Case Study

National Telecommunications Provider
Security Operations Center

Industry:

Internet, Telecommunications, Cloud
Services, Data Centres, ISP/MSSP

Business Challenge:

- 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

IT Environment:

Hybrid Infrastructure without perimeter
Azure Cloud
Cisco based network stack
1400+ Windows based endpoints
600+ networking devices

Solution:

- Splunk ES as SIEM base for SOC
- Cloud based deployment, log storage and archiving with Amazon EC2,S3,EBS,Glacier services
- MITRE based SOC best practices with improved incident detection, response and forensics process
- 1 month dry run to decrease FP

Results:

- Full visibility of threats and anomalies within the organization
- Decreased incident detection & response time
- Trained and skilled SOC team

Background:

A National Telecommunications and Internet Technologies provider, established in early 2000. They hold the largest market share throughout the biggest East European country with significant backing and investment from the United States. With a wide Service offering including fixedline and digital radio and satellite communications, as well as wideband Internet access, data transmission, and international transit of traffic. They currently own and operate 90% of all fiber optical lines used by organizations throughout the Nation, with a broad customer base that includes corporate customers, financial institutions, hospitality organizations, telecommunications operators, and government organizations.

The Challenge:

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.

People, Process, & Technology:

Upon initiation we worked with our client to conduct a Gap Analysis as part of Discovery phase to better understand the current state of the security foundation and controls (CIS20) the organization already had in place. With our findings we were able to build out a customized road map for further improvements and cooperation with our client. Utilizing the following tools and methodologies we began to build SOC center for our client from scratch:

- Splunk used as SIEM with Enterprise Security, Anomaly detection, Behavioral analytics components
- Cisco and Checkpoint technologies
- HIDS
- Microsoft Windows Tech Stack
- Threat Intel
- Honeypots
- Cloud based log collection, storing, processing on Amazon AWS

With these we were able to work in tandem with the IT and Security team to set up Security Policies and improve on group policies within the Organization. Furthermore in conjunction with the internal IT team we worked to establish tailored rules for the SIEM and in all we set up:

63	112	125	20
correlation rules	rules	dashboards	threat intel sources

Upon completion of we conducted a 1 month discovery workshop with our client, in order to identify false positives and accurately set up security processes. We provided client with access to web based SIEM Console access, so it's security department was capable faster react on incidents, conduct investigations and manage SIEM independently after full testing and production deployment.
Finalizing our work we conducted personnel educational awareness trainings, IT Security team trainings and knowledge transfer, and helped them to improve incident response and forensics processes with full visibility on incidents and security events within the organization.

The Result:

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.

"UnderDefense helped us reduce time to investigation from weeks to hours or even minutes, allowing us to focus our time on key problems more effectively and limit time spent on false positives. With this we can confidently provide our customers with a guarantee that their businesses and data is secured 24/7."

CISO – National Telecommunications Group

About UnderDefense:

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.

USA, New York
375 Park Avenue, Suite 2800, NY
Tel: +1.929.999.5101
email: help@underdefense.com

Poland (EU), Wrocław
Rzeźnicza str. 28-31, 50-130
Tel:+48 792-229-273
email: help@underdefense.com

Ukraine, Lviv
Heroiv UPA 73 k.38, Lviv, 79014
Tel: +38 063-11-357-66
email: help@underdefense.com