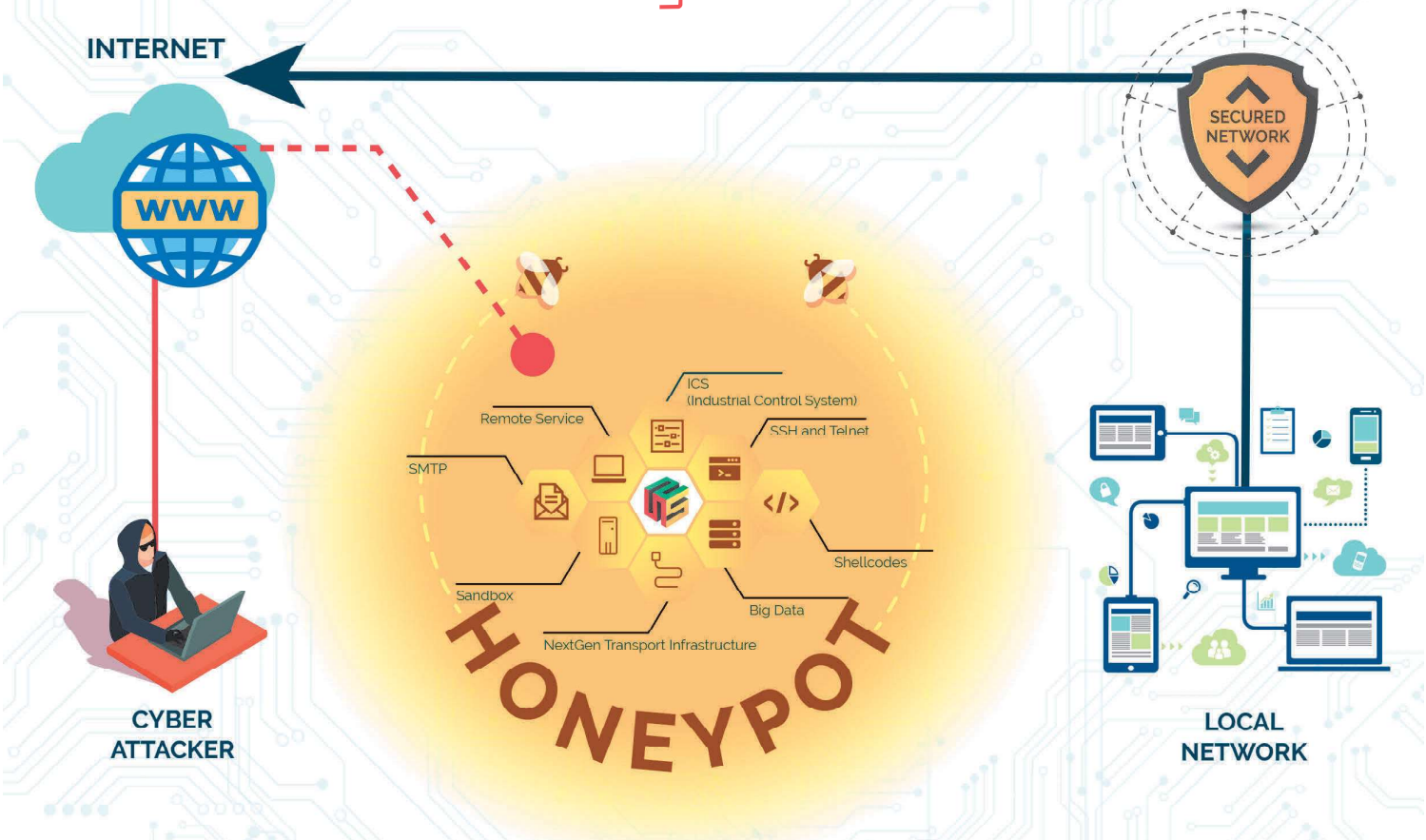
SENTINEL CYBER RESILIENCE and SECURITY SUITE with IPv6

Unified Threat Intelligence



The detection of unknown and advanced threats relies on the painstaking, hands-on efforts of security analysts, rather than automated rules or signature-based detection mechanisms. Threat hunting requires highly qualified and experienced professionals to trawl through huge volumes of data, identifying artefacts that the most sophisticated automated measures fail to detect.

Sentinel Unified Threat Intelligence provide rigorous protection against the most advanced current and even future threats to better protect themselves. Threat Intelligence services designed to mitigate these risks to ensure you're notified about the most dangerous Advanced Persistent Threats in time to take evasive action.

Sentinel Unified Threat Intelligence helping you understand whether you are currently under attack, how and by whom, how is it affecting your systems and what you can do about it. Threat intelligence derived from external trusted sources enables you to detect threats, preventing them before they can penetrate internal networks.

THREAT EXECUTIVE DASHBOARD

- Real-Time Monitoring
- Complete Security Visibility
- High Scalable
- Many IDS compatibility
- Multi-Engine Correlation
- Ease of Use

NIDS (NETWORK INTRUSION DETECTION AND PREVENTION SYSTEM)

- Vulnerabilities that allow a remote hacker to control or access sensitive data on a system.
- Misconfiguration (e.g. open mail relay, missing patches, etc.).
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.
- Denials of services againts the TCP/IP stack by using mlformed packets.
- Preparation for PCI DSS audits.

HBIDS (HOST-BASED INTRUSION DETECTION SYSTEM)

- Application Platform.
- Continuous second-by-second updates of dark intelligence from the global Norse Intelligence Network
- Deploys inline or out-of-band offloading expensive SIEMs and catching what you're missing now » Detects incoming and outgoing IP- and URLbased attacks

ICS (INDUSTRIAL CONTROL SYSTEM) HONEYPOT

Collect intelligence about the motives and methods of adversaries targeting industrial control systems

SMTP HONEYPOT

- Log full text emails attempted to be sent
- Logs credentials from logon attempts
- Logs everything
- Controlled Relay

REMOTE SERVICE HONEYPOT

- RDP Man In The Middle proxy which record session
- RDP Honeypot
- RDP screenshoter
- RDP client
- VNC client
- VNC screenshoter
- RSS Player
- Listens on a port and logs responses to a static VNC Authentication challenge

NEXTGEN TRANSPORT INFRASTRUCTURE HONEYPOT

Collect intelligence about the motives and methods of adversaries targeting next-generation transport infrastructure.

SSH AND TELNET HONEYPOT

- Fake filesystem with the ability to add/remove files.
- Possibility of adding fake file contents so the attacker can cat files such as /etc/passwd.
- Session logs stored in an UML Compatible format for easy replay with original timings
- Saves files downloaded with wget/curl or uploaded with SFTP and scp for later inspection
- SFTP and SCP support for file upload
- Support for SSH exec commands
- Logging of direct-tcp connection attempts (ssh proxying)
- Forward SMTP connections to SMTP Honeypot
- Logging in JSON format for easy processing in log management solutions
- Many, many additional commands

SHELLCODES HONEYPOT

- A Small Footprint
- Reliable Performance
- Enhanced Security
- Ecosystem Excellence
- A User-Friendly Experience
- Faster workload deployment
- Increased application performance
- Higher server availability
- Eliminated server sprawl and complexity

BIG DATA HONEYPOT

- New and modern IDS front-end
- The capability to have a full transcript of the network traffic
- Full Packet Capture adoption
- Helpful for network forensics
- Network Intrusion Detection
- Situational Awareness
- Offensive Reconnaissance
- Complete Security Visibility
- Highly Scalable
- Real-Time Monitoring

SANDBOX HONEYPOT

Use vulnerability type emulation instead of vulnerability emulation. Popular attack type emulation is already in place: Remote File Inclusion sandbox, Local File Inclusion providing files from a virtual file system and HTML injection via POST requests.

SENTINEL UNIFIED THREAT INTELLIGENCE ENFORCE USING IPV6