SECURITY OPERATION CENTER

JOAS ANTONIO

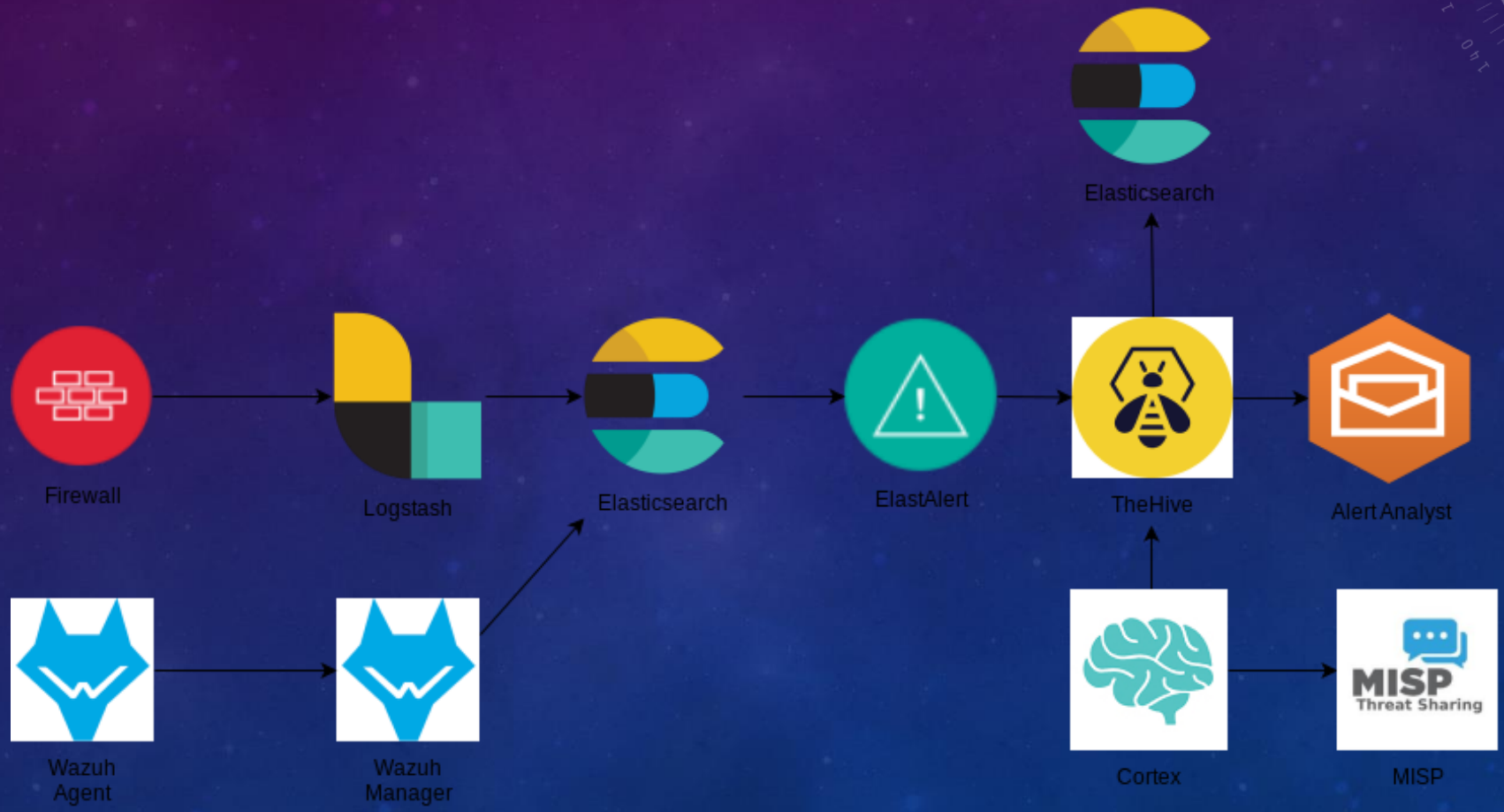
DETAILS

- Information about Open Source or Near Open Source SOC tools
- **LinkedIn**: https://www.linkedin.com/in/joas-antonio-dos-santos

SOC OPEN SOURCE TOOLS

- **IDS/IPS:** SNORT, SURICATA, ZEEK, OpenWIPS-ng, Sguil, OSSEC
- **Vulnerability Scanner:** OpenVas, Vega, OWASP-ZAP, Nikto, Tenable Community
- **Network Monitor:** Nagios, Cacti, Icinga2, Zabbix, Prometheus
- **Log Management:** NXLog, Graylog, Elasticsearch and Logstash, Fluentd, Flume, Octopussy, Logalyze, Logstalgia
- **Threat Detection and File Monitor:** Wazuh, osquery, Security Onion, Samhain
- **Endpoint Security:** OpenEDR, Wazuh, Comodo
- **Firewall:** Pfsense, Iptables, Ipfire, OPNSense, Smoothwall, NG Firewall
- **Threat Intelligence:** Maltego, MISSP, Virus Total, X-Force, Talos, VirusShare, Anyrun, Automated Indicator Sharing, Infragard, Mitre Att&ck
- **Adversary Emulation:** Infection Monkey, APT Simulator, Caldera, Red Canary
- **SIEM:** OSSIM, Splunk Trial, Elasticsearch, Sagan, Mozdef, Apache Metron
- **Ticket Services:** SpiceWorks, osTicket, SuiteCRM, Liberum
- **Incident Response:** Cynet 360, GRR Rapid Response, AlienVault, Cyphon, Volatility, Autopsy, XSOAR, CyberCPR, FTK Imager, Doorman, Mozdef, CimSweep, TheHive, SIFT
- **Malware Analysis:** Yara, GRR, Bro, Cuckoo Sandbox, Anyrun
- **WAF:** ModSecurity, Cloudflare, WebKnight

SOC OPEN SOURCE TOOLS



SOC 1 Project Management Approach Example

OBJECTIVES & TASKS

PLAN

OBJECTIVES

- Define and confirm “client” and any additional specific requirements
- Develop and set up a execution plan.

TASKS

- Setup an deliver training
- Deliver kick-off meeting with stakeholders
- Confirm control objectives and scope
- Confirm roles and responsibilities of the project team members
- Discuss and clarify project timing
- Confirm initial project tasks and set initial interview / meeting dates
- Distribute initial Documentation list

COMPREHEND

OBJECTIVES

- Execute risk assessment
- Identify relevant controls
- Collect relevant information
- Identify areas for dual purposed testing

TASKS

- Execute a risk analysis and analyse portfolio to identify and determine test strategy
- Review controls workbook to identify controls that can be tested once for leverage in multiple reports
- Gather and review documentation
- Document controls considered relevant to the in-scope environment and selected criteria
- Execute interviews with key stakeholders

TEST

OBJECTIVES

- Analyse information gathered and conduct testing
- Provide management with findings and recommendations
- Provide roadmap for remediation

TASKS

- Conduct management interviews
- Compile and analyse documentation to support testing requirements
- Identify gaps in the control environment
- Discuss any issues or gaps with management

REPORT

OBJECTIVES

- Provide and deliver reports to “client”

TASKS

- Prepare and submit final report
- Lessons learned
- Identify changes
- Execure close-out meeting

SOC – PEOPLE, TECHNOLOGY AND PROCESS