encode
cyber threat management

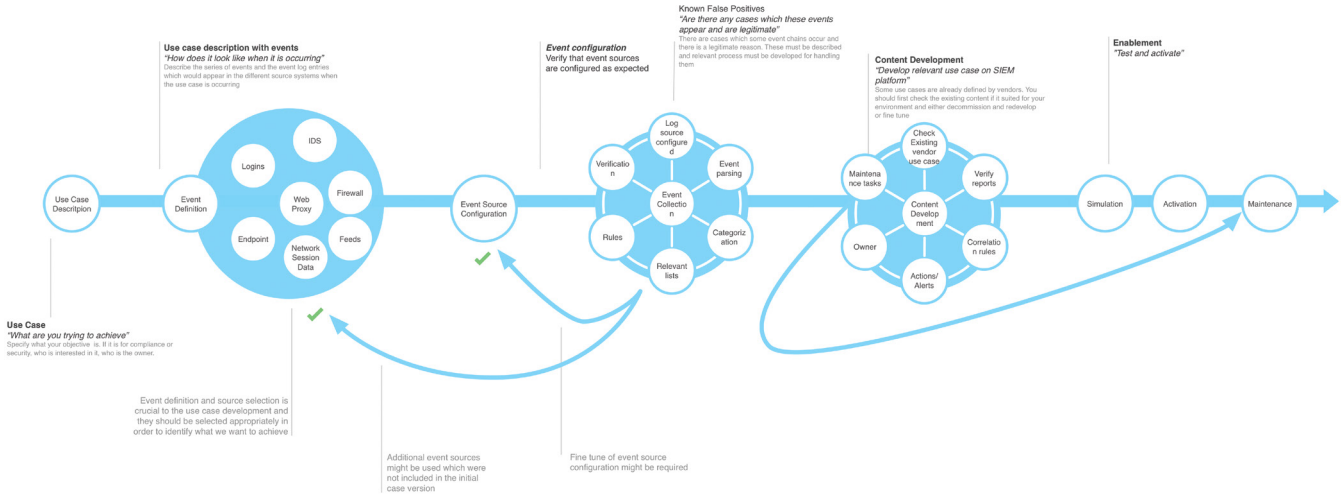
Whitepaper

Defending against sophisticated cyber attacks

Introduction

The growing sophistication of cyber-attacks makes the protection of an organization's assets a demanding and urgent task. Organizations need to advance their efforts to confront the wide range of cyber threats targeting their networks and systems on a daily basis. In this document, we introduce our approach and recommendations on how your organization should enhance its defense-in-depth strategy in order to defend against these types of attacks and help you minimise the threat risk. The main objective of this whitepaper is to list the main technical security controls that should be in place to strengthen your current security posture. However, we will not touch on the non-technical aspects (such as the need of a security awareness program) that are part of the high level security strategy. We present the role and capabilities of our Enorasys SIEM solution and we list the minimum event sources that is required to integrate to develop specific threat use cases. Lastly, we present the main features of our User Behavior Analytics solution called Enorasys Security Analytics and we describe the need for such a solution.

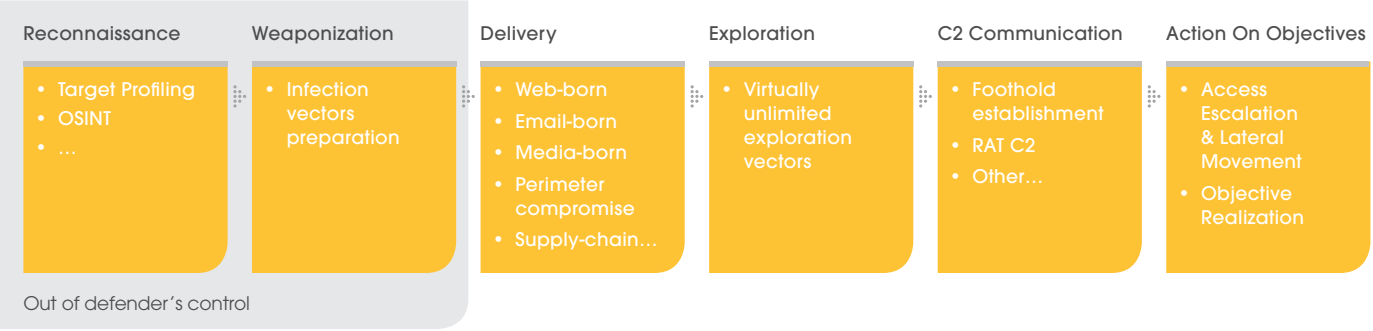
Organizations need to advance their efforts to confront the wide range of cyber threats targeting their networks and systems on a daily basis.



Defense-in-depth and Security Monitoring

When we are talking about defense we are implicitly referring to prevention, detection and response. In this document, we will focus on the prevention and detection phases of a defending strategy. The objective of this paragraph is, first of all, to list the security controls that can be utilized in order to address (prevent or/and detect) the steps of an attack per stage within the kill chain (Figure 1) and furthermore we clearly identify the log/event sources that are required by our SIEM solution so that we ensure an adequate level of coverage of our Use Cases framework.

Figure 1
Cyber Kill Chain



> When we are talking about defense we are implicitly referring to prevention, detection and response.

Let's take a closer look at the traditional as well as the next generation security solutions that can be deployed and examine the type of protection that can provide across all phases of an attack in the kill chain. We need to mention that this list (Table 1) is by no means exhaustive as far as we mainly focus on solutions that enhance the level of visibility (via logs) relevant to the 24x7 Security Monitoring services.

Table 1

Recommended security solutions for realizing your defense-in-depth strategy

Security Solution	Attack Phase	Main Features
Secure Email Gateway	Delivery Action on Objectives (Data exfiltration)	✓ Phishing protection ✓ Spam protection ✓ Malware protection ✓ DLP
Network Advanced Malware Detection	Delivery C2 Communication	✓ Behavior Analysis ✓ Sandboxing – Micro Virtualization ✓ Application Control
Next Generation Firewall (Egress)	Delivery C2 Communication Action on Objectives (Data exfiltration)	✓ Application visibility & control ✓ URL filtering ✓ Advanced malware protection ✓ User identity visibility & control ✓ Intrusion prevention ✓ DPI (& SSL Decryption) ✓ DLP
Secure Web Gateway	Delivery C2 Communication Action on Objectives (Data exfiltration)	✓ Malware protection ✓ (Sandboxing, File reputation File, File analysis, File retrospection, etc.) ✓ URL filtering and dynamic content analysis ✓ Application visibility and control ✓ DLP
Network Activity and Visibility	Delivery C2 Communication Action on Objectives	✓ Deep Packet/Content Inspection ✓ Network Session Recording and Analysis
Advanced Endpoint Defense • Endpoint Security systems (AV/HIPS) • Endpoint Visibility and Control • Application Control/White-listing • Exploit Prevention • Endpoint Hardening (SRP, EMET)	Delivery Exploitation C2 Communication Action on Objectives	✓ HIDS/HIPS ✓ FIM ✓ Malware protection ✓ Advanced security controls (Data Execution Prevention, Mandatory Address Space Layout Randomization, etc.) ✓ Enforcement of strict security policies (application control /whitelisting, device control, etc.) ✓ Endpoint Visibility and Control
DAM/DBF	Action on Objectives	✓ Monitor and audit all database activity ✓ Alert on policy violations ✓ Block based on security policies
WAF	Exploitation	✓ Block offending traffic ✓ Alert on security events and violations ✓ Web-shell detection
Network IPS/IDS	Exploitation Action on Objectives	✓ Monitor network traffic for malicious activity. ✓ Actively prevent/block intrusion. ✓ Alert on malicious packets.
Honeypots/Baits	Action on Objectives	✓ Attacker deception ✓ Detection
Privileged Identity Management	Action on Objectives (Privilege Elevation/Account Takeover)	✓ Control and audit administrative access

Our Managed Security Services are designed around a Use Case framework. Our Use Cases are designed in order to cover all main threat areas and corresponding attack scenarios. The ENCODE MSS Use Cases monitor events, utilize intelligence and evaluate context in order to detect security incidents and policy violations. Therefore, we can see that the quality and completeness of events is a critical factor for the effectiveness of our use cases deployment in our SIEM platform. To ensure that an adequate level of visibility and coverage of our Use Cases framework is achieved in the context of a monitored environment, a minimum set of event types and event sources is required. In the following table we list our requirements in event sources that should be integrated with SIEM. Moreover, we specify for which stage of an attack the corresponding logs are expected to provide visibility.

Table 2

Required event sources to integrate with our SIEM

Event Source	Event Type	Attack Stage
Domain Controller	• Domain Authentication events • Security and System events	• Enterprise Privilege Escalation • Local Privilege Escalation • Lateral Movement • Account Takeover
Windows Member Servers	• Security and System events	• Enterprise Privilege Escalation • Local Privilege Escalation • Lateral Movement • Account Takeover
Exchange Server	• Security and System events • IIS Access events (OWA) • SMTP logs	• Delivery • Lateral Movement • Account Takeover • Local privilege escalation
Secure Email Gateway	SEG alerts	• Delivery
Web Server	• Security and System events • Web Server Access events • Security and System events • File system audit logs or File access monitoring logs or File integrity monitoring logs	• Delivery • Exploitation • Lateral Movement • Local privilege escalation
WAF	• WAF alerts	• Delivery • Exploitation
Database Server	• Database standard audit events • Security and System events • File system audit logs or File access monitoring logs or File integrity monitoring logs	• Lateral Movement • Local privilege escalationw
DAM/DBF	• DAM/DBF alerts	• Lateral Movement

Table 2 Cont...

Required event sources to integrate with our SIEM

Event Source	Event Type	Attack Stage
Advanced Endpoint Solution	• Advanced Endpoint solution events/alerts	• Delivery • Exploitation • Lateral Movement • Internal Recon • Establish Persistence • Local privilege escalation • Stage & Exfiltration
Secure Web Gateway (plus external Threat Feeds)	• Access events	• Delivery • C2 Communication • Stage & Exfiltration
Next Generation Firewall (plus external Threat Feeds)	• Events and alerts	• Delivery • C2 Communication • Stage & Exfiltration • Lateral Movement • Internal Recon
Network IPS/IDS	• IDS/IPS alerts	• Delivery • Internal Recon
RAS	• RAS Authentication events	• Exploitation • Account Takeover

The role of MSS and Enorasys Security Analytics

After walking through our approach and suggestions on which technical security controls an organization should have in its arsenal and what are the expected logs to collect and monitor we should determine the role of the Managed Security Services and the underlying platform (Enorasys SIEM and Enorasys Security Analytics) within the organization's Incident Handling procedure. The objective of the MSS is to provide you with an early warning when an Indicator of Attack or an Indicator of Compromise is identified. The main objective of our service is to proactively pinpoint suspicious activity by "connecting the dots".

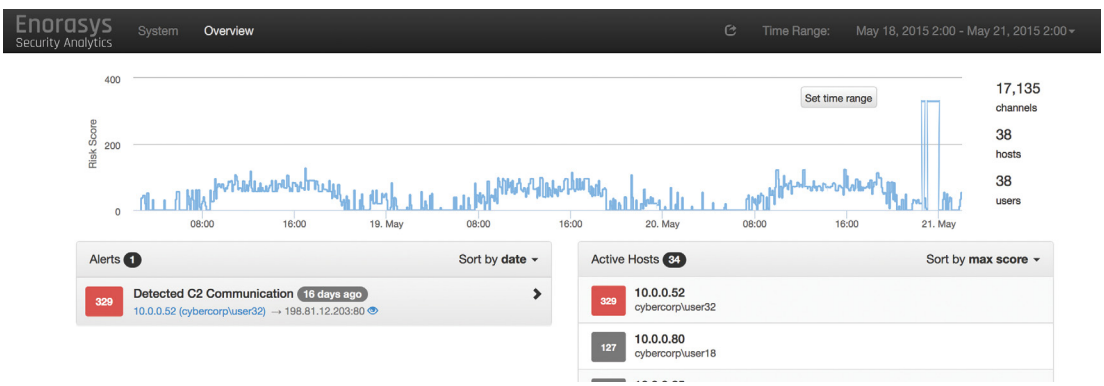
SIEM solutions, regardless of the vendor, have been designed in order to correlate in near real-time events based on a predefined set of rules applying on specific event categories. This is not fit for purpose when it comes to advanced threats. What is more, it is quite difficult to build the context of what is "normal activity" and what is not. Due to the way the correlation engine is designed a SIEM solution can detect only the "known knowns", provided that these have been configured as rules. So, we can see that a SIEM solution reaches its limit when it is exclusively fed with events from the applied security solutions and monitored devices as well as with threat intelligence feeds. When it comes to advanced cyber threats we can consider that infection is inevitable. The main challenge

of detecting such an attack is that the evasion and 'stealthy' techniques used by the attacker are so sophisticated following the attacker's dogma: "Be as close to 'normal' activity as possible". In this case, to accomplish early compromise detection we have designed and developed a leading security analytics solutions namely Enorasys Security Analytics.

Beyond SIEM

Enorasys Security Analytics is an advanced User Behavior Analytics solution designed from the ground up to deliver early compromise detection by understanding the "attack logic" and exploitation path of the advanced and determined adversary. This is realized through "focused" Big Data Security Analytics harnessing powerful machine-learning techniques and encapsulated offensive and defensive expertise. Enorasys Security Analytics comes with a set of pre-packaged security analytics modules, each providing continuous risk scoring of specific user and network node activities that have been designed and built with a focus on providing true early warning against targeted, evasive cyber-attacks, commonly known as "Advanced Persistent Threats" (APTs). The aim of this solution is to detect unknown C2 communication as early as possible. For more details on the Enorasys Security Analytics product please contact our Sales representatives.

In our MSS platform, Enorasys Security Analytics feeds Enorasys SIEM with alerts on high-risk activity and our SOC analysts run further investigation and analysis utilizing the events collected on both systems. In the context of our MSS services our Cyber Operations team use our Enorasys Security Analytics platform to proactively hunt for signs of sophisticated, targeted cyber-attacks as they unfold within our clients' environments. We call this process "Proactive Hunting", since we don't simply rely on monitoring and correlation of events to alerts, but rather our teams uses our Security Analytics system to proactively pinpoint suspicious activity, which when identified is surgically investigated and handled through our Response Orchestration system.



encode
cyber threat management

Encode UK
Level 33,
25 Canada Square,
London E145LB

encodegroup.com
+44 (0) 2070388305
info@encodegroup.com