

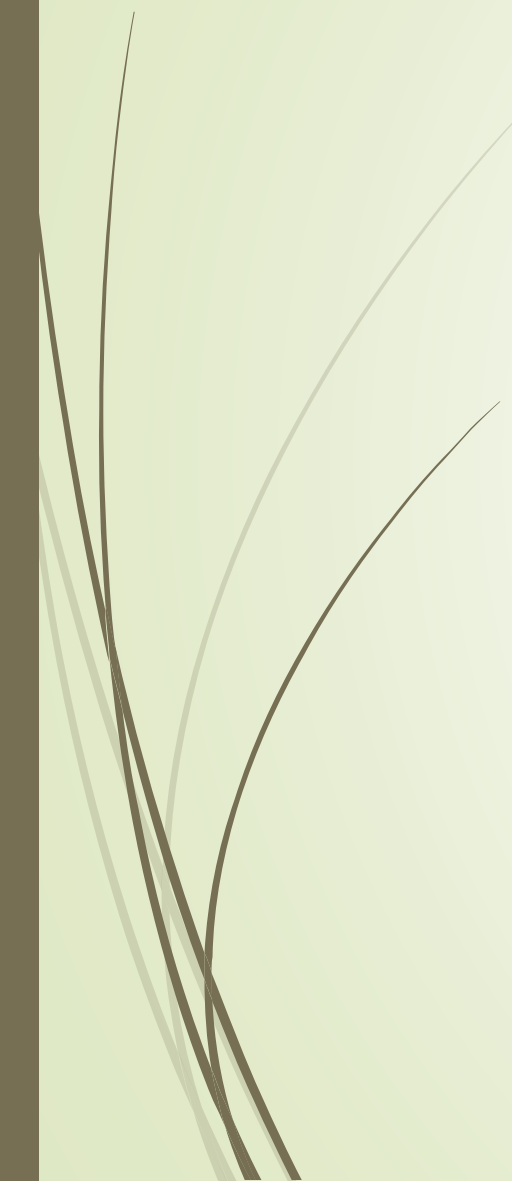


Discover and Defend Attacks on computers/networks

Joachim Mammale



Introduction

- Detecting threats
 - Network design
 - SIEM
 - Security Onion
 - Q&A-Session
- 



Introduction

3 words – how do they relate one to another?

- Threat
- Vulnerability
- Risk



Introduction

3 words – how do they relate one to another?

- Threat
- Vulnerability
- Risk

When threat and vulnerability exist together, a risk is present.



Detecting threats

- Signatures – valid but are not enough
- An IP-address that was 5 weeks ago malicious might now be legitimate
- Intelligence feeds can be outdated
- Example: If a threat actor compromises a major organization then IOCs (eg. IP addresses and domains used by the adversaries) are published so that you can block them in your environment or get them blocked automatically by the products you use (eg. Firewall)
- -> Adversaries read these reports, change their strategy and use other IPs
- IOCs get useless



Beaconing

- ▶ Definition:
 - ▶ Regular connections from an internal machine to an external destination
- ▶ Instead of relying on automated analysis (IPS signatures) also check connection persistency/beaconing
- ▶ If an endpoint is running malware the machine will regularly call home to a Command&control-server for instructions (eg. send list of files of the infected computer to C&C-server)



Detecting threats


- ▶ Question: How can traffic be analyzed?
- 



Detecting threats

- ▶ Question: How can traffic be analyzed?
- ▶ Screenshot of wireshark – removed in online version

Could you tell if this includes malicious traffic?




Zeek + RITA

- ▶ Zeek: Is not an active security device like a firewall but a tool that sits on a sensor and observes network traffic
- ▶ Interprets what it sees and creates transaction logs
- ▶ Eg. Splits up traffic into its different types
 - ▶ dns.log, http.log, ntp.log, dhcp.log, ftp.log
- ▶ RITA: Reads zeek logs
 - ▶ Detects signs of beacons in network traffic
 - ▶ Identifies long connections
 - ▶ Views user-agent strings
 - ▶ Checks for blacklisted domains and hosts

Zeek + RITA

UserAgent	Times Used
WicaAgent	1
Microsoft-CryptoApi/9.0	34
Microsoft-WNS/9.0	100
Microsoft-Delivery-Optimization/8.0	333
No JA3 hash generated	355
Mozilla/4.0	3500

Data adapted



Zeek + RITA

- ▶ Zeek can also detect which domains and subdomains were contacted (in numbers)
- ▶ Check for domains that are contacted only a few times or are suspicious/unknown and then investigate those further



Detecting threats

- ▶ Score-model: Start with 100 points
 - ▶ 80-100 is suspect
 - ▶ 0-30 is benign /legitimate
- ▶ Example: Every 5 minutes a server is communicating with an external domain
 - ▶ You see that it is NTP which is legitimate to send regular requests -> -30 points
 - ▶ You see that the domain belongs to Microsoft -> -20 points
 - ▶ You see that the domain of the certificate matches Microsoft -> -20 points

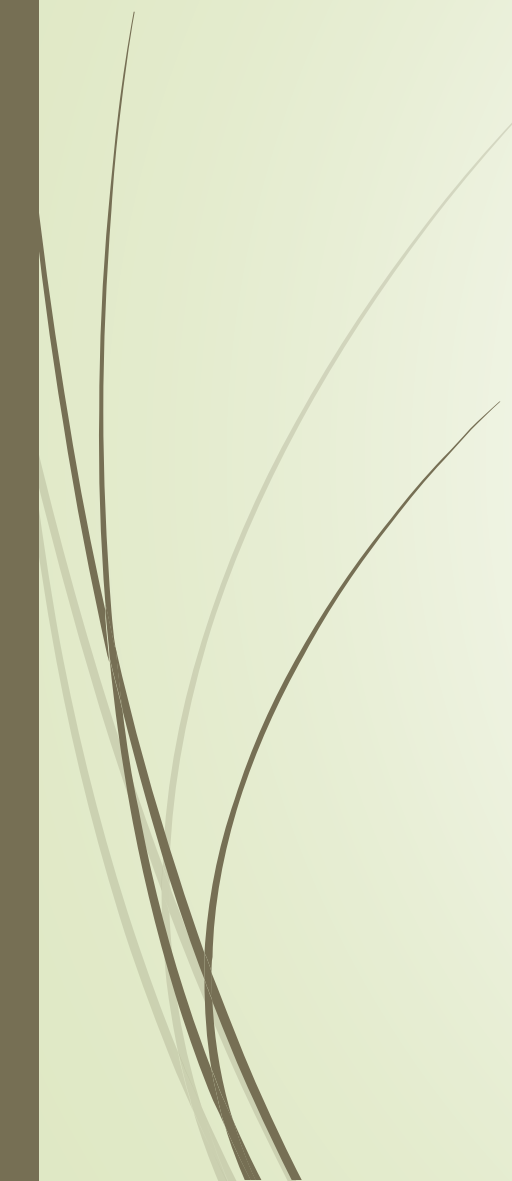


Questions until now?





Defending

- ▶ What can be done to defend against threats?
 - ▶ Let's limit for a moment to things that are placed inside of our network
 - ▶ Ideas?
- 



Defending

- Firewall (WAF, NextGen)
- IDS/IPS (Intrusion Detection/Prevention) Systems
- Proxy
- Zones
- VLANs



Firewall

- ▶ Inspects each packet passing through the firewall and accepts or rejects it based on defined rules
- ▶ Define default implicit deny-rule (everything that is unknown is blocked/rejected)
- ▶ Difference between block and reject
 - ▶ Block: silently drops a connection; (best for WAN-rules)
 - ▶ Reject: notifies the sender about the close rule; (best for LAN-rules)
- ▶ Decide based on source ip, destination ip, source port, destination port and protocol
- ▶ What happens if an attacker sends ssh-traffic over port 80?



Firewall

- NextGen Firewall
- Is able to analyze the traffic at the application layer

OSI-Model

#	Name	Elements	Protocol examples
1	Application	Gateway, Proxy	HTTP, SMTP
2	Presentation		WMV, JPEG, MOV
3	Session		Session management
4	Transport		TCP/UDP
5	Network	Router, Layer-3-Switches	IP
6	Data Link	Layer-2-Switches	MAC
7	Physical	Network cables, Repeater, Hub	1000BASE-T

How to remember the order: **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way



Firewall

- ▶ NextGen Firewall
- ▶ Is able to analyze the traffic at the application layer
- ▶ Inspect the actual content of a packet, not just its headers
 - ▶ Eg. Drop any peer-to-peer application packet
 - ▶ Prevent users from visiting a site
- ▶ Can be used not only to protect a network from hackers but also from unwanted traffic



IDS/IPS

- ▶ IDS (Intrusion Detection System)
 - ▶ Do not substitute firewalls
 - ▶ Support firewalls by adding a further layer of security protecting the network from well-known attack vectors
- ▶ NIDS (Network Intrusion Detection System)
 - ▶ Inspect the application payload to detect any potential attack
 - ▶ Example1: Detection of Mimikatz (extracts passwords from memory) payload
 - ▶ Example2: Detect violation of policy rules (eg. No android phones on internal networks but only on guest-network; no dropbox allowed in network)
 - ▶ Tools: Suricata



IDS/IPS

- ▶ HIDS (Host Intrusion Detection System)
 - ▶ Monitor application logs, file-system changes and changes to the operation system
 - ▶ Tools: Splunk, OSSEC
- ▶ IPS (Intrusion Preventing System)
 - ▶ As the name says: they do not only detect but also prevent



Proxy

- ▶ Acts as a middle man between a device and a remote server
- ▶ Caching proxy
 - ▶ Attempts to serve client requests by delivering content from itself without actually contacting the remote server
- ▶ Internet Content Server
 - ▶ Used in organizations to prevent users from accessing prohibited websites



VLANs (Virtual Local Area Network)

- ▶ Is a separate broadcast domain (logical separation) that is partitioned and isolated in a computer network
- ▶ Can be used to partition a network into segments, eg:
 - ▶ Production
 - ▶ Voice Over Ip
 - ▶ Network management
 - ▶ Guest Internet Access
 - ▶ Demilitarized Zone (DMZ, machines that have webservice facing the internet)



Zones

- Grouping of interfaces (eg VLANs and/or physical interfaces)
- When used with firewall rules, zones provide a convenient method of managing security and traffic for a group of interfaces



Zones

Public zone (ISP Transit, Guest Wifi, BYOD)

DMZ, Demilitarized Zone (FrontEnd-Server)

Service zone (DHCP/DNS-server, VPN-Endpoints)

Management zone (Switch/Router-management, Jump hosts)

Internal network (managed clients, VOIP, server, cameras, printers)

Zones

		Destination				
		Public zone	DMZ	Service zone	Management zone	Internal network
Source	Public zone (ISP Transit, Guest Wifi, BYOD)	X				
	DMZ (FrontEnd-Server)	X	X			
	Service zone (DHCP/DNS-server, VPN-Endpoints)			X		
	Management zone (Switch/Router-management, Jump hosts)		X	X	X	X
	Internal network (managed clients, VOIP, server, cameras, printers)		X	X		X

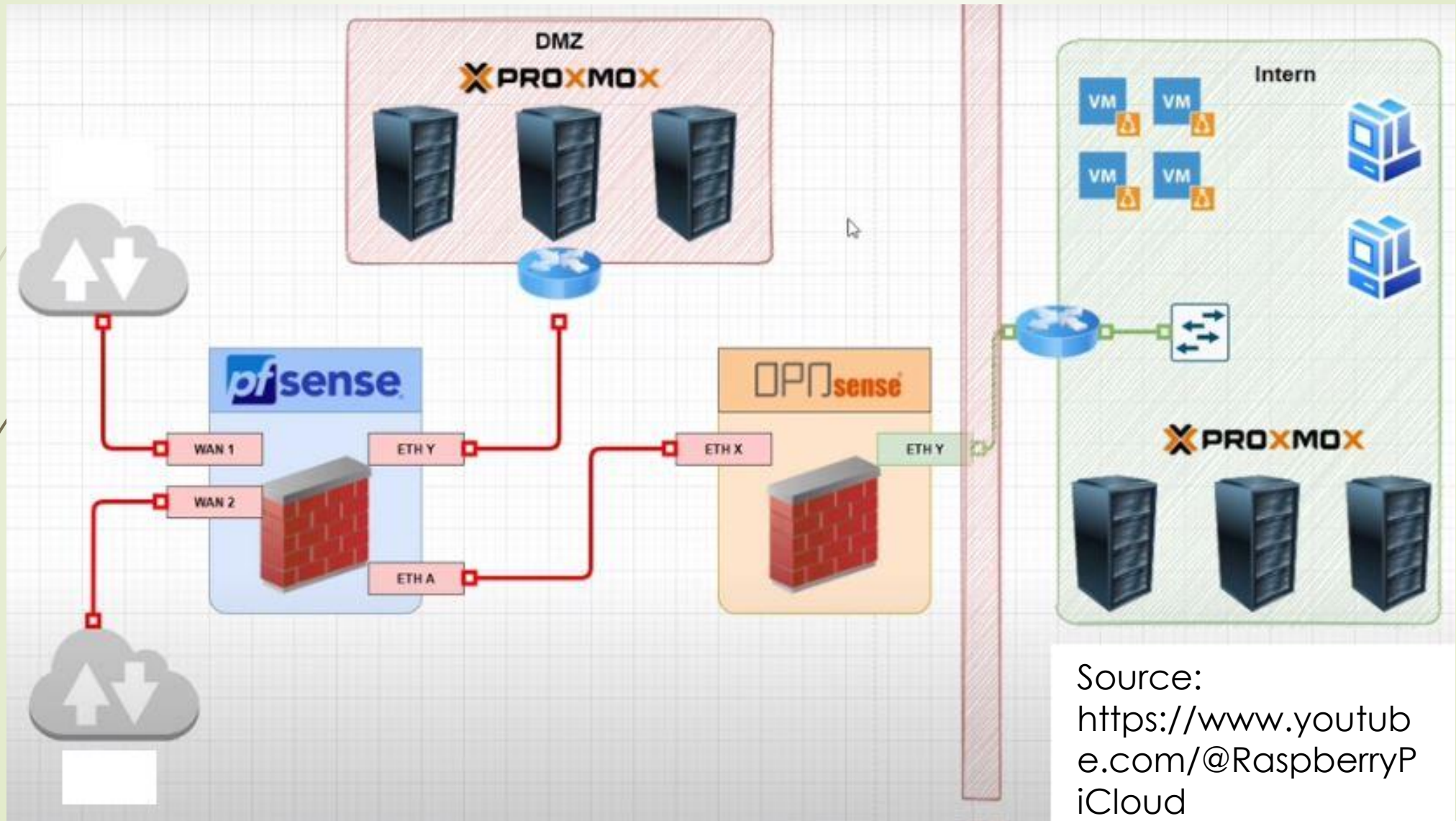
Source: Secnovum




Zones

- ▶ Having different zones allows logging traffic in transit between zones
- ▶ Can be compared with an airport: Inside zones (Checkin, Duty-free, boarding) there are no controls but when transiting between zones (customs or at the gate) controls are in place

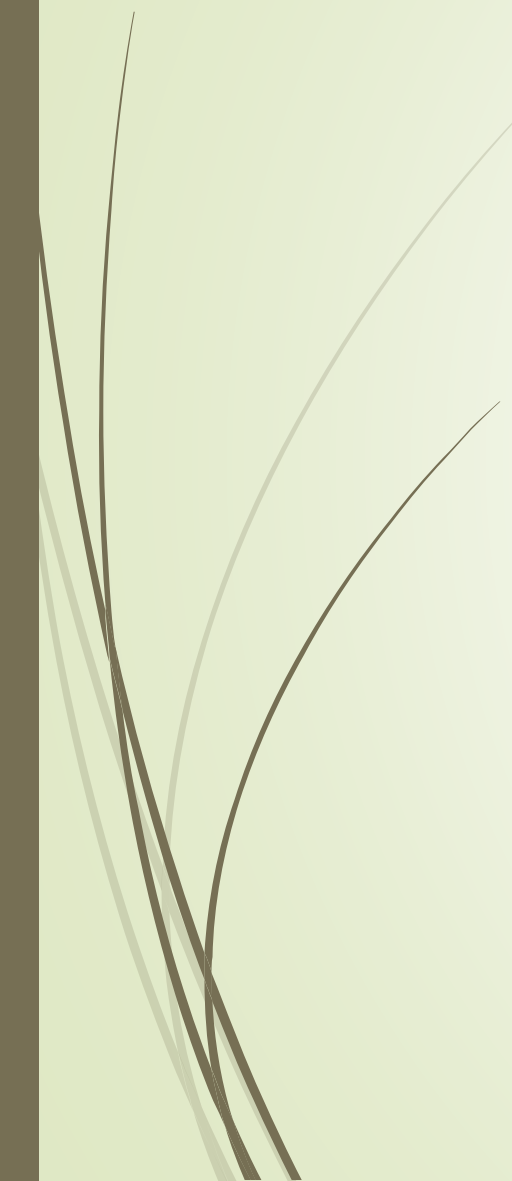
Network design overview



Source:
<https://www.youtube.com/@RaspberryPiCloud>



SIEM (Security Incident and Event Management)

- ▶ Detects, saves and indexes log files and other event data
 - ▶ Allows to get a centralized and merged view on data
 - ▶ Enables admins and analysts to analyze security incidents
- 

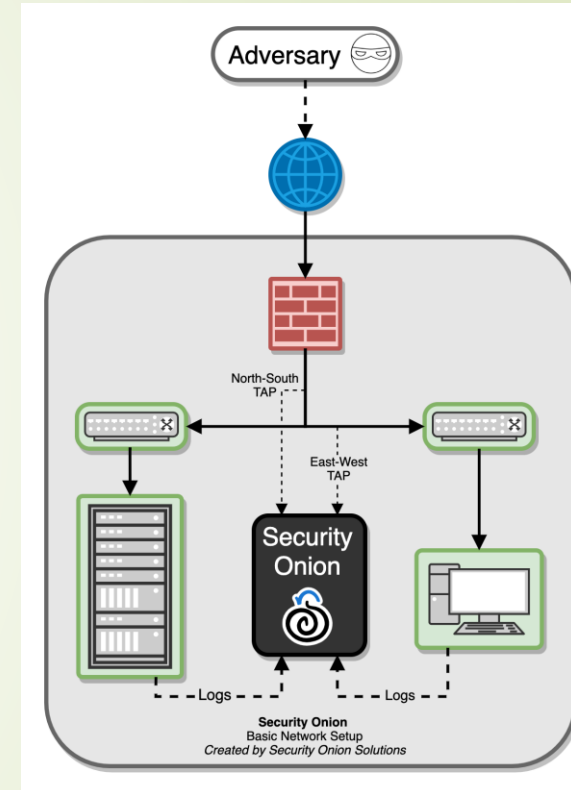


Security Onion

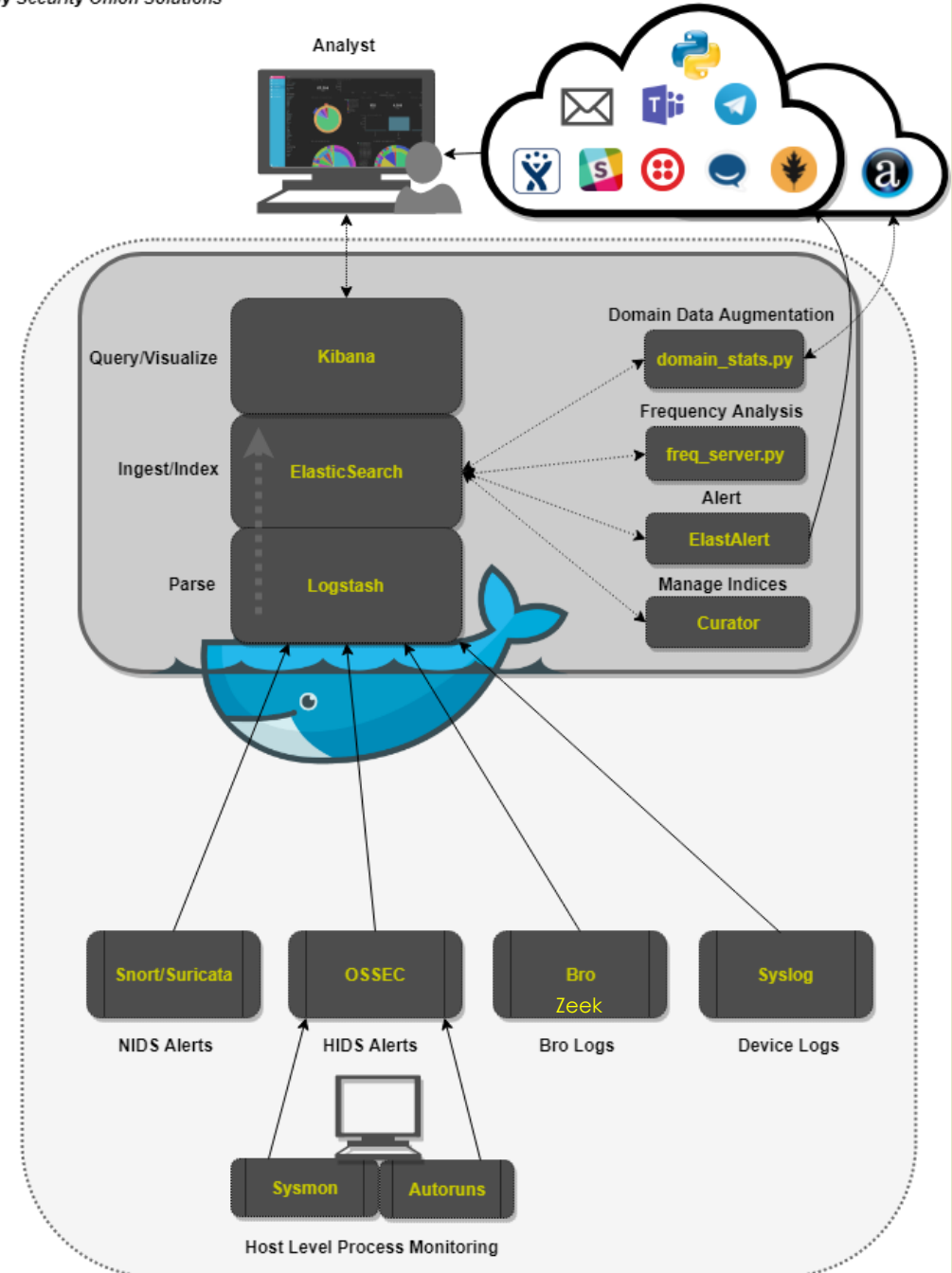
- ▶ free and open platform for Network Security Monitoring (NSM) and Enterprise Security Monitoring (ESM)
- ▶ NSM: monitors your network for security related events
 - ▶ Identify vulnerabilities or expiring SSL certificates
 - ▶ Incident response and network forensics
- ▶ ESM: includes endpoint visibility and other telemetry

Security Onion

- ▶ monitor north/south traffic to detect an adversary entering an environment, establishing command-and-control (C2) or data exfiltration and others
- ▶ monitor east/west traffic to detect lateral movement
- ▶ fill in blind spots with additional visibility in the form of endpoint telemetry
- ▶ consume logs from servers and workstations so that you can then hunt across all of your network and host logs at the same time.



Security Onion



- Overview
- Alerts
- Dashboards
- Hunt
- Cases
- PCAP
- Grid
- Downloads
- Administration

Tools

- Kibana
- CyberChef
- Navigator

Alerts

Options v

Total Found: 103

Q v Group By Name, Module



2021/06/30 00:00:00 AM - 2021/07/01 00:00:00

Choose the timespan to search, or click the calendar icon to switch to relative time

REFRESH

Fetch Limit

50

Filter Results

	Count	rule.name	event.module	event.severity_label
	59	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)	suricata	low
	4	ET MALWARE Trickbot Checkin Response	suricata	high
	4	ET POLICY HTTP traffic on port 443 (POST)	suricata	medium
	3	ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1	suricata	medium
	3	ET MALWARE VNCStartServer BOT Variant CnC Beacon	suricata	high
	3	ET MALWARE VNCStartServer USR Variant CnC Beacon	suricata	high
	3	ET POLICY PE EXE or DLL Windows file download HTTP	suricata	high
	2	ET HUNTING curl User-Agent to Dotted Quad	suricata	medium
	2	ET INFO Dotted Quad Host DLL Request	suricata	medium
	2	ET MALWARE Win32/Trickbot Data Exfiltration M2	suricata	high
	2	ET POLICY curl User-Agent Outbound	suricata	medium
	1	ET DNS Query to a *.top domain - Likely Hostile	suricata	medium
	1	ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010	suricata	high
	1	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	suricata	high
	1	ET HUNTING Suspicious POST with Common Windows Process Names - Possible Process List Exfiltration	suricata	high
	1	ET HUNTING Suspicious Windows Commands in POST Body (ipconfig)	suricata	medium
	1	ET HUNTING Suspicious Windows Commands in POST Body (net config)	suricata	medium
	1	ET HUNTING Suspicious Windows Commands in POST Body (net view)	suricata	medium
	1	ET HUNTING Suspicious Windows Commands in POST Body (nltest)	suricata	medium



Security Onion

- ▶ It's not enough to set up a solution and then walk away and let it work in its own
- ▶ Data can be collected and analyzed, but not all malicious activity looks malicious at first glance.
- ▶ Automation and correlation can enhance intelligence and assist in the process of sorting through false positives and malicious indicators
- ▶ But at the end it needs humans that monitor the solution
- ▶ Security Onion will provide visibility into your network traffic and context around alerts and anomalous events, but it requires a commitment from you the defender to review alerts, monitor the network activity, and most importantly, have a willingness, passion, and desire to learn.



Questions?

