Security Operations & Dashboards

SOC as a (managed) Service in Microsoft Environments

Norbert Breidohr

23.07.2019

STIHL Worldwide

The STIHL Group on all 5 continents

- 38 own sales and marketing companies in Europe, Asia / Oceania, America and Africa, and 120 importers worldwide
- Represented in approximately 160 countries by more than 45,000 specialist retailers
- Production sites in Germany, the USA, Brazil, Switzerland, Austria, China, Philippines

Starting point

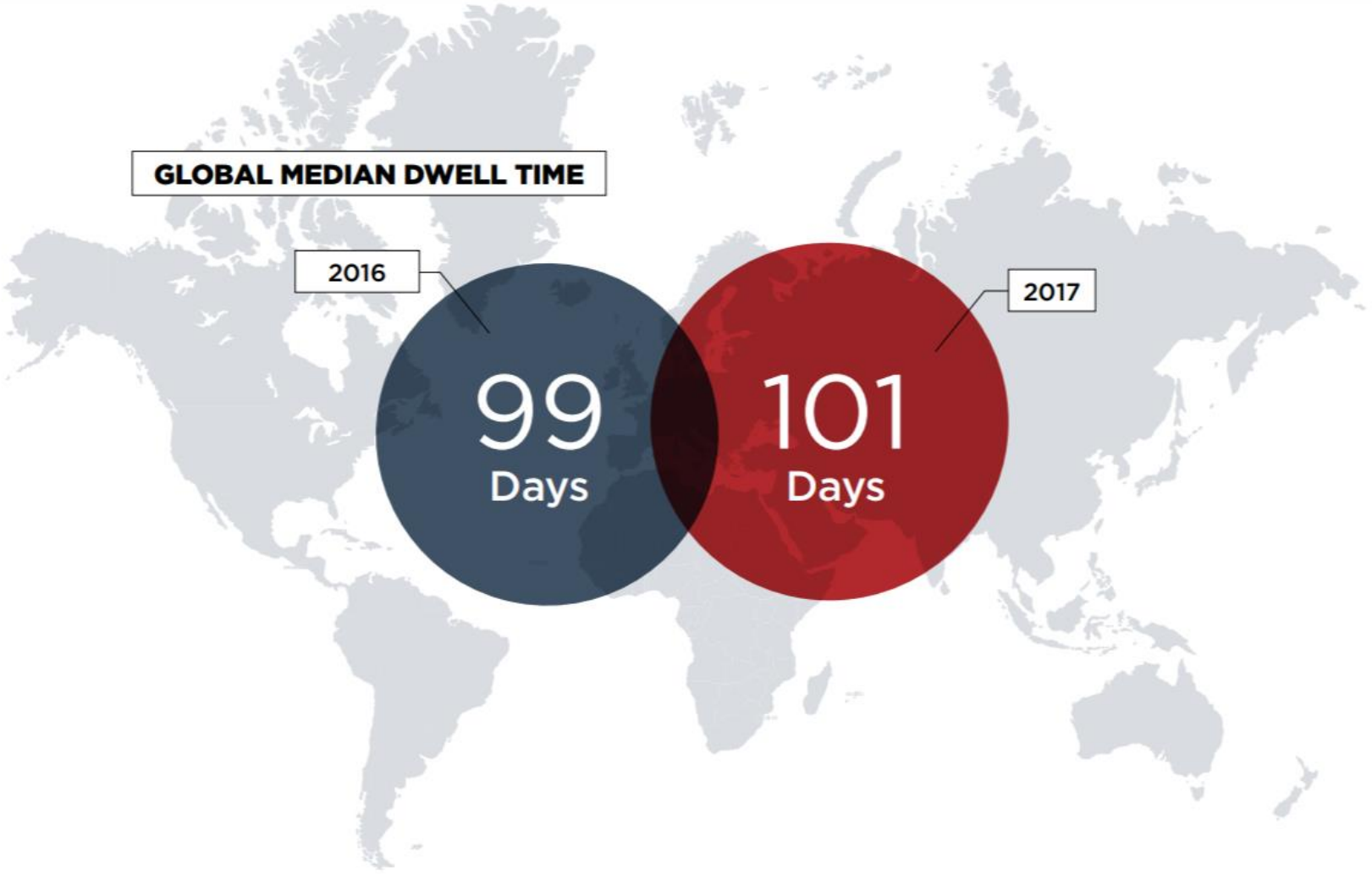
- High dwell time expected internally (First contact → detection)
  - Partly proofed by Penetration tests
- Very busy operational units
  - Focus on functional improvements and business enablement
- No global visibility (except System Monitoring) for security relevant activities

IT Security activities in the past

Protect	Detect	Respond
• Technical solutions, firewall, AV, Anti Spam, Sandbox, hardening…	• Partly automation, coincidence	• Ad-hoc, no dedicated or fixed structure and process

→ Subsidiary based solutions are not sufficient
→ Global implementation necessary

Dwell Time – First contact until detection



STIHL organizational change

Department *IT Security* founded and staffed start of 2018.
Focus areas around SOC:

- Security Operations Center (SOC)
  - Always available operational unit to verify and analyze security relevant events
  - Continuous update of patterns based on STIHL
  - Integration to standard operations means higher risk to overlook something

- Emergency Response Team (ERT)
  - Standardize Emergency Response activities on global level with dedicated team

Security Status - Target

Protection	Detect	Respond
• Technical solutions, firewall, AV, Anti Spam, Sandbox, hardening…	• Structured analysis of security relevant activities • Leveraging external expertise • Automation in detection • Reduce potential dwell time	• Standardized emergency processes • Standard escalations in case of an incident

→ Scope: Reduction or Prevention of damage for STIHL or the invidivual employee

Detect - Optimization tracks

SIEM/SOC

- Establish visibility on Security related events
- Manage Security Events

Vulnerability Management

- Establish visibility on vulnerabilities
- Ensure and organize mitigations

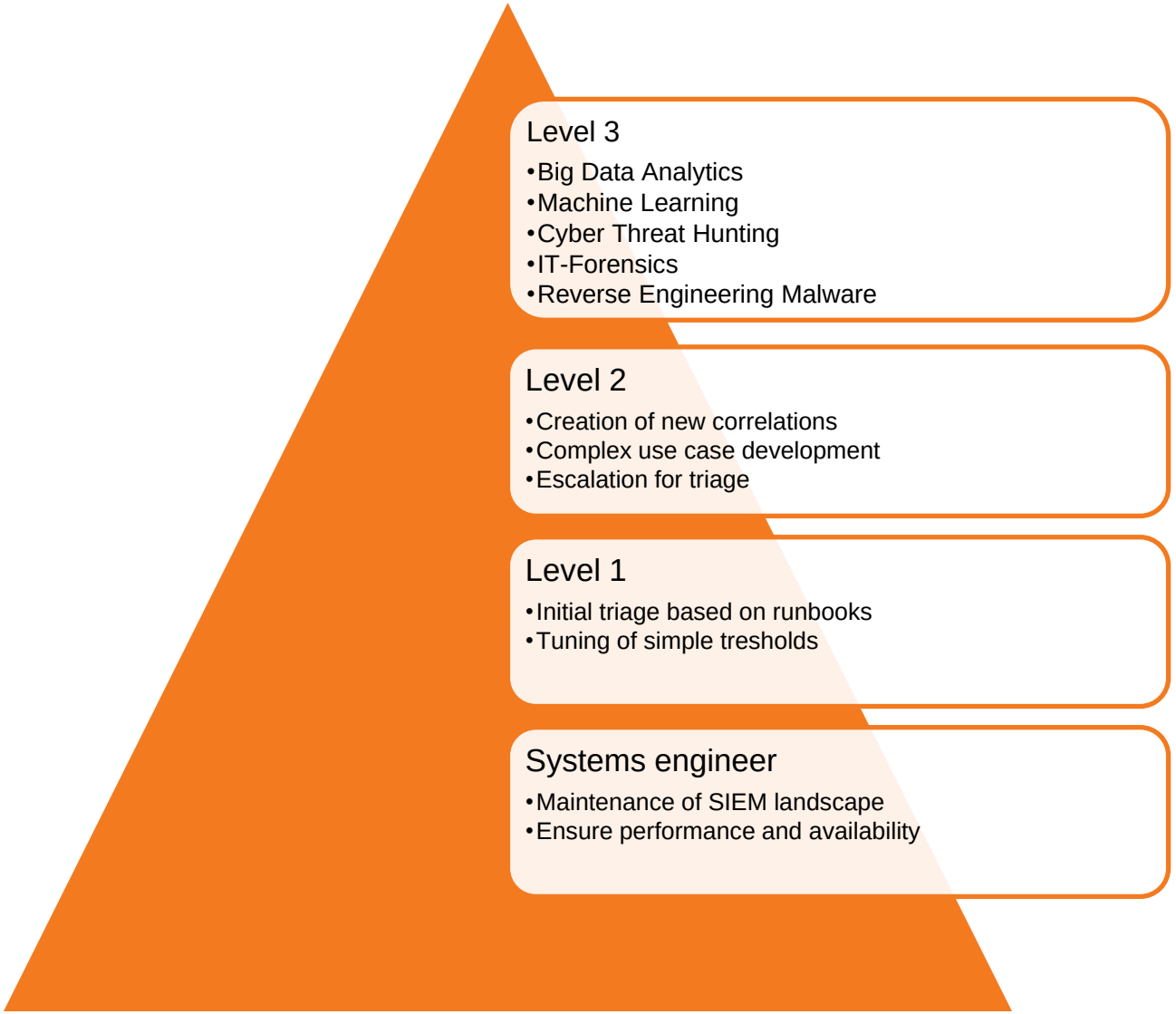
Enhanced detection

- Test and implement enhanced detection capabilities

STIHL SOC Project
Initial thoughts

- DIY vs. Managed Service
- SOC requirements:
  - 24 hours / 7 days
  - Expertise on current threat landscape
  - Analytics skills
  - Tooling skills
- DIY would require a dedicated team as this is a permanent task

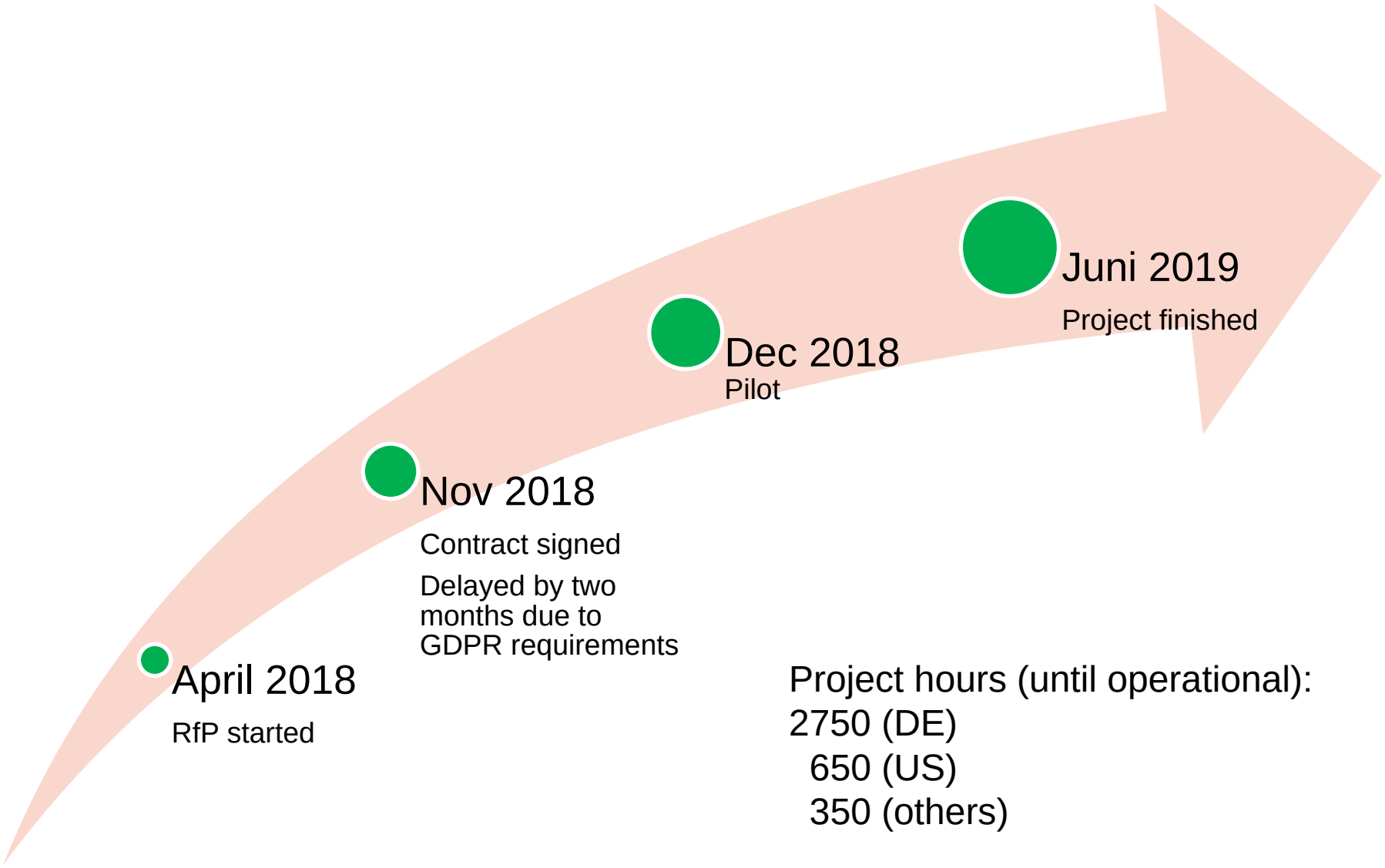
SOC Roles and responsibilities



STIHL SOC Project

- Increase visibility
- Empower STIHLs Security Team to mitigate or prevent threats to individuals or the organization
- Ensure compliance with laws and internal regulation
- Establish a global virtual security team with US and DE members
- Scope on Business IT
- Extension to Production IT possible

STIHL SOC Project Timeline



Project hours (until operational):
2750 (DE)
650 (US)
350 (others)

Provider Threat Manager

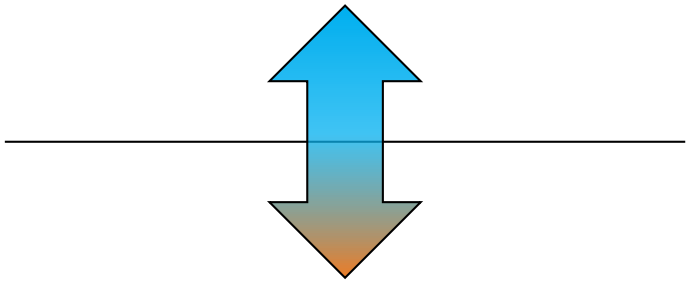
[redacted] Analysts Roles

- Platform care and feeding
- Triage alerts
- Alert Investigation
- False Positive Suppression
- Platform Tuning / IOC dev
- Threat Hunting
- Case Creation
- Notification
- Incident response assistance
- Custom reporting

Customer Roles

- Receive notifications
- Internal investigations
- Update cases with resolution
- Work directly with Threat Manager analysts
- Coordinate with law enforcement

Provider activities



STIHL Security Team

Technical onboarding limitations

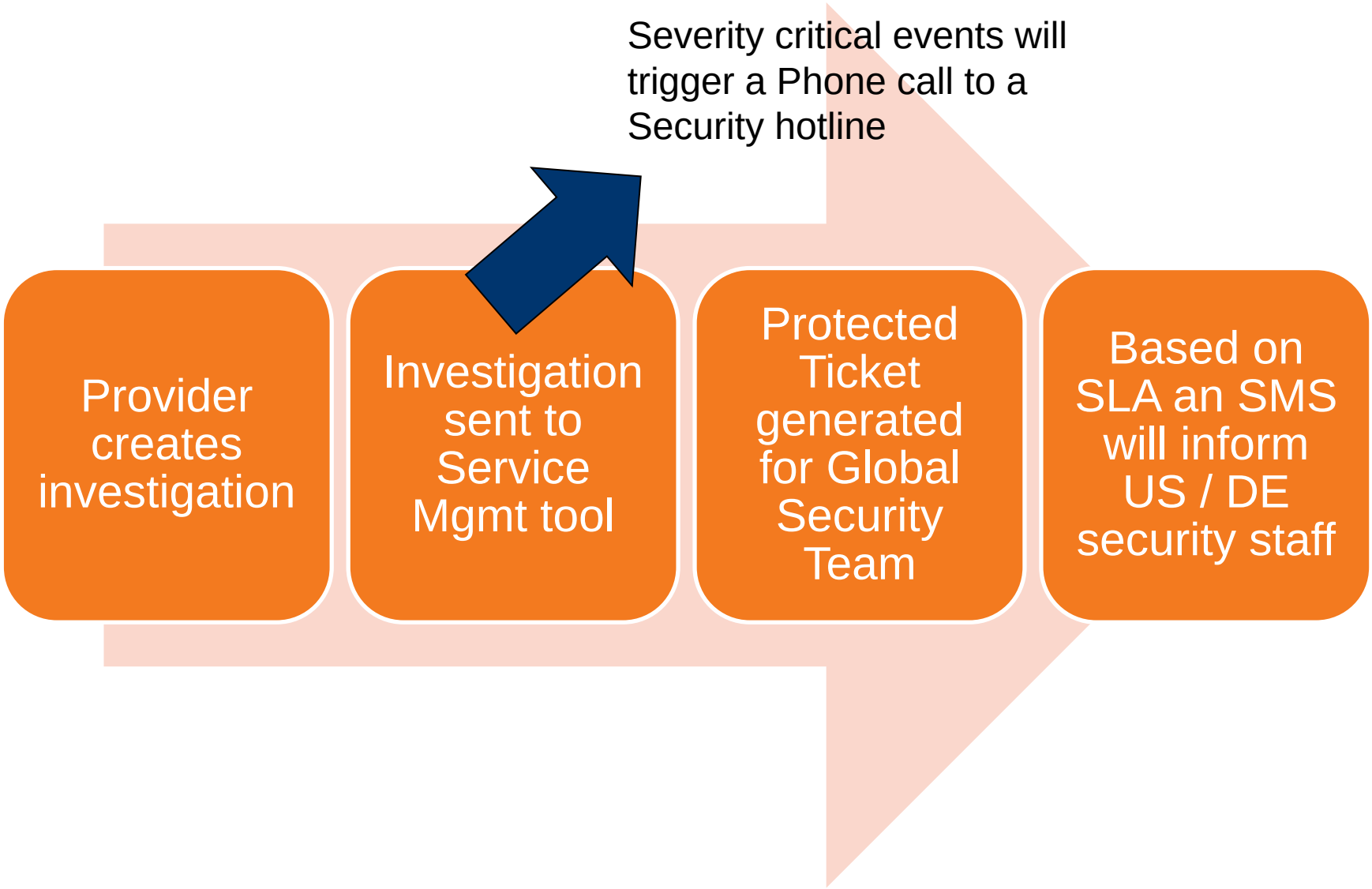
- Requirement from STIHL: no additional software on servers
- Event collectors are only running on ESX and HyperV
  - Linux appliance (near zero-touch)
  - No Google Cloud support so far
- Windows Event Collection Servers collect data from global Windows systems

- Sites with 200 servers and more will get dedicated Collector (Windows Events) and Sensor (AV)
- Remote sites will use US and DE based shared service Collectors / sensors

Onboarding procedures

- On-site installation assistance (STIHL DE) – Oct. 2018
  - Initial configuration and connection of systems with provider experts for three days
  - Finalizing critical component connections with provider and infrastructure experts
  - Provider: ensure proper parsing
- Weekly calls (STIHL DE/US + Provider)
  - Current operational issues
  - Initial investigations
  - Tuning
- Project finished / Start of operation – End of June 2019

Investigation workflow



Operations integration / Response optimization (Standard incident)

SOC (Provider)

- Identification of potential and active threats
- Identify countermeasures

STIHL Security Team

- Evaluation of proposed measures
- Start countermeasures or give order to execute them

Local IT

- Execution of the countermeasures
- Report back to the security team

STIHL Security Team

- In case of Local IT is not capable of executing the countermeasures:
  - Evaluating of necessary containment actions
  - Access on local systems with emergency accounts and HQ teams

Operations integration / Response optimization (Major incident)

SOC (Provider)

- Identification of potential and active threats
- Identify countermeasures

STIHL Security Team

- Evaluation of proposed measures
- Start countermeasures or give order to execute them

Major incident handling

- Escalation to Local IT + IT hierarchy
- Activate Emergency Response team
- Activate company emergency plan

Emergency Reponse team

- Security Team + Incident Handler + **external partner**
- Execute countermeasures on-site and remote

Virtual Security Team

- Virtual team consisting of US and DE employees
- Virtual team will work on all SOC-provided security incidents
  - No country-based scoping
  - With adaquate availability
- There is NO projected number of critical incidents that we expect

Virtual Security Team
Availability

- SIEM investigations will be feed into Service Mgmt tool
- These tickets will have special access control restrictions

- Critical incidents will be escalated immediately
  - 12-hours DE
  - 12-hours US
  - Escalation to HQ operations in case of no-response

- Non-critical incidents will accept 4-hours reaction time
  - Reduce night-activity to minimum

- Escalations will base on SLA tracking and SMS dispatch

Virtual Security Team
Work days / weekends

	6 – 18 (standard hours)
	On-call work

Detect
Challenges today

- Identities not harmonized (AzureAD, SAP-ID, Windows ID not seen as ONE identity)
- Log formats are often not as documented
- Use cases for hybrid environments mostly based on STIHL requirements
- Some collectors need to be reachable from the internet

Detect - Optimization tracks

SIEM/SOC

- Establish visibility on Security related events
- Manage Security Events

Vulnerability Management

- Establish visibility on vulnerabilities
- Ensure and organize mitigations

Enhanced detection

- Test and implement enhanced detection capabilities

Detect - Optimization tracks

SIEM/SOC

- Establish visibility on Security related events
- Manage Security Events

Vulnerability Management

- Establish visibility on vulnerabilities
- Ensure and organize mitigations

Enhanced detection

- Test and implement enhanced detection capabilities

Enhanced Detection under investigation

- Sysmon on all servers
- Sysmon on all clients
- Extend AV protection to endpoint detection & response (EDR)

- Further log sources

Defender‘s Dilemma

Attackers have to be right *once*

Defenders have to be right every time, everywhere… *forever*

STIHL Information Security
Thanks!