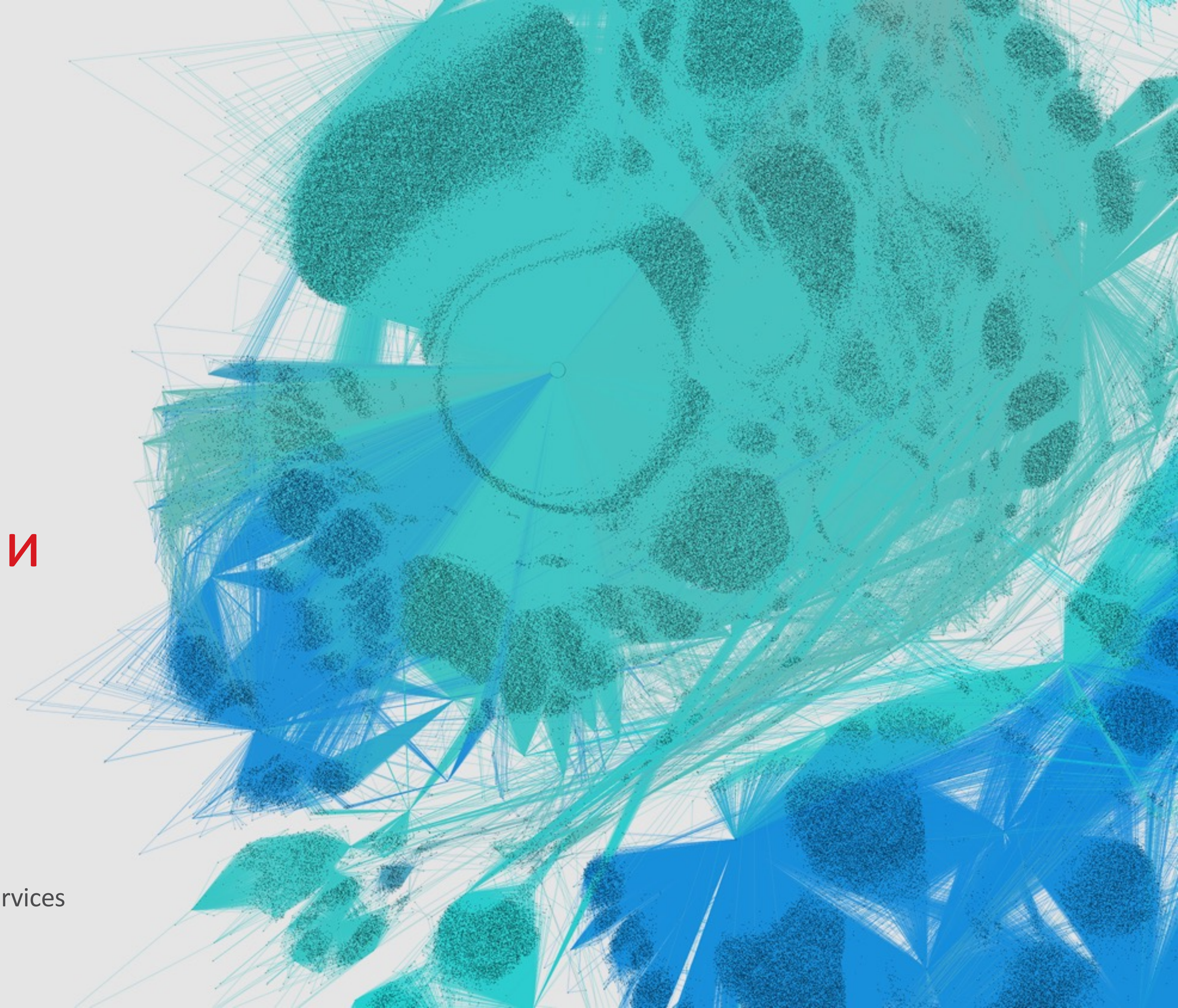
Реагирование на киберинциденты и этичный хакинг

Опыт Trend Micro

Almaty, Kazakhstan – 11.11.22

Nikolay Romanov, Director, IR & Professional Services



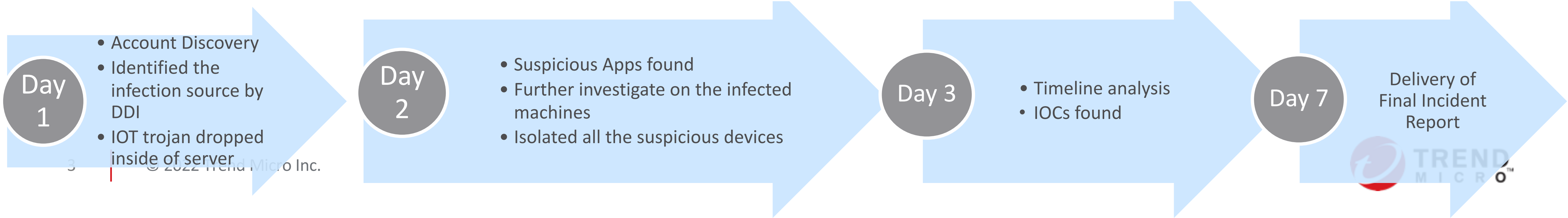
IR use case

🟦 Sensor Rule

🟩 Prevented by Product

MITRE ATT&CK Matrix – triggered areas

Reconnaissance	Execution Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Execution	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
🟦 Account discover using DDI	🟦 T1586 Compromise Accounts 🟦 Powershell 🟦 PC hunter 🟦 T1547 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder 🟦 Drop Troj.Win32.TRX. XXPE50FFF042 🟩 Create Medusalocker	🟦 T1078 Valid Accounts 🟩 T1053 Scheduled Task	🟩 T1112 Modify Registry	N/A	🟦 T1018 Remote System Discovery 🟩 T1063 Security Software Discovery	🟩 T1053 Scheduled Task T1204 User Execution	🟦 T1105 Remote File Copy	N/A	N/A	N/A	🟩 T1486 Data Encrypted for Impact T1489 Service Stop



Day 1

- Account Discovery
- Identified the infection source by DDI
- IOT trojan dropped inside of server

Day 2

- Suspicious Apps found
- Further investigate on the infected machines
- Isolated all the suspicious devices

Day 3

- Timeline analysis
- IOCs found

Day 7

Delivery of Final Incident Report

TREND MICRO Services Benefits

- Hundreds of Trend Micro experts at your side
- Access to industry-leading Trend Micro technologies & solutions
- Rapid response with guaranteed SLO for fastest mitigation
- Analysis extends across the network & endpoints
- Combined reactive & proactive strategy for pre-emptive reaction
- Local taskforce presence around the globe

OFFENSIVE security SANS ATT&CK®

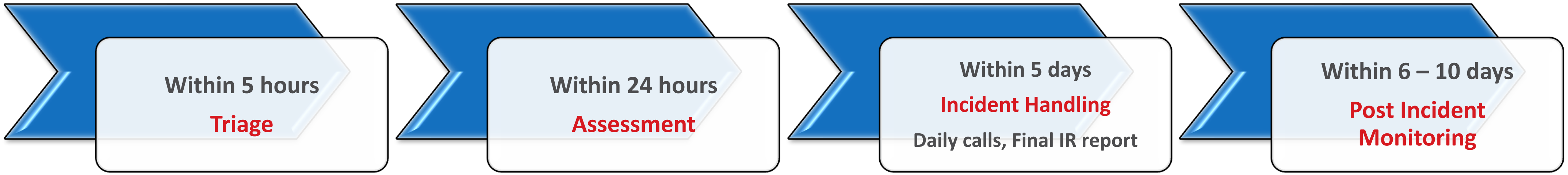
Our Services – Incident Response

TREND MICRO™
INCIDENT RESPONSE

Service 1: (**Reactive**) Forensic Investigation

- **“Classic” Incident Response** → Remediating, containing and investigating an ongoing cyber security incident
- Commonly **up to 3 weeks**
- **Focus** on speedy fulfilment of goals set by customer, mostly:
  - Rebuild IT environment (monitor network traffic, backups, forensic analysis of individual assets etc)
  - Support with information in discussions with crisis management

Response IR milestones



Within 5 hours
Triage

Within 24 hours
Assessment

Within 5 days
Incident Handling
Daily calls, Final IR report

Within 6 – 10 days
Post Incident Monitoring

- Receive customer's request
- Initiate the IR process
- Create ticket
- Fill the scoping sheet info
- Collect Logs from the machines pointed out by analyst or from minimum/default scope

- Analyze logs collected by the field team
- Create an initial report including the action plan
- Action Plan should include:
- Advise if any further logs/files that need to be collected
- Any urgent containment and cleaning actions
- Brief assessment according to the given information

- Daily call to discuss action items, recovery plan and timeline
- Criteria for bringing environment online (discussion with customer)
  (depends on confidence level of the customer with the solution(s) endpoint/network solutions available)
- 5th day discuss final incident report

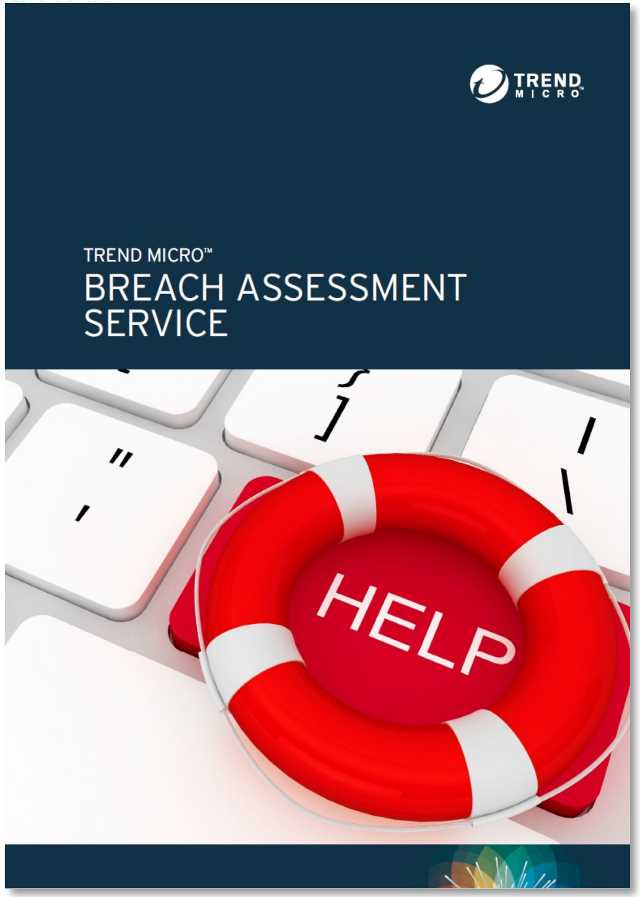
- Follow through recommendations (assisted by the field engineers)
- Solution Offerings
- Health check (paid or not paid)

Closure:

- (Product) stabilize environment + customer accepted the solution

(Per Incident)
- Indicators detected
- Incident Report presented to customer (2 weeks Q&A)

Our Services – Breach Assessment



TREND MICRO™

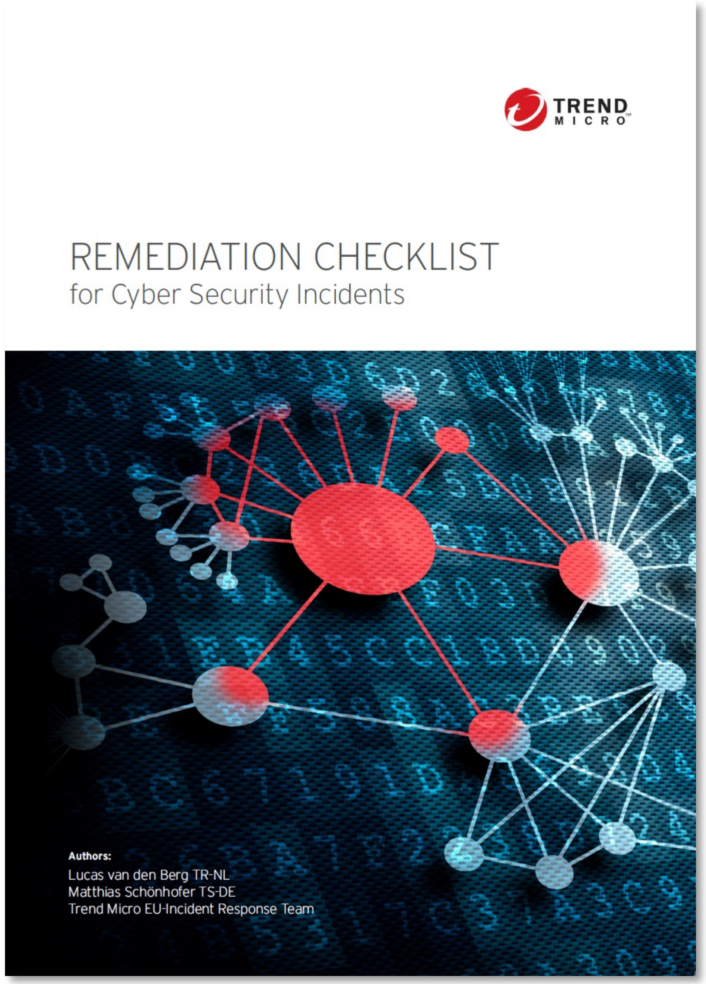
BREACH ASSESSMENT SERVICE

Service 2: (**Proactive**) Breach Assessment

- **“Background” Service** → Investigate & report on the state of play in an ongoing or (!) alleged cyber attack
- Helpful to **discover the blind spots** rapidly (3-5 days)
- **Focus** on “What is the risk we are currently exposed to?” – before or after an attack!

IR Engagement Process – Triage Call

- **Situation** => Attack suspected, ongoing or finished?
- **Processes, Politics, Plans** => Readiness, Insurance Policy, Business Continuity Plan, Third Party involvement etc?
- **Estate & Assets** => Amount of servers, endpoints, affected assets, domain structure, required external to internal communication and vice versa;
- **Trend Customer Footprint** => Platforms, Deployment or Rollout Status, MXDR Customer?
- **Customer Expectations** => What do they expect from us, what can we deliver?



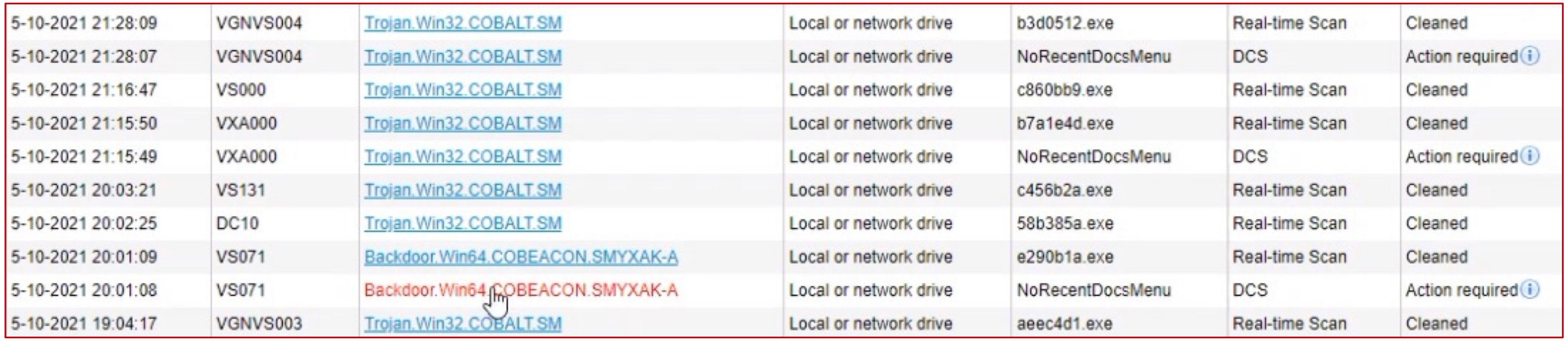
TREND MICRO

REMEDIATION CHECKLIST
for Cyber Security Incidents

Authors:
Lucas van den Berg TR-NL
Matthias Schönhofer TS-DE
Trend Micro EU-Incident Response Team

Breach Assessment - Threat Hunting (Example)

Customer's Metadata



5-10-2021 21:28:09	VGNVS004	Trojan.Win32.COBALT.SM	Local or network drive	b3d0512.exe	Real-time Scan	Cleaned
5-10-2021 21:28:07	VGNVS004	Trojan.Win32.COBALT.SM	Local or network drive	NoRecentDocsMenu	DCS	Action required ⓘ
5-10-2021 21:16:47	VS000	Trojan.Win32.COBALT.SM	Local or network drive	c860bb9.exe	Real-time Scan	Cleaned
5-10-2021 21:15:50	VXA000	Trojan.Win32.COBALT.SM	Local or network drive	b7a1e4d.exe	Real-time Scan	Cleaned
5-10-2021 21:15:49	VXA000	Trojan.Win32.COBALT.SM	Local or network drive	NoRecentDocsMenu	DCS	Action required ⓘ
5-10-2021 20:03:21	VS131	Trojan.Win32.COBALT.SM	Local or network drive	c456b2a.exe	Real-time Scan	Cleaned
5-10-2021 20:02:25	DC10	Trojan.Win32.COBALT.SM	Local or network drive	58b385a.exe	Real-time Scan	Cleaned
5-10-2021 20:01:09	VS071	Backdoor.Win64.COBEACON.SMYXAK-A	Local or network drive	e290b1a.exe	Real-time Scan	Cleaned
5-10-2021 20:01:08	VS071	Backdoor.Win64.COBEACON.SMYXAK-A	Local or network drive	NoRecentDocsMenu	DCS	Action required ⓘ
5-10-2021 19:04:17	VGNVS003	Trojan.Win32.COBALT.SM	Local or network drive	aeec4d1.exe	Real-time Scan	Cleaned

- 12:00: Cobalt Strike Detections found in Customer's Environment
- 13:00: Triage Call w/ Customer
- 16:00: Customer agrees to Engagement
- 20:00: Network sensor (DDI) logistics to customer's site
- 20:51: Network sensor (DDI) operational
- 22:00: Active Attack activities observed (Security Agent Unloaded)
- 22:30: Disconnected from Parent Company and Internet
- 23:00: Ransomware detonated in Parent Company

Analysis of Forensic Evidence - Forensics Lab Example ☺

Our Services – Red Teaming

TREND MICRO™

TREND MICRO RED TEAMING

Systematically improve your Cyber Resilience by understanding how and where an Attacker can hit you best.

Red Teaming / Purple Teaming

- Carefully Planned, Expertly Executed, Tightly **Controlled Simulation of a Real-World Cyber Attack t**o identify weaknesses within the Cyber Security Posture
- Utilizing newly gained Intelligence will help to crucially improve Cyber Defenses

The Red Team Arsenal

Key toolset:

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

Tactics, Techniques and Procedures:

- Exploitation of known Vulnerabilities
- Social Engineering
- Phishing
- Privilege Escalation
- Lateral Movement
- Persistence

Social Engineering

How do we plan a Red Teaming Exercise?

Preparation Phase

Red Teaming Phase

Closure Phase

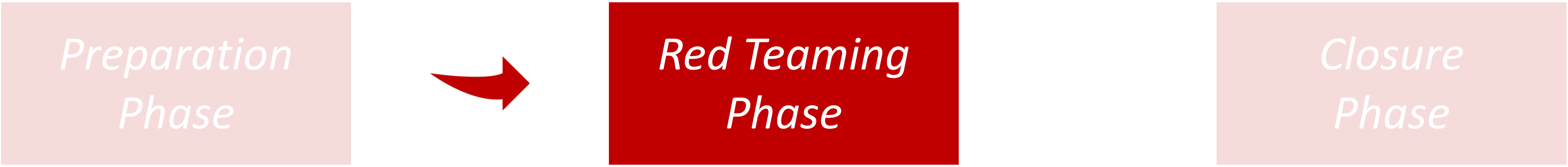
Initial Interviews & Customizing

- To present available RT Scenarios: APT, Insider Threat, Ransomware, etc depending on customer’s specific Threat Landscape exposure
- Goals: What are your specific objectives for this Red Teaming exercise?
- Safety Guardrails: Assets to be excluded, general exercise handling, duration, legal aspects.

Legal Framework

- Cyber Agreement: NDA, Roles & Responsibilities, Commercial Terms, T&C.
- Rules of Engagement (RoE): Targets, Exclusions (Black List), Tools, TTP’s etc.

How do we plan a Red Teaming Exercise?



Preparation Phase

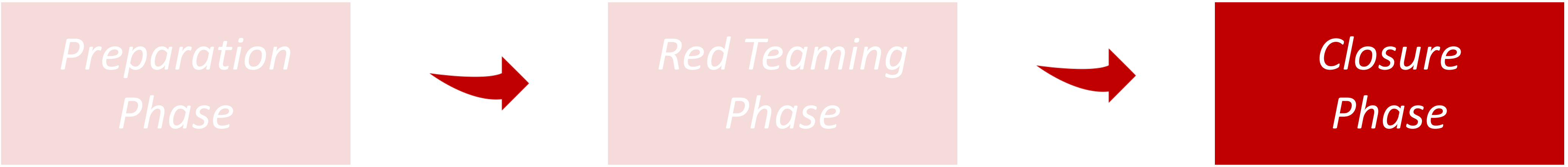
Red Teaming Phase

Closure Phase

Execution of Red Teaming Exercise

- Adversary emulation to infiltrate customer network according to agreed RoE
- Accompanying Purple Teaming if agreed upon
- Incident Response services (if required)

How do we plan a Red Teaming Exercise?



Preparation Phase

Red Teaming Phase

Closure Phase

Lessons Learned

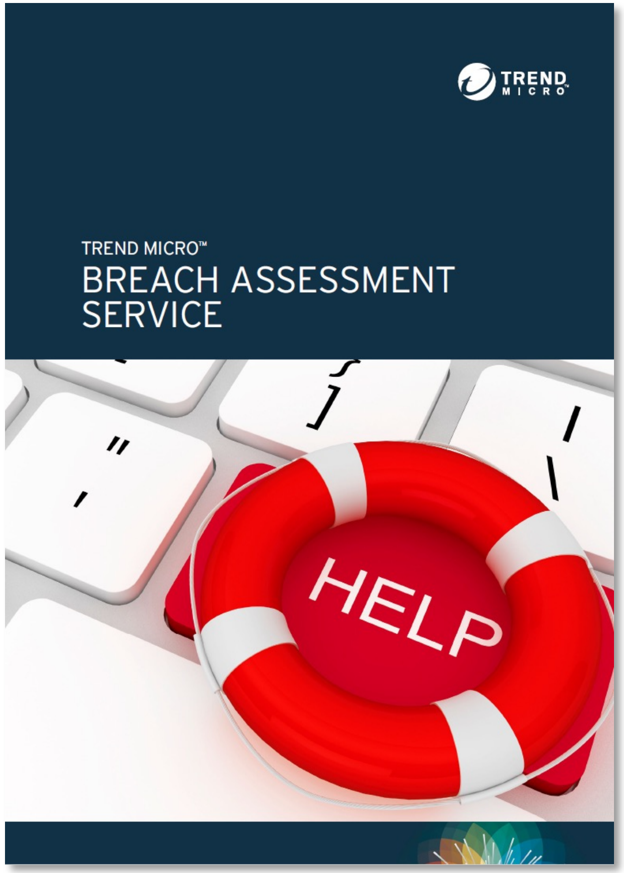
- Goal is to go over all attack scenarios and discuss how the threat could have been detected and mitigate
- Also: RT‘ing can be repeated after 10-12 months cycle to test improvements

Final Red Team Report

- Standardized report describing the RT exercise, findings, IOC‘s, recommendations and a portoflio of all associated documents the initial Threat Landscape assessment completed in the Preparation Phase

Each engagement always provide

- **CONTINUOUS MONITORING** to help a customer with on-going attacks containment
- **TRUST** Support & Help in criticial situation often creates beneficial situation to improve Trend Micro standing with customer
- **ROOT CAUSE ANALYSIS REPORT** with all the comprehensive details and recommendations



TREND MICRO™
BREACH ASSESSMENT
SERVICE

THE ART OF CYBERSECURITY

Automated hybrid cloud workload protection via calls to Trend Micro APIs. **Created with real data by Trend Micro threat researcher and artist Jindrich Karasek.**