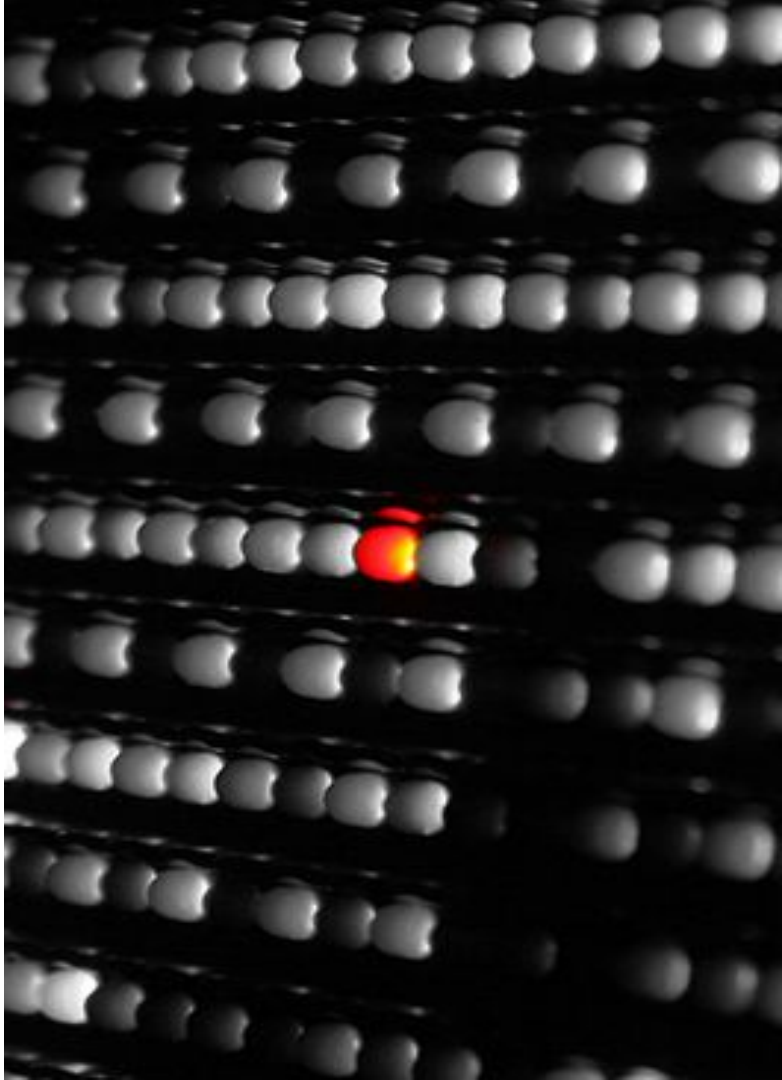
SOC Team Roles

Job Title	Duties
Tier 1 Alert Analyst	Continuously monitors the alert queue; triages security alerts; monitors health of security sensors and endpoints; collects data and context necessary to initiate Tier 2 work.
Tier 2 Incident Responder/ Threat Hunters	Performs deep-dive incident analysis by correlating data from various sources; determines if a critical system or data set has been impacted; advises on remediation; provides support for new analytic methods for detecting threats.
Tier 3 Subject Matter Expert/ Hunters	Possesses in-depth knowledge on network, endpoint, threat intelligence, forensics and malware reverse engineering, as well as the functioning of specific applications or underlying IT infrastructure; acts as an incident "hunter," not waiting for escalated incidents; closely involved in developing, tuning and implementing threat detection analytics.
SOC Manager	Manages resources to include personnel, budget, shift scheduling and technology strategy to meet SLAs; communicates with management; serves as organizational point person for business-critical incidents; provides overall direction for the SOC and input to the overall security strategy.

UNDER DEFENSE

Technical Challenge

2240 devices, 518 servers,1722 agents
Splunk Enterprise **2TB/day** 31 subnets,
Splunk Enterprise Security **500GB/day** index
PCI DSS compliant network



Client - Online Gaming and Gambling Platform

Industry:

Online Gambling Provider

Client overview:

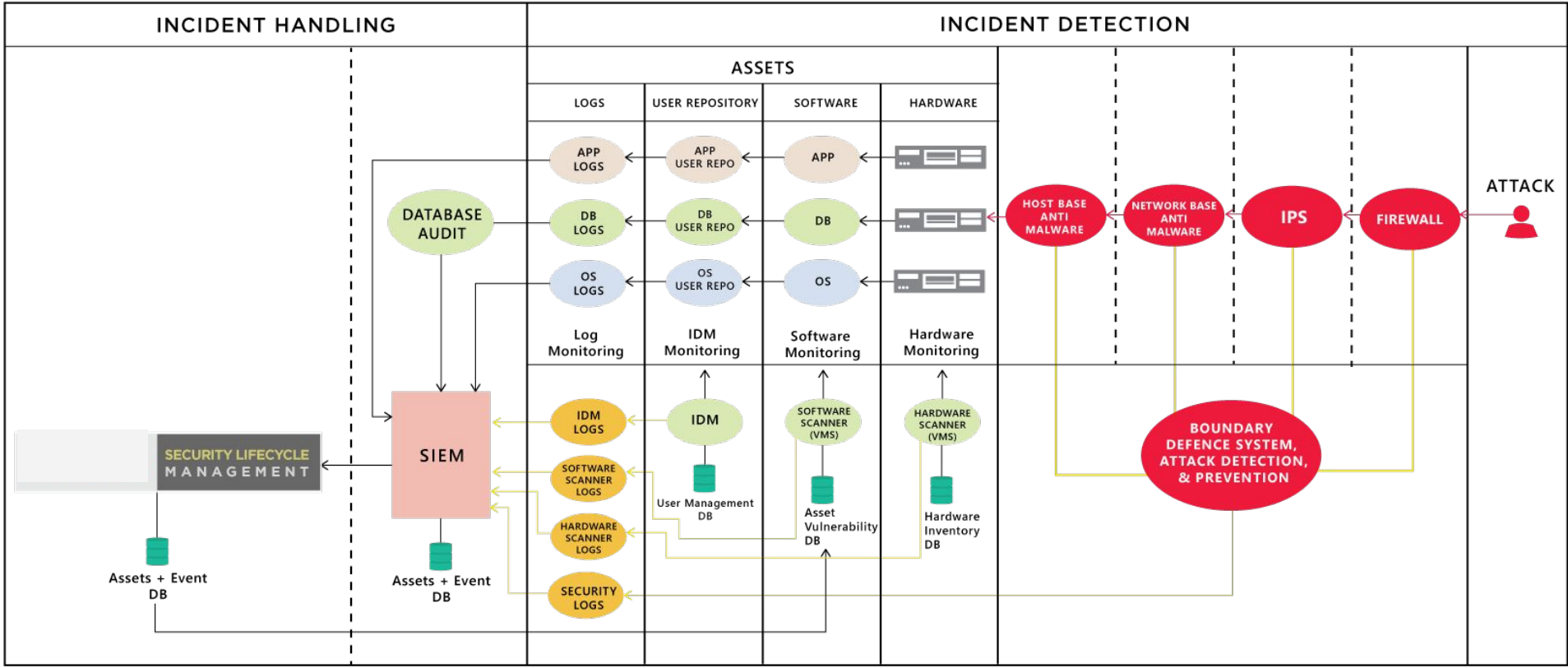
Swedish public company that offers a number of online gambling products, such as casino, poker, bingo, sports betting and scratch cards through more than 200 online gaming brands.

Technical

2240 devices, 518 servers,1722
Splunk Enterprise **2TB/day** 31
Splunk Enterprise Security **500GB/day**
PCI DSS compliant network

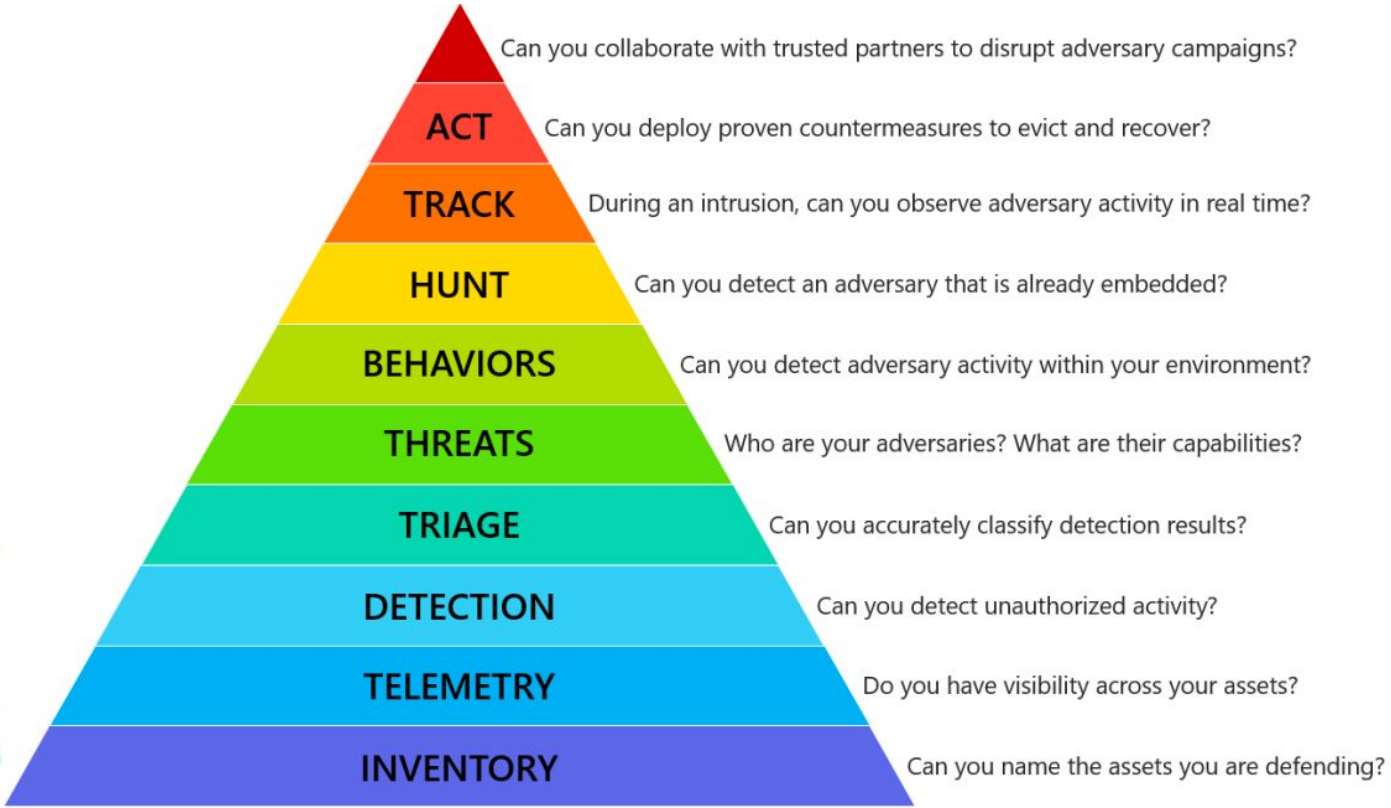
UNDER DEFENSE

Architecture

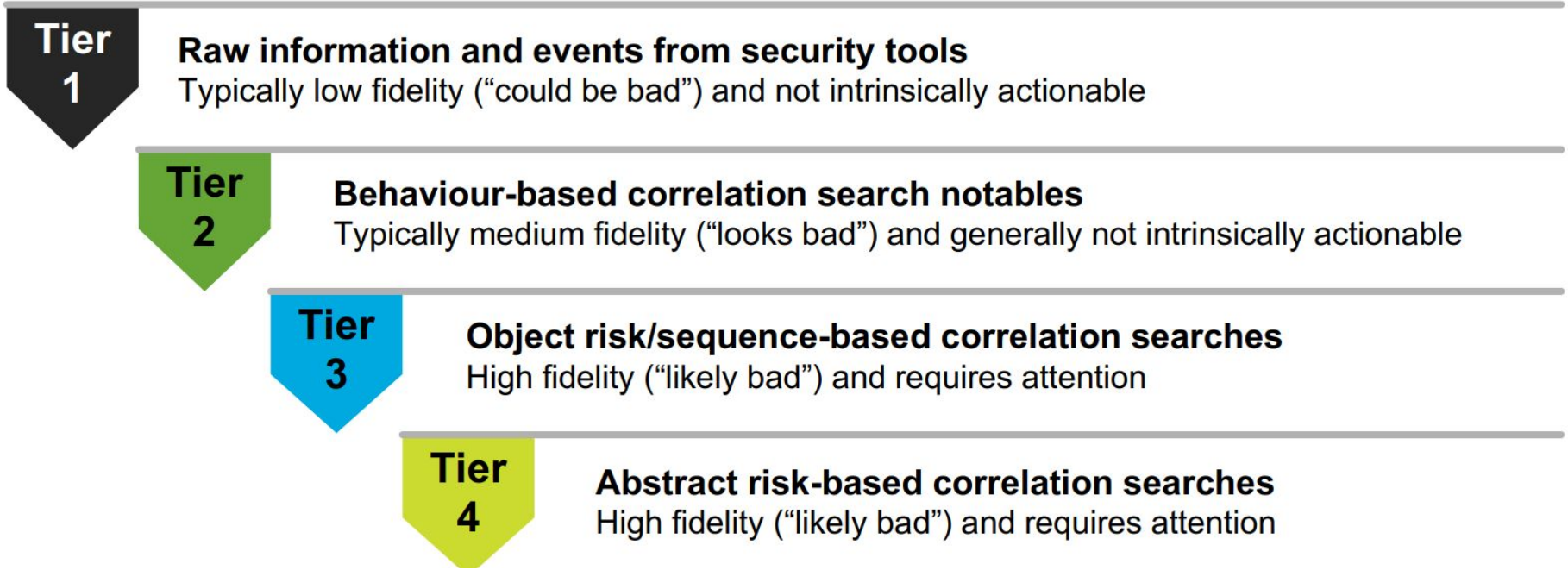


UNDER DEFENSE

Security Pyramid



UNDER DEFENSE



UNDER DEFENSE

Basic use cases monitored

- Reverse Shell on machine
- Monitor Vulnerabilities on machines
- Threat activity - connection to remote malicious ip
- Powershell Code Execution
- Ransomware behavior detection
- Privileged Account used
- Cleared logs on workstation
- File share scanning
- Service AutoRun monitoring
- Fake Windows Processes
- Malicious Command Line Executions
- Ransomware Note Files
- SMB traffic Allowed
- Spike in SMB traffic
- Brute Force attack
- Successful and unsuccessful Windows Update
- Domain Object changed
- Access Control

UNDER DEFENSE

Implementation phases

1. Discovery/Preparation phase

The UnderDefense Account Manager contacted client to schedule a service orientation call. The goals of the call and further onsite visit:

- Introduction to the UnderDefense SOC People, Processes, and Technology
- Identify points of contact
- Define requirements for toolset deployment
- Identify devices on which to report
- Provide connectivity requirements for toolset communication
- Assess the client network and environment
- Review architecture documentation
- Perform risk assessment
- Inventory of all devices, employees, access permissions etc
- Assess severity levels for critical assets

UNDER DEFENSE

Implementation phases

2. Installation Workshop

After Service Orientation Call had been performed, client was contacted to schedule the installation of security monitoring solution. The goals of the installation call was:

- Install the data collector
- Install the central server (for on-premises deployments)
- Create customer access to the central server (for on-premises deployments)
- Test and validate toolset connectivity
- Integrate nodes to be monitored
- Transition to service deployment

Implementation phases

3. Service Deployment and Security Monitoring

Further deployment actions have performed by client's Service Delivery Manager and the UnderDefense Security Operations Center. The subsequent steps included:

- Develop customized correlation rules
- Dry run monitoring service for 1 month - filtering false positive, false negatives, intrusions etc. Review the status of the onboarding project plan
- Client IT team to identify the cyberthreats
- Validate contacts to receive alerts & reports
- Determine the Incident Response policies and processes
- Build out daily and monthly security reports
- Conduct internal operation readiness review
- Integration with defect tracking system like Jira etc.

UNDER DEFENSE

Implementation phases

4. Training and Integration

- Training for client IT/Security team about Splunk ES
- Testing Monitoring SLA
- Validating Incident Response Plan in action
- Updating IRP and Splunk correlation rules
- Dry run of cyber threats

UNDER DEFENSE

Results

By focusing on the basics, we supported our client in building and running an effective Security Operations Center that delivered organizational value through, strong governance that generated consistency, accountability and proper integration with other relevant areas of the organization. Thus allowing proper integration of technologies that provide insightful information to support decision making and effective response.

As the result, we created

163 correlation rules	**125** dashboards	**112** rules	**20** threat intel sources

with client oriented context

UNDER DEFENSE

Client - Telecom

Industry:

Telecommunications

Client overview:

A Telecommunications and Internet Technologies provider, established in early 2000. With a wide Service offering including fixed line and digital radio and satellite communications, as well as wideband Internet access, data transmission, and international transit of traffic.

UNDER DEFENSE

Project goals

Analyze Login Activity
Challenge:
Identify unusual user activity

Analyze Endpoint Activity
Challenge:
Identify the root cause of the infection

Analyze Network Events
Challenge:
Identify how an attacker entered your network

UNDER DEFENSE

Client info: problems encountered

Problem:

Given the nature of its service offering, national reach and large volume, high-profile customers, our client identified a problem it needed to solve in order to maintain and grow its business:

“How can it provide assurance to its users regarding the controls it implements to protect the privacy and confidentiality of users’ data as well as the security, availability, and processing integrity of the systems that generate their customers ability to connect to a global world”.

Use case:

Improving security in the way of continuous log management

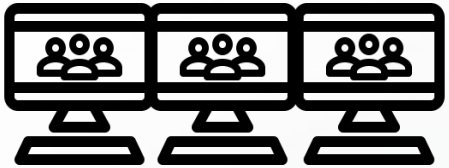
UNDER DEFENSE

Client info: business challenges

- Provisioning of a Security Operations Center (SOC) to detect, prevent and response for cyber attacks in a most cost effective way
- Improving maintenance of Network security parameters
- Improve Incident management and response

UNDER DEFENSE

Client info: Infrastructure



1400+ Windows based endpoints

100 + Linux based endpoints

600+ networking devices

UNDER DEFENSE

Why Splunk?

General causes

- Turn Machine Data Into Answers
- Conduct investigations
- Detect malicious actions and malware
- Detect ransomware source
- Reconstruct events
- Anomalies detection

Client's specific causes

- Improve organization security
- Do not repeat Petya security incident
- Get visibility on organization from security perspective
- Response to Incidents
- Understand root cause
- Log collection required by compliance

UNDER DEFENSE

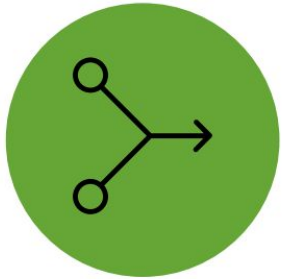
Security Features provided:

Threat Intelligence

Incident Management

Asset & Identity

Risk



Adaptive Response

Security & Compliance Reporting

Incident Investigations & Forensics

Monitor & Detect Known/Unknown Threats

Security Analytics

Insider Threat

Fraud Detection

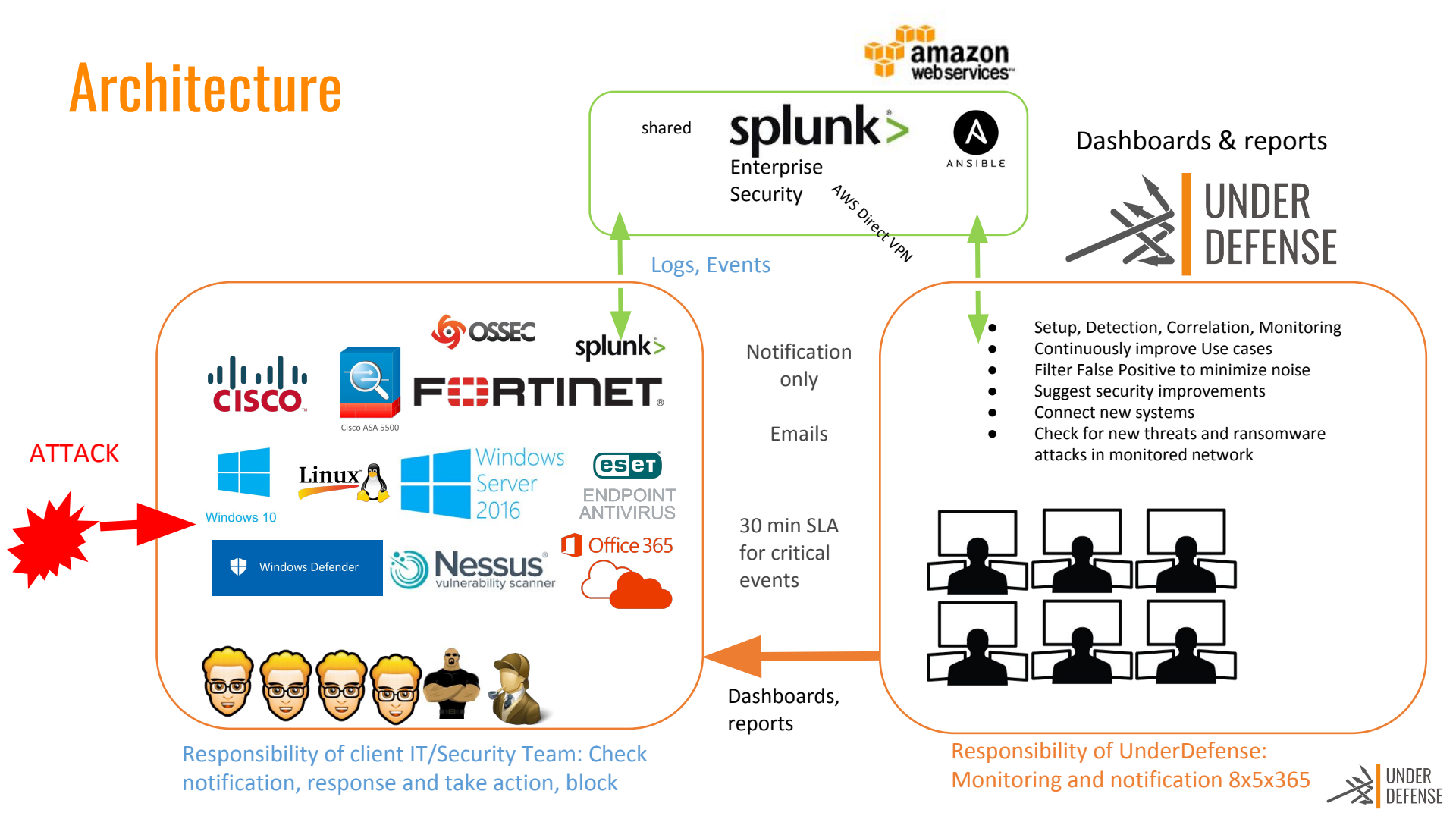
UNDER DEFENSE

Technology stack:

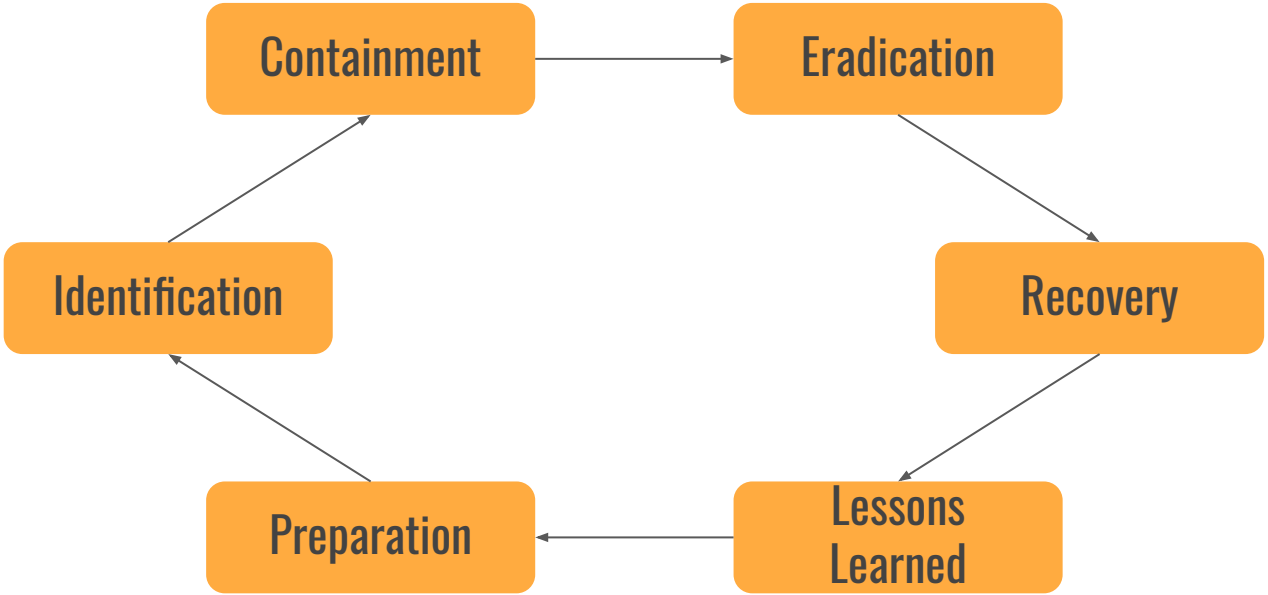
- In-house office environment (agent event gathering):
- Windows Event Log Collection
- Windows Defender Logs
- ESET antivirus logs collected
- Linux server's logs
- Network devices logs (Cisco ASA) + netflow
- PCI DSS compliant environment (agentless event gathering):
- Windows Event Collector
- ESET antivirus logs collected
- OSSEC logs
- Network devices logs(Cisco ASA) + netflow

UNDER DEFENSE

Architecture



Continuous Improvement Cycle



UNDER DEFENSE


SECURITY MONITORING

300+ correlation and triage searches in portfolio

Cloud

- AWS Cross Account Activity.
- AWS Cryptomoning.
- AWS Network ACL Activity
- Public S3 Bucket in AWS

Endpoint

- NotAVirus activity(rundll32, winRS, wmic, wevtutil, Fsutil. Net.exe, sc.exe)
- User/Group interaction(creation, changing, deletion)
- Process/Service monitoring(creation, modification, deletion, injection)
- Antivirus activity(Critical Host with Recurring Malware attack)

Threat Intelligence

- Reverse shell connection
- Connection to C&C server

Insider Threat

- Large Web Uploads
- Sources Sending a High Volume of DNS Traffic
- Activity from Expired User Identity
- User with Increase in Outgoing Email

ATP Detection

- Fake processes
- Registry keys Used for Persistence
- Malicious PowerShell Process with Obfuscation Techniques

UNDER DEFENSE

MITRE ATT&AK Correlations Implemented

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-hop Proxy
	PowerShell	Create Account	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	Disabling Security Tools	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Replication Through Removable Media	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process Injection	Extra Window Memory Injection	Two-Factor Authentication Interception	System Network Connections Discovery				Standard Application Layer Protocol
	Scripting	Hooking	SID-History Injection	File Deletion		System Owner/User Discovery				Standard Cryptographic Protocol
	Service Execution	Hypervisor	Scheduled Task	File System Logical Offsets		System Service Discovery				Standard Non-Application Layer Protocol
	Signed Binary Proxy Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories		System Time Discovery				Uncommonly Used Port
	Signed Script Proxy Execution	LSASS Driver	Valid Accounts	Image File Execution Options Injection						Web Service
	Third-party Software	Logon Scripts	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	Modify Existing Service		Indicator Removal from Tools						
	User Execution	Netsh Helper DLL		Indicator Removal on Host						
	Windows									

UNDER DEFENSE

Service Levels and Incident Notification

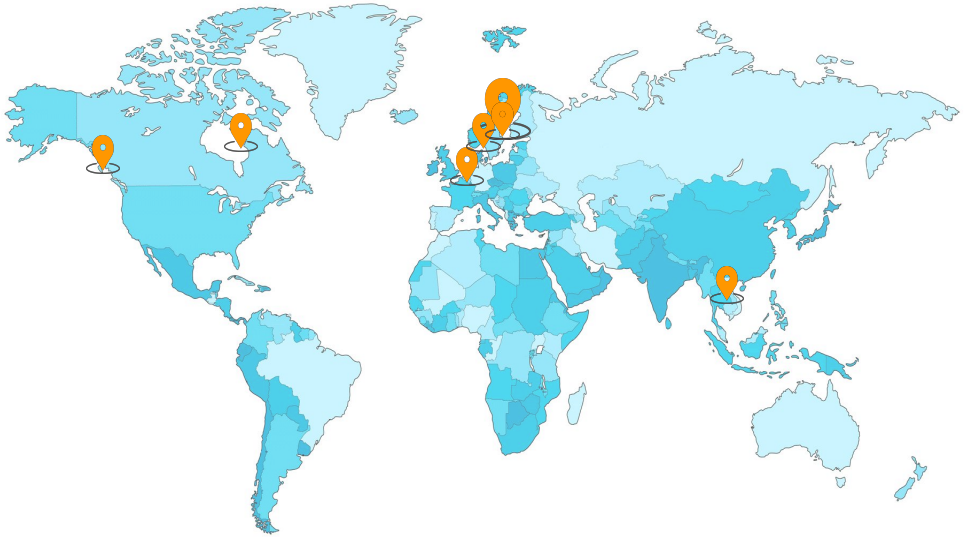
Severity	Action	Notification
P1 / Critical	Acknowledgment*	Within 15 minutes
	Response time**	Within 30 minutes
	Escalation to Manager	Within 2 hours
P2 / High	Acknowledgment	Within 30 minutes
	Response time	Within 1 hour
	Escalation to Manager	Within 4 hours
P3 / Medium	Acknowledgment	Within 3 hours
	Response time	Within 6 hours
	Escalation to Manager	Within 24 hours
P4 / Low	Acknowledgment	Within 8 hours
	Response time	Within 24 hours
	Escalation to Manager	As Required

*Acknowledgement is the time taken to deliver confirmation to the customer of ticket creation.
**Response time is the elapsed time from Acknowledgement to Confirmation that a SOC Analyst is investigating the issue.

UNDER DEFENSE

Our Locations

1. Lviv (Delivery)
2. Wroclaw (Delivery)
3. New York (Sales)
4. Malta (Sales)
5. Munich (Sales)
6. San Francisco (Sales)
7. Indonesia (Sales)
8. Vienna (Sales)



Lviv, Ukraine, Eastern Europe

Lviv is an acknowledged cultural capital of Western Ukraine and since the early 2000s, and has become one of the top IT hubs in Europe. The IT industry's annual growth rate in the city is averaging 20%, with currently employed workforce totaling 15 000+ specialists. The reason why Lviv's IT emerged so quickly is that there are two major Western Ukraine's universities as well as large amount of smaller colleges which produce 3 000+ IT graduates each year. City also stands out as a geographically favorable location, featuring 1-2 hr flight to the main European business centers such as Vienna, Zurich and Munich and 1 hour drive to Poland.

Few facts about IT in Lviv:

15000
professionals work in IT in Lviv

15%
Of Ukrainian IT people work in Lviv

+20%
predicted annual growth in the industry

60 1000
working population in Lviv are employed in ITi

UNDER DEFENSE


Thank you for your trust
Call us now at +1 929 999 5101